

Open Vocational Education Program

CYBER SECURITY ASSISTANT



NATIONAL INSTITUTE OF OPEN SCHOOLING

(An autonomous organisation under MoE, Govt. of India)

A-24-25, Institutional Area, Sector-62, NOIDA-201309 (U.P.)

Website: www.nios.ac.in, Toll Free No. 18001809393

COURSE TEAM

ADVISORY COMMITTEE

Chairman

NIOS, NOIDA, U.P.

Director (Vocational)

NIOS, NOIDA, U.P.

CURRICULUM COMMITTEE

Prof. Pachigolla Venkata Suresh
Director, School of Computer and
Information Sciences, IGNOU
New Delhi

Dr. Deepti Mehrotra
Director, Amity Institute of
Information Technology
Amity University, Noida

Dr. Anurag Jain
Guru Gobind Singh IP University
New Delhi

Mr. Ram Ganesh
CEO, IB Hubs
Hyderabad

Dr. Balakrishnan Athiyaman
Scientist F & amp;
Head, Ministry of Earth Sciences
Noida, U.P.

Ms. Radhika B.
Deputy Director
(Vocational Education Department)
NIOS, NOIDA, U.P.

LESSON WRITERS

Mr. Deepanshu
Assistant Secretary
Academic Assessment
CBSE , Delhi

Mr. Pulkit Rathi
Deputy Superintendent of Police
National Investigation Agency
New Delhi

Ms. Mohini Arora
HOD (Computer Science)
Air Force Golden Jubilee Institute
Subroto Park, New Delhi

Mr. Vijay Kumar Prajapati
TGT (Computer Science)
Directorate of Education
GNCT of Delhi

Mr. Mayank Bhushan
TGT (Computer Science)
Directorate of Education
GNCT of Delhi

Ms. Sarika Minocha
PRT (Computer Science)
Apeejay School, Delhi

EDITORS

Ms. Purvi Kumar (editor)
PGT & Head of IT
Ganga International School
New Delhi

Mr. Akshay Kumar (editor)
PGT (Computer Science)
Directorate of Education
GNCT of Delhi

COURSE COORDINATOR

Ms. Anchal Goswami
Academic Officer (ICT)
NIOS, NOIDA, U.P.

TYPESETTING

M/s Sri Krishna Graphics
Delhi

A Word With You

Dear Learners

In today's interconnected world, where technology drives nearly every facet of our lives, safeguarding our data and digital systems has become an indispensable necessity. As cyber threats continue to evolve in complexity, acquiring knowledge in cyber security has transitioned from a mere option to a critical requirement. By developing expertise in this field, you not only enhance your personal security but also position yourself for wider career opportunities in one of the most rapidly growing and essential sectors worldwide.

The **Cyber Security Assistant** course has been specially designed to equip you with the knowledge and practical skills required to address the ever-evolving challenges in cybersecurity. The curriculum is aligned with the qualification pack for **Cyber Security Assistant at Level 3.5**, encompassing essential areas such as cyber security fundamentals, network security, vulnerability assessment, penetration testing, and cybercrime awareness. In addition to theoretical knowledge, you will gain practical experience with industry-standard tools like Nmap, Nessus, and Wireshark, enabling you to effectively identify and mitigate vulnerabilities, secure networks, and safeguard digital platforms.

The course also emphasizes critical employability skills like effective communication, problem-solving, and digital literacy. You will also learn about cyber laws, digital hygiene, and India's cybersecurity initiatives, preparing you for real-world scenarios. Through practical exercises, case studies, and a user-friendly approach, this course ensures that you are not just learning but truly building a foundation for a successful career in cyber security.

You will certainly find this journey exciting, informative, and transformative. Practice diligently, engage with the material, and unlock your potential to become a skilled **Cyber Security Assistant**.

Wishing you the very best for a secure and successful future!

Course Team NIOS

Contents

1. Operating System	1
2. Overview of Web Development	30
3. Computer Networks	50
4. Web Application and Security	77
5. Employability and Communication Skills	92
6. Fundamentals of Cyber Security	116
7. Introduction to Network Security	151
8. Vulnerability Assessment and Penetration Testing	185
9. Digital Forensics: Processes and Documentation	203
10. Operating System Security	226
11. Cyber Awareness	236
12. Understanding Cyber Law and IT Act, 2000	254



1

OPERATING SYSTEM

INTRODUCTION

An operating system is one of the major parts of the computer system. Without an operating system, no computer will be able to run any other program or application. The first program that loads up with the computer booting is referred to as an operating system. The hardware and the operating system communicate by communicating with the BIOS (Basic Input Output System). It performs the basic functions such as keyboard input recognition, output to the display screen, tracking files and directories on the disk, control of peripheral devices such as disk drives, printers, etc. In this lesson, you will learn about an operating system in detail.



OBJECTIVES

After reading this lesson, you will be able to:

- explain the definition and structure of an operating system;
- describe various functions and management service roles provided by OS;
- describe features and file systems of Windows and Linux operating system;
- demonstrate basic usage of the command line. (Windows and Linux).

1.1 OPERATING SYSTEM

An operating system is a bridge between the user and the computer hardware. It is one of the most important systems of software that manages all operations on the computer. Some examples of operating system are DOS, Microsoft windows (Windows 95, Windows XP, Windows 10, Unix, Linux, macOS)



Notes

Operating system performs the following tasks:

- An operating system performs several crucial tasks to keep a computer functioning properly. When the computer is powered on, a boot program loads the operating system into memory. Once the OS is loaded, it takes control and manages all the other application programs installed on the system.
- The operating system is responsible for managing the computer's hardware, software, and various resources. This includes overseeing memory, registers, processors, devices, and information, ensuring everything works efficiently together.
- Application programs, such as Google Maps, Swiggy, and BookMyShow, request services from the operating system through a defined interface known as the **Application Program Interface (API)**. This allows the apps to interact with the system and perform necessary tasks.
- Users interact directly with the operating system through a user interface. This can either be a **Command-Line Interface (CLI)** or a **Graphical User Interface (GUI)**, depending on the system's design and user preference.

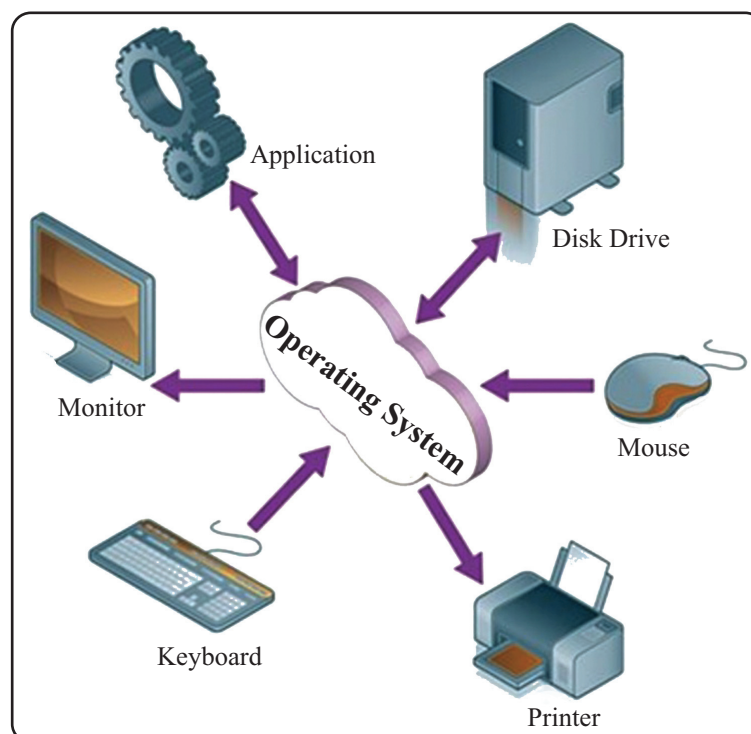


Fig. 1.1



Characteristics of Operating System

Let's discuss some characteristics of operating system:

- **Concurrency:** An operating system is able to handle multiple tasks and multiple users at the same time, providing efficient multitasking and resource allocation.
- **Hardware Abstraction:** It provides an extra layer that acts as an interface between hardware and operating system, to simplify communication and enhance system performance.
- **Fault Tolerance:** The operating system is able to handle hardware and software failures. It can easily perform error detection and recovery mechanisms, hence preventing data loss.
- **Compatibility:** The operating system is compatible with a wide range of hardware and software devices, supporting software and hardware operations across different platforms and configurations.
- **Security:** Operating system provides protection from unauthorized access and firewall, through mechanisms like user authentication and firewalls, thus enhancing overall system security.



INTEXT QUESTIONS 1.1

Multiple choice questions:

1. The operating system work between
 - (a) User and Computer
 - (b) Network and User
 - (c) One user to another user
 - (d) User to software
2. Which of the following is not an operating system?
 - (a) Windows
 - (b) Java
 - (c) Linux
 - (d) DOS
3. Which program is loaded after starting a computer?
 - (a) Window desktop
 - (b) Network connection program
 - (c) Operating system
 - (d) CMD



Notes

4. What operations are performed by an operating system?
 - (a) Maintaining recycle bin
 - (b) Transfer files
 - (c) Opens a program
 - (d) All of the above
5. The operating system manages;
 - (a) recovery
 - (b) booting from disk
 - (c) disk initialization
 - (d) all of the above mentioned
6. If the computer system does not have a/an it will not boot.
 - (a) Interpreter
 - (b) Compiler
 - (c) Operating System
 - (d) Assembler

1.2 OPERATING SYSTEM STRUCTURE

The operating systems are large and complex. A common design approach to designing an operating system is splitting the system into smaller elements, or modules to smaller, more manageable tasks. Also, every segment is a part of the operating system. The structure of an operating system can be perceived as the method which links together and integrates different components of an operating system into its kernel which represents the core part of any operating system, acting as an intermediary between hardware and various processes.

The various structures of an operating system are explained in greater detail in the following sections.

1.2.1 Simple Structure

The Simple structured operating systems are small, simple and have limited capabilities. Microsoft Disc Operating system (MS-DOS) followed Simple Structure (refer Fig.1.2). The interfaces and levels of functionality are not well separated. In MS-DOS, application programs are able to access the resident system programs as well as the base hardware. Base hardware can be accessed by drivers, resident programs and application softwares. This type of operating system may crash the entire system if one of the user program fails as all layers of the structure are interconnected.

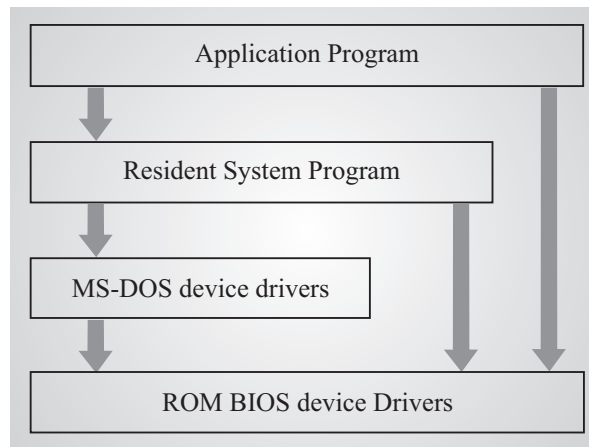


Fig. 1.2: Simple Structure of an MS-DOS Operating System

1.2.2 Monolithic Structure

Older versions of the Unix operating system followed a monolithic structure. The entire operating system works in kernel space. It alone defines a high-level virtual interface over computer hardware. Since, everything in the kernel is packed into one level we call it a monolithic structure. The execution of the monolithic kernel is quite fast because the services such as memory management, file management, process scheduling, etc., are implemented under the same address space. If there is an error in any module, it could affect the entire application's availability. Due to this reason implementation and maintenance is very difficult in this structure.

1.2.3 Layered Approach

Operating systems can be divided into a number of layers(levels) that are smaller and more appropriate. In layered structure the functionalities are broken into different layers and an OS can retain much greater control over the computer. In a layered approach, the bottom layer (layer 1) is the hardware; the highest layer (layer 6) is the user interface. The layers between layer 1 and 6 are for CPU scheduling, memory and process management and I/O buffer. This layering structure is depicted in Fig.1.3.

The advantage of the layered approach is simplicity of construction and error detection.. All lower-level layers are examined before the upper layer is examined. We need to be careful in designing the layers as upper layers only make use of lower layers' capabilities. The main disadvantage of layered structure is that data needs to be modified and passed on at each layer with an added overhead due to which performance of the entire system is compromised in layered structures for example Windows NT.



Notes

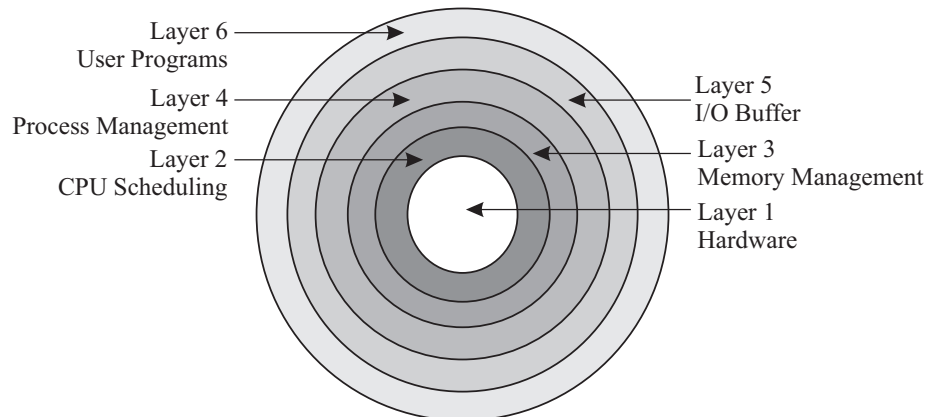


Fig. 1.3: Layered Approach of an Operating System

1.2.4 Microkernels

A microkernel is a type of operating system kernel that is designed to provide only the most basic services required for an operating system instead of having a big kernel with many functionalities. In a microkernel, the user services and kernel services are implemented in different address spaces.

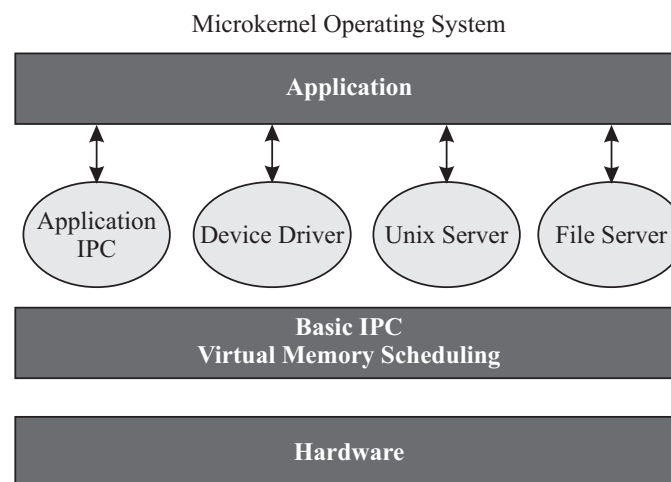


Fig. 1.4: Microkernel Operating System

All non-essential components are removed from the kernel and implemented as system and user level programs.

Core functionalities to the kernel such as memory management and process scheduling are provided in microkernels. Other services, such as device drivers and file systems, are implemented as user-level processes that communicate with the microkernel indirectly by exchanging messages. (refer Fig. 1.4)

This design allows the operating system to be more modular and flexible than traditional monolithic kernels. Operating system can be easily extended. All new services can also be added to user space and do not require kernel modification. It is a more secure and stable operating system because it has a smaller attack surface.



1.2.5 Modular Structure

A modular operating system is built from separate modules that perform specific functions. A modular operating system is one that is composed of independent components that can be added, removed, or replaced without affecting the whole system. Each module can communicate with other modules through well-defined interfaces, and can be loaded or unloaded dynamically as needed. This design approach offers several benefits for developers, users and administrators of operating systems.

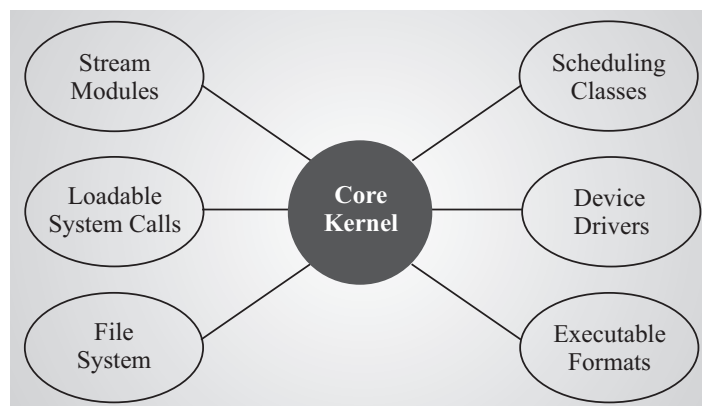


Fig. 1.5: Modular Structure of an Operating System

1.2.6 Hybrid Systems

A hybrid operating system is a combination of monolithic and microkernel operating systems. It is a combination of elements from both Operating Systems.

It has a kernel that provides more functions and services. It also has modules or processes that run in user mode and communicate with the kernel and each other through various mechanisms, such as message passing, shared memory, or direct function calls.

The advantage of a hybrid operating system is that it balances between performance and modularity, as it can optimize the communication or switching between different components depending on the situation. The disadvantage is that it is more complex and inconsistent, as it has different design principles or interfaces for different components. Examples of hybrid operating systems are Windows NT, MacOS X, and Android.

**INTEXT QUESTIONS 1.2****Multiple Choice Questions:**

1. In layered approach of Operating Systems
 - (a) Bottom Layer is the User interface
 - (b) Bottom Layer is the hardware
 - (c) Highest Layer is the hardware
 - (d) None of the above
2. is a combination of both monolithic and microkernel operating system.
 - (a) Simple Structure
 - (b) Modular OS
 - (c) Hybrid system
 - (d) None of the above
3. Which operating system followed monolithic structure.
 - (a) Windows
 - (b) Android
 - (c) Unix
 - (d) IOS
4. An operating system structure that is composed of independent components that can be added, removed, or replaced without affecting the whole system.
 - (a) Modular
 - (b) Simple
 - (c) Hybrid
 - (d) Monolithic
5. What operating system structure does WindowsNT have?
 - (a) monolithic kernel with modules
 - (b) Microkernel
 - (c) monolithic kernel
 - (d) hybrid kernel

1.3 FUNCTIONS OF AN OPERATING SYSTEM

An operating system is the basic structure of any computer system, and it works as a bridge between the user and application software with the help of hardware. It maintains smooth and efficient running through resource management, task coordination and an assured security environment for the applications running on it. The main operations and functions of an operating system are as follows:

Operating System

- Process Management
- Memory Management
- I/O device management
- File Management
- Network Management
- Security and Protection
- User Interface
- Backup & Recovery



Notes

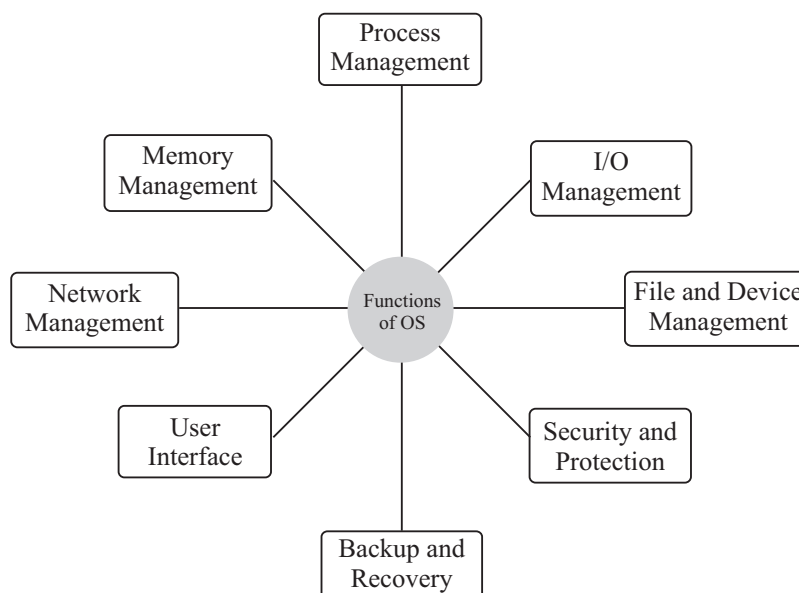


Fig. 1.6: Functions of an Operating System

- **Process Management:** A program is a set of logical instructions given to the computer and a program that is in an execution state is called a process. A process needs certain resources-such as CPU time, memory, files and I/O devices to accomplish its tasks. These resources are allocated to the process either when they are created or while they are executing. Process management involves various tasks like creation, scheduling, termination of processes. Processes are allowed to use the CPU for a limited time, which may be a fraction of a second. To enhance CPU utilization and allow multiple processes to run, process scheduling is performed by the OS. The operating system is responsible for creation, deletion, and scheduling of various processes that are being executed at any point of time.



Notes

- **Memory Management:** The operating system manages the computer's primary memory and provides mechanisms for optimizing memory usage. It allocates or deallocates memory space as needed. The OS keeps track of every memory location that is either assigned to some process or is free. It also checks how much memory should be assigned to each process.
- **I/O Management:** We interact with the computer by providing information through input output devices. The operating system manages input/output devices such as printers, keyboards, mouse and displays. It provides the necessary drivers and interfaces to enable communication between the devices and the computer.
- **File Management:** The operating system is responsible for organizing and managing the file system, including the creation, deletion, and manipulation of files and directories.
- **Network Management:** The operating system provides networking capabilities such as establishing and managing network connections, handling network protocols, and sharing resources such as printers and files over a network.
- **Security & Protection:** The operating system provides a secure environment for the user, applications and data by implementing security policies and mechanisms such as access controls and encryption.
- **User Interface:** The operating system provides a user interface that enables users to interact with the computer system. This can be a Graphical User Interface (GUI), a Command-Line Interface (CLI), or a combination of both.
- **Backup and Recovery:** The operating system provides mechanisms for backing up data(duplicating and storing at a safe location) and recovering it in case of system failures, errors or disasters.



INTEXT QUESTIONS 1.3

Multiple Choice Questions:

1. A program that is in an execution state is called a
 - (a) Data
 - (b) Process
 - (c) Program
 - (d) All of the above



2. is responsible for organizing and managing the file system, including the creation, deletion, and manipulation of files and directories.
 - (a) Process management
 - (b) Memory Management
 - (c) File Management
 - (d) I/O Management
3. Process scheduling is performed by
 - (a) Operating System
 - (b) Scheduler
 - (c) C.PU.
 - (d) I/O Management
4. Which one of the following errors will be handled by the operating system?
 - (a) lack of paper in printer
 - (b) connection failure in the network
 - (c) power failure
 - (d) all of the mentioned

1.4 FEATURES OF WINDOWS 10 OPERATING SYSTEM

Windows operating system is the graphical user interface (GUI) based operating system developed by Microsoft corporation. It is one of the most popular and widely used operating system in the world. The first version of the Windows operating system was released in 1985, with upgraded versions introduced in the following years.

Microsoft Windows 10 is one of the popular version of Windows operating system released on 29th July, 2015. It included lots of new features and improvements as compared to previous versions of Windows which can be described as follows :

- **Start Menu:** It is located on the taskbar. It has been expanded and it is easier to find important apps.
- **Windows Back-up:** With Windows Backup, you can keep your data safe and secure. You can now backup installed apps and other important information on your PC.
- **Sync your PC and phone:** Using Windows 10 you can make and take calls. Reply to text messages. Check and even dismiss notifications. This feature is available for Android.
- **Microsoft Edge:** Microsoft Edge is fast, secure and easy to use web browser. It has built-in learning and accessibility tools that enhance your browsing experience.
- **OneDrive backup:** OneDrive backup is available in Windows 10. This keeps your photos, documents and other files safe.



Notes

Operating System

- **Snap assist:** Snap open windows side by side to maximize your screen space, utilize multiple monitors, and enjoy the benefits of touch-enabled displays.
- **Action Center:** The action center is a window that allows you to access useful shortcuts and tools quickly. Various services like Wi-Fi, Bluetooth and location are available in it.
- **Microsoft account:** A Microsoft account can be your one passport to all things from Office to Xbox and more.
- **Desktop groups:** With desktop groups, you can organize your open apps and windows into separate “desktops” to make it easier to switch between work and play modes. This feature was introduced in Windows 10.
- **Firewall and network protection:** Windows comes with built-in security features to help safeguard against viruses, malware, and ransomware etc.
- **Parental controls and protection:** Windows can manage screen time, limit access to mature content, and control online purchases for their children. InPrivate browsing is also blocked, disabling incognito browsing by the child.
- **File Explorer:** The file explorer in Windows 10 allows the user to access files. You can open, close, delete, share and copy your files easily with the help of file explorer.
- **Task View:** This view can be opened by clicking on the Task view from the Taskbar. It allows the user to change the tab that is open. You can also use it to see all the tabs at one time and remove any tab you do not want.



INTEXT QUESTIONS 1.4

Multiple Choice Questions:

1. Windows 10 was created by
 - (a) Sun Microsystems
 - (b) Microsoft
 - (c) Apple
 - (d) IBM
2. Using Windows 10 Operating system
 - (a) You can make calls
 - (b) Send Messages
 - (c) Check for notifications
 - (d) All of the above



3. Which of the following is a component of the Windows operating system?
 - (a) Microsoft Edge
 - (b) Microsoft Word
 - (c) Photoshop
 - (d) None of the above
4. Which utility opens windows side by side to maximize the screen space?
 - (a) Sync
 - (b) Snap Assist
 - (c) Start button
 - (d) One drive
5. Start Button is located on the
 - (a) Taskbar
 - (b) Title Bar
 - (c) Status Bar
 - (d) None of the above
6. What is Microsoft Windows?
 - (a) Operating system
 - (b) Graphics program
 - (c) Word Processing
 - (d) Database program

1.5 BASIC WINDOWS COMMANDS

Windows basic commands can be typed using Microsoft Command Prompt. Microsoft command prompt is a command-line interpreter (CLI) for the Windows OS. A CLI is a program intended primarily to read operating system instructions typed through a keyboard by the user and accomplish a wide range of tasks. This interface shields the user from directly accessing the operating system kernel, also called shells. Given the name of the Command Prompt executable file, cmd.exe, the Command Prompt is friendly named cmd. It is also said to be the console. Command line interpreter is available with Windows NT, Windows 10 etc. To open the command prompt in Windows 10, follow these steps:

Press Windows + R to open the Run command window.

OR

Type “cmd” in the search box located on the taskbar.

- mkdir/md
 - This command is used to create directories or subdirectories.
Syntax: mkdir <drive> <path> <press enter key>
Example: mkdir directory2023
(This command will create a directory (directory2023) within the current directory)



Notes

```
Command Prompt
C:\Users\India>mkdir root
C:\Users\India>cd root
C:\Users\India\root>S_
```

- Cd of chdir (*Change directory*)
 - This command changes the current working directory to a specified directory.

Syntax : cd destination <press enter key>

Example: cd Windows

```
Command Prompt
C:\>cd windows
C:\Windows>
```

- Chkdsk (*Check Disk*)
 - This command is used to check and repair issues in the disk.
- Chkdsk Syntax : chkdsk <press enter key>
- Cls
 - This command clears the cmd screen.
- Cls Syntax : cls <press enter key>

```
Command Prompt
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

C:\Users\India>cd documents
C:\Users\India\Documents>cls
```



After executing the command

```
CA: Command Prompt
C:\Users\India\Documents>_
```

- Copy

- This command copies one or more files to another location.

Syntax : copy <source file> <destination file> <press enter key>

Example: copy c:\test.txt d:

(This command will copy “test.txt” from C: drive to D:)

- Date

- This command is used to display date or change it..

Syntax : date <press enter key>

Output: The current date will be displayed and will ask for new date.

```
CA: Command Prompt - date
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

C:\Users\India>date
The current date is: 12-04-2024
Enter the new date: (dd-mm-yy) _
```

- Del/Erase

- This command is used to delete one or more files. This command is the same as the erase command. Deleted files will not be retrieved.

Syntax : del <file name> <press enter key>

Example: del try.txt <press enter key>

- Dir

- This command is used to display files and folders.

Syntax: dir <press enter key>



Notes

Operating System

```
CA: Command Prompt
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

C:\Users\India>dir
Volume in drive C is SSD-05
Volume Serial Number is 4492-191E

Directory of C:\Users\India

10-04-2024  22:51    <DIR>        .
10-04-2024  22:51    <DIR>        ..
18-05-2021  15:38    <DIR>        .cura
26-06-2022  23:21    <DIR>        .ms-ad
22-11-2021  09:38    <DIR>        .openshot_qt
27-09-2020  16:44    <DIR>        .swt
02-08-2021  09:09    <DIR>        .vscode
18-07-2020  14:58    <DIR>        3D Objects
27-09-2020  16:39             15 advanced_ip_scanner_Aliases.bin
27-09-2020  16:39             15 advanced_ip_scanner_Comments.bin
27-09-2020  16:39            446 advanced_ip_scanner_MAC.bin
18-07-2020  14:58    <DIR>        Contacts
08-10-2020  08:55    <DIR>        Documents
12-04-2024  12:22    <DIR>        Downloads
18-07-2020  14:58    <DIR>        Favorites
18-07-2020  14:58    <DIR>        Links
19-11-2022  10:08    <DIR>        Music
19-10-2023  09:02    <DIR>        OneDrive
18-07-2020  14:58    <DIR>        Saved Games
23-01-2023  13:31    <DIR>        Searches
26-06-2021  13:49    <DIR>        Videos
               3 File(s)          476 bytes
              18 Dir(s) 34,702,270,464 bytes free

C:\Users\India>
```

- Exit
 - This command exits the command line interface, terminating the current session.

Syntax: exit <press enter key>

```
CA: Command Prompt
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

C:\Users\India>exit
```

- ipconfig
 - Displays all current TCP/IP network configuration values. It displays Internet Protocol version 4 (IPv4) and IPv6 addresses.

Syntax: Ipconfig <press enter key>

(To display the full TCP/IP configuration)



Notes

```

C:\Users\India>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::e750:f510:fd49:48ec%15
    IPv4 Address. . . . . : 192.168.0.104
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\India>
```

- move
 - The move command is used to relocate files, folders or directories.
Syntax: Move <source> <destination> <Press enter key>
Example: move linux.ppt c
- print
 - This command sends a text file to a printer. A file can print in the background if you send it to a printer connected to a serial or parallel port on the local computer.



Notes

Operating System

Syntax:

Example: print /d:lpt2 report.txt

- ping:
 - This command is the primary TCP/IP command used to troubleshoot network connectivity, reachability, and name resolution.

Syntax: ping <press enter key>
- ren
 - This command is used to rename a file or directories.

Syntax: ren <filename> <new name> <press enter key>

Example: ren working.txt working2023.txt
- rmdir or rd
 - This command is used to delete a directory. Deleted directory will not be recovered.

Syntax: rmdir <directory name> <press enter key>

Example: rmdir root
- systeminfo
 - This command displays detailed configuration information about the computer and its operating system.

Syntax: systeminfo <press enter key>

CA: Command Prompt

```
C:\Users\India>systeminfo

Host Name:                DESKTOP-CNAQKOC
OS Name:                  Microsoft Windows 10 Home Single Language
OS Version:               10.0.19045 N/A Build 19045
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         India
Registered Organization:
Product ID:                00327-35061-17693-AAOEM
Original Install Date:     18-07-2020, 14:55:19
System Boot Time:         10-04-2024, 22:50:29
System Manufacturer:      Dell Inc.
System Model:              Vostro 15-3568
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 78 Stepping
BIOS Version:              Dell Inc. 2.6.0, 15-05-2018
Windows Directory:        C:\Windows
System Directory:          C:\Windows\system32
```



- time
 - This command displays or changes system time. It is used without parameters

Syntax: time <press enter key>

```
CA: Command Prompt - time

C:\Users\India>time
The current time is: 13:41:28.99
Enter the new time:
```

- tree
 - This command displays the directory structure of a path or the disk in the form of a graphical tree.

Syntax: tree <press enter key>

```
CA: Command Prompt

C:\Users\India>tree
Folder PATH listing for volume SSD-05
Volume serial number is 4492-191E
C:..
|_ .cura
|   |_ 15.04.6
|_ .ms-ad
|_ .openshot_qt
|   |_ assets
|   |_ blender
|   |_ cache
|   |_ presets
|   |_ preview-cache
|   |_ profiles
|   |_ recovery
|   |_ thumbnail
|   |_ title
|   |_ transitions
|_ .swt
|   |_ lib
|       |_ win32
|       |_ x86
```



INTEXT QUESTIONS 1.5

Multiple Choice Questions:

1. Which command is used to relocate a file or folder to another location.
 - (a) copy
 - (b) move
 - (c) Ren
 - (d) locate



Notes

2. The command to change or display date is
 - (a) Datetime
 - (b) Date
 - (c) Chdate
 - (d) None of the above
3. The command to display the configuration of a computer is
 - (a) System
 - (b) Config
 - (c) Systeminfo
 - (d) All of the above
4. Command is used to check network connectivity
 - (a) Ping
 - (b) Netconn
 - (c) Network
 - (d) None of the above
5. command is used to delete a directory
 - (a) Rd
 - (b) Rem
 - (c) Del
 - (d) Del dir
6. command is used to change time.
 - (a) Chtime
 - (b) Changetime
 - (c) Time
 - (d) All of the above
7. Which of the following commands is used to summarize the disk usage?
 - (a) chkdsk
 - (b) usg
 - (c) fdisk
 - (d) disk

1.6 FEATURES OF LINUX OPERATING SYSTEM

Linux is a free and open-source(freely available code) operating system (OS) that evolved from a kernel created by Linus Torvalds in 1991. It is based on the Unix operating system and has become one of the most popular operating systems. Linux is supported on every platform making it the most widely supported operating system. Various versions of Linux are already available on the internet for use. Linux is an interface between computer/server hardware, and the programs which run on it. Kernel is the core of the Operating system. Some important features of Linux operating system are:

- **Multiuser Capacity:** The users can share the system resources such as RAM, hard drive, and application program at same time. But they have to use it in different terminals.



- **Multitasking:** Multiple applications can run simultaneously by effectively dividing the CPU time. Examples of multitasking operating system are UNIX, IBM's OS/390, Windows Vista, Windows XP, and Windows 7, 8, 9, and 10.
- **Security:** It secures data in three ways:
 - Authentication:** By assigning a password and login ID
 - Authorization:** By assigning read, write and execute permissions
 - Encryption:** It converts the files into an unreadable format.
- **Graphical User Interface (GUI):** It is a command line that can be converted into a Graphical User Interface by installing some packages. The most popular method for getting a GUI in a Linux system is logging into a Ubuntu server and installing its desktop environment.
- **File System:** It provides a hierarchical system to arrange files and directories.
- **Application Support:** It consists of a software repository for users to download and install several applications, which gives the user a vast range of applications to download the application of their choice.
- **Open Source:** This Linux code is freely available to all, and it's a community-based development project which allows the user to modify, analyze the code and redistribute the codes.
- **Shell:** The Shell command-line interpreter on Linux acts as a line between the user and the kernel, which runs the program known as commands. It is efficient and takes less time and space while executing the tasks.
- **Portability:** Portability doesn't mean the smaller size. Here, it means that Linux supports different kinds of hardware, which means that the software can perform similarly on different types of hardware/machines.
- **Performance:** Linux operating systems are known for their performance, offering high stability, efficiency, and scalability, making them widely used in various applications.
- **Lightweight Infrastructure:** Linux can be configured into a lightweight infrastructure by using minimal resources, streamlined services, and optimized kernel settings, ideal for resource-constrained environments or embedded systems.
- **Live USB:** Live USB of a Linux operating system allows booting and running the OS from external media without installation, useful for testing, recovery or portable computing.



Notes

Operating System

- **Compatibility with cloud computing:** Linux is highly compatible with cloud computing platforms, offering a wide range of distributions and tools for cloud deployment, scaling, and management.
- **Frequent New Updates:** Linux operating systems receive frequent updates, including security patches, bug fixes, and new features, ensuring ongoing improvements and staying up-to-date with evolving technology.

Many software vendors released their own Linux OS(kernel, application) for distribution.

Some of the Linux Distribution (Operating System) are:

- Debian
- Red Hat
- Ubuntu
- SUSE
- Fedora



INTEXT QUESTIONS 1.6

Multiple Choice Questions:

1. Which is the core of the operating system
 - (a) Shell
 - (b) Script
 - (c) Command
 - (d) Kernel
2. Which OS is based on Linux
 - (a) Debian
 - (b) Ubuntu
 - (c) Red Hat
 - (d) All of the above
3. Which of the following is not true about Linux?
 - (a) Linux is not available to everyone
 - (b) Linux is developed by collaborators from around the World
 - (c) Linux is secure OS
 - (d) Frequent updates are available



4. Software which is developed and modified freely is called
 - (a) Application Software
 - (b) Open Source Software
 - (c) System Software
 - (d) None of the above
5. Features of Linux Operating system
 - (a) It is multi user OS
 - (b) It is a multitasking OS
 - (c) It is highly secure OS
 - (d) All of the above

1.7 BASIC LINUX COMMANDS

The shell provides a way to communicate with the operating system. The shell is the Linux command line interpreter. It is simply an application running on top of the kernel and provides a powerful interface to Linux operating system. They are the basic tools used to interact with Linux on an individual level. Each shell has varying capabilities and features and the user should choose the shell best suited for their needs.

Linux commands are used to perform a variety of tasks, including displaying information about files and directories.

To open the Linux terminal, press “CTRL + ALT + T” keys together or type terminal in search bar present on taskbar.

Note: When you first login, your current working directory is your home directory.

- **cd** (*change directory*)
 - This command allows you to change the directory.
Syntax: cd [destination] <press enter key>
Example: cd hardware
- **Cp**(*Copy*)
 - This command copies a file or a directory.
Syntax: cp <source file> <destination><press enter key>
Example: cp text.doc merge.txt
- **Cat** :
 - This command shows the content of a file. It copies content from one file to another, concatenates the contents of multiple files etc.
Syntax: cat <file name> <press enter key>
Example: cat test.txt <press enter key>



Notes

Operating System

- **chmod** (*Change mode*)
 - This command is used to change the access mode of a file or a directory. It can be used to modify the permission so that it can grant or restrict access to directories and files.

Syntax: `chmod <press enter key>`

- **Date:**
 - This command displays the system date and it allows in setting the date and time of system.

Syntax: `date <press enter key>`

```
$ date
date
Fri Apr 12 14:13:47 IST 2024
```

- **Free:**
 - This command displays free and used memory in the system.

Syntax: `free <press enter key>`

```
$ free
total        used        free      shared  buff/cache   available
Mem:    131806800    1917188    124573472        3572     5316140    128664624
Swap:    4194300           0         4194300
$
```

- **Ls** (*list*)
 - This command lists the contents of a directory. There are many options that can be added to ls command.

Syntax: `ls <press enter key>`

```
$ ls
fontlist-v330.json shiv ss.txt try
$
```

- **Help:**
 - The help command is the simplest way to get information regarding a built-in shell command. It helps you fetch information from the shell's internal documentation.

Syntax: `help <name of the command> <press enter key>`

Example : `help cd <press enter key>`



- **rmdir(remove)**
 - This command removes or deletes a directory that is empty. Directory once deleted will not be recovered.
Syntax: rmdir Syntax: <press enter key>
Example:rmdir hardware
- **rm(remove)**
 - This command removes or deletes a directory that is not empty and has files and sub directories. Directory once deleted will not be recovered.
Syntax: rm hardware <press enter key>
Example:rm hardware
- **mv(Move)**
 - This command moves or rename a file or a directory or moving a file or directory to another location.
Syntax: mv <source> <destination> <press enter key>
Example:mv practice.txt praclinux.txt
(This command is used to rename practice.txt to praclinux.txt)
- **mkdir (make directory)**
 - This command creates a directory.
Syntax: mkdir <name of directory> <press enter key>
Example: mkdir hardware <press enter key>
- **Pwd (Print working directory)**
 - This command prints the current working directory.
Syntax : pwd <press enter key>
- **Passwd :**
 - This command is used to change user passwords, but it offers additional functionalities such as updating password, unlocking accounts etc.
Syntax: passwd <press enter key>
Example: passwd <press enter key>
(This command allows you to change password of current working directory)



Notes

```
$ passwd
Changing password for webmaster.
Current password: |
```

- Ping host:
 - This command is a powerful tool that allows users to check the status of their internet connection and diagnose network-related issues.
Syntax: ping [options] host_or_IP_address
Example: ping www.google.com
- Touch:
 - Touch is a common Linux command to make an empty file or modify the file timestamps.
Syntax: touch <file name> <press enter key>
Example : touch try.txt <press enter key>
- Whoami:
 - This command is used to display who you are logged in as
Syntax: whoami <press enter key>
hj



INTEXT QUESTIONS 1.7

Multiple choice Questions:

1. Which command is given to rename a file or directory in Linux?
(a) Mv (b) Cp
(c) Clear (d) Lpr
2. Which command is used to delete folders?
(a) Del (b) Rmdir
(c) Rd (d) Remove
3. Which command do you use to clear the prompt screen?
(a) Cd (b) Clear
(c) Cls (d) All of the above



4. What does the cmd command do?
 - (a) Run a command
 - (b) Start a new command shell
 - (c) Close the command shell
 - (d) Clear the screen
5. Which command is used to get help about a command in Linux?
 - (a) info
 - (b) cat
 - (c) man
 - (d) help
6. Which of the following commands is used to create file in Linux?
 - (a) touch
 - (b) cat
 - (c) echo
 - (d) All of the above
7. What command can be used to get information about yourself?
 - (a) Which
 - (b) pwd
 - (c) i/4
 - (d) whoami
8. Which command is used to change the file permission in Linux?
 - (a) Chown
 - (b) Chmod
 - (c) Fdisk
 - (d) None
9. Which of the following commands is used to change the working directory?
 - (a) cd
 - (b) chdir
 - (c) changedir
 - (d) cdir
10. Which of the following commands is used to list contents of directories?
 - (a) lp
 - (b) dir
 - (c) ls
 - (d) tar



WHAT HAVE YOU LEARNT

- An operating system is the first program loaded when a computer boots. It acts as an essential interface between the user and computer hardware, allowing users to interact with the system through interfaces like **Command-Line Interface (CLI)** and **Graphical User Interface (GUI)**.

Types of Operating System Structures: Operating systems can have different structures, including: **Simple Structure, Monolithic Structure, Layered Approach, Microkernels, Modules, Hybrid Systems**



Notes

- The OS performs several key functions, such as: **Process Management, Memory Management, I/O Device Management, File Management, Network Management, Security and Protection, User Interface, Backup and Recovery**
- **Microsoft Windows 10** is a widely used OS that introduced new features such as the **Start Menu, Microsoft Edge**, and improved synchronization between PCs and mobile devices.
- **Linux Operating System** is a free, open-source OS known for its **multiuser** and **multitasking** capabilities, security, portability, and hierarchical file system. It also includes the **Shell**, a command-line interpreter.
- Both **Microsoft Command Prompt** and **Linux Shell** serve as command-line interfaces, allowing users to execute commands and manage the system through text-based input.



TERMINAL QUESTIONS

1. Define Operating system.
2. List different services offered by the operating system.
3. Explain the following terms in brief.
 - (a) Monolithic
 - (b) Microkernel
4. Explain the layered approach of an operating system.
5. Explain the term Process.
6. Write the difference between multiuser and multitasking feature of Linux.
7. Justify whether following statements are true or false
 - (a) The user application interacts directly with O.S.
 - (b) Shell is part of operating System
8. Explain the usage of chmod command in Linux.
9. What information is presented when the following commands in the windows command line are entered?
 - (a) date
 - (b) whoami
 - (c) passwd
10. What do you understand about open source software? Give some examples.



ANSWERS TO INTEXT QUESTIONS



Notes

1.1

1. (a) 2. (c) 3. (c) 4. (d) 5. (d) 6. (c)

1.2

1. (b) 2. (c) 3. (c) 4. (a) 5. (d)

1.3

1. (b) 2. (c) 3. (a) 4. (d)

1.4

1. (b) 2. (d) 3. (a) 4. (b) 5. (a) 6. (a)

1.5

1. (b) 2. (b) 3. (c) 4. (a) 5. (a) 6. (c)
7. (a)

1.6

1. (d) 2. (d) 3. (c) 4. (b) 5. (d)

1.7

1. (a) 2. (b) 3. (c) 4. (b) 5. (d) 6. (a)
7. (d) 8. (b) 9. (a) 10. (c)

Key Learning Outcomes

After learning this lesson, the learner will be able to:

- Describe the main functions and structures of an operating system.
- Describe features and file systems of Windows and Linux operating system.
- Demonstrate basic command-line operations in Windows and Linux operating system.



2

OVERVIEW OF WEB DEVELOPMENT

This chapter introduces the fundamental concepts, tools and technologies related to web development. Using these fundamentals gives you an in-depth understanding about how modern sites and online-based platforms are implemented. Web development is an increasingly fascinating and critically important area today. In plain terms, the development of sites and web-based applications on which internet operation bases can be termed web development.



OBJECTIVES

After reading this lesson, you will be able to learn:

- describe one-tier, two-tier, and three-tier architectures;
- differentiate between client-side and server-side programming;
- explain HTML, JavaScript, and CSS, and demonstrate basic codes;
- create a simple login page using PHP;
- describe database connectivity and characteristics of a DBMS;
- write and execute basic SQL queries using MySQL;
- explain identification and prevention of SQL injection vulnerabilities.

2.1 WEB DEVELOPMENT

Web development is the process of creating websites and web applications that run on the internet. It involves building the parts of a website that users see and interact

with, like the design and layout (front-end), as well as the behind-the-scenes systems that handle data and functionality (back-end). Using tools like HTML, CSS, JavaScript, and programming languages such as Python or PHP, web developers create everything from simple blogs to complex online platforms. Modern web development also focuses on making websites easy to use, accessible to everyone, and compatible with different devices, ensuring a smooth experience for users.



Notes

2.2 WEB APPLICATION ARCHITECTURES

Web application architectures define how the components of a web application are organized and interact with each other. These architectures can be classified into one-tier, two-tier, and three-tier systems based on how data and functionality are distributed:

1. **One-Tier Architecture (Single Tier):** In this architecture the user interface, business logic, and data storage exists on a single system. For example, a desktop application where all the data and processing happen on your computer. It is simple to implement but not suitable for complex applications or many users.
2. **Two-Tier Architecture:** The application is divided into two parts: the client and the server. The client (e.g., a web browser or app) handles the user interface, while the server manages the database and processes data. For example, a simple website where your browser requests information from a server. This architecture works well for small applications but can struggle with scalability as users increase.
3. **Three-Tier Architecture:** In this design, the application is divided into three layers:
 - **Presentation Layer:** The front-end where users interact (e.g., a website or app interface).
 - **Application Layer:** The middle layer (business logic) processes data and handles requests from the user interface.
 - **Database Layer:** The back-end where data is stored and retrieved.

This architecture is more scalable, secure, and easier to maintain, making it ideal for larger and more complex applications, such as e-commerce platforms as shown in Fig. 2.1.

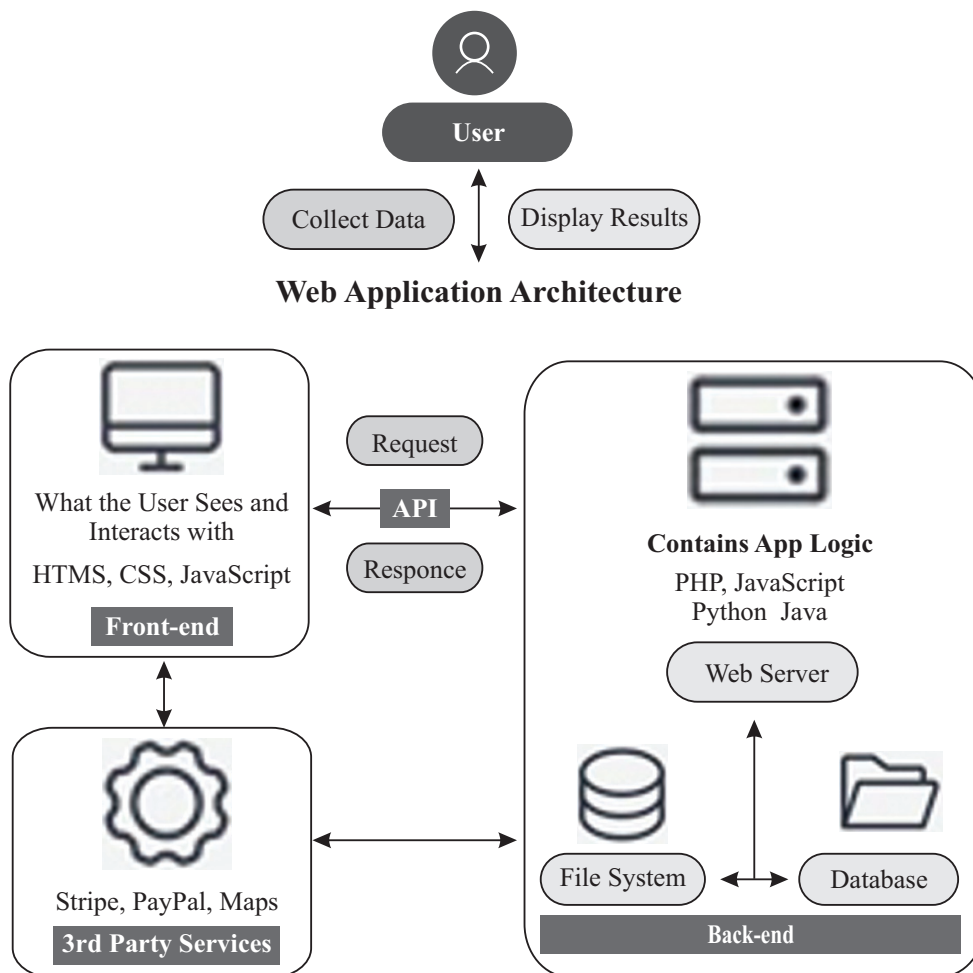


Fig. 2.1: Web Application Architecture

2.3 CLIENT-SIDE AND SERVER-SIDE PROGRAMMING

Client-side programming and server-side programming are two key parts of web development that work together to make websites and web applications function properly.

2.3.1 Client-Side Programming

It is the programming executed on the user's device (like a computer or smartphone) in the web browser. It is responsible for everything you see and interact with on a website, such as text, images, buttons, and forms. Technologies like HTML (for structure), CSS (for styling), and JavaScript (for interactivity) are used for client-side programming. For example, when you click a button and see



a pop-up or animation, that's client-side programming in action. It focuses on making the website look good and respond to user actions without needing to contact the server for every interaction.

2.3.2 Server-Side Programming

It is the programming executed on a web server, the powerful computer where the website's data and functionality are stored. Server-side programming handles tasks like storing and retrieving data, processing user requests and managing security. Technologies like PHP, Python, Java, or Node.js are used for server-side programming. For instance, when you log in to a website, the server-side code checks your username and password in the database to verify your identity before granting access.

When you visit a website, the browser (client-side) sends a request to the server (server-side) to fetch data, like a webpage or your account details. The server processes this request, sends the necessary data back, and the client-side code displays it in a user-friendly way.

- **Client-side:** What you see and interact with.
- **Server-side:** What happens behind the scenes to make everything work.

Table 2.1: Difference between Client-Side Programming and Server-Side Programming

Parameters	Client-Side Programming	Server-Side Programming
Location of Execution	Executes on the user's device (browser).	Executes on the server.
Purpose	Handles user interface, interactivity, and presentation.	Manages data processing, storage, and backend logic.
Languages Used	HTML, CSS, JavaScript	PHP, Python, Java, Ruby, Node.js
Data Access	Limited to what is sent by the server.	Accesses and manages databases and server resources.
Security	Less secure as code can be viewed and modified by users.	More secure as code and logic remain on the server.
Examples of Tasks	Form validation, animations, dynamic content updates.	User authentication, database queries, API handling.
Dependency	Relies on the browser for execution.	Requires a server to run.
Performance	Fast for rendering UI but depends on browser performance.	Depends on server capacity and can handle heavier tasks.



Notes

Overview of Web Development

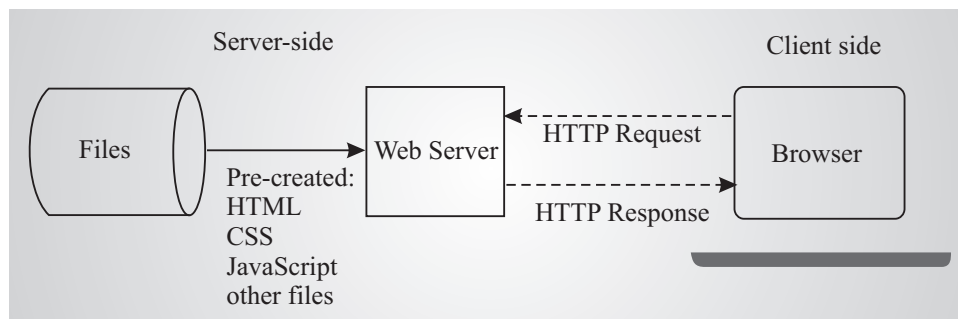


Fig. 2.2: Client and Server Side



INTEXT QUESTIONS 2.1

1. Fill in the blank

- Web development involves building the visible parts of a website and the behind-the-scenes systems that handle data and functionality
- In architecture, the user interface, business logic, and data storage exist on a single system.
- The layer in three-tier architecture is responsible for processing data and handling requests from the user interface.
- is responsible for making the website look good and respond to user actions without needing to contact the server for every interaction.
- Technologies like PHP, Python, and Node.js are commonly used in programming to handle tasks like processing user requests and managing security.

2.4 FRONT-END DEVELOPMENT

In its simplest terms, web development can be split into two categories: front-end and back-end development. Front-end development pertains to creating the visual and interactive elements users engage with, such as layouts, buttons, and forms. This is achieved using languages like HTML (HyperText Markup Language) for structure, CSS (Cascading Style Sheets) for styling, and JavaScript for interactivity.

Front-end development focuses on building the user interface of a website or web application. It ensures that users can see and interact with the content effectively.



The three foundational technologies used in front-end development are:

2.4.1 HTML (HyperText Markup Language)

HTML is the backbone of any website. It defines the structure and content of web pages using tags. For example:

- `<h1>` to `<h6>` tags are used for headings.
- `<p>` is used for paragraphs.
- `<img>` embeds images, and `<a>` creates links.

HTML organizes the information that users see, like text, images, and links, into a readable and structured format.

Example

```
<!DOCTYPE html>
<html>
<head>
<title>My First Page</title>
</head>
<body>
<h1>Welcome to My Website</h1>
<p>This is a paragraph.</p>
<a href="https://example.com">Visit Example</a>
</body>
</html>
```

2.4.2 CSS (Cascading Style Sheets)

CSS is used to style the HTML content, controlling how it looks. It allows developers to set colors, fonts, layouts, and spacing, creating visually appealing web pages.

To make all headings blue, CSS might include `h1 { color: blue; }`.

CSS also supports responsive design, making websites look good on different devices, like phones and tablets, by using media queries.

**Example**

```
<!DOCTYPE html>

<html>

<head>

<style>

h1 {

color: blue;

text-align: center;

}

p {

font-size: 16px;

line-height: 1.5;

}

</style>

</head>

<body>

<h1>Welcome to My Website</h1>

<p>This is a styled paragraph.</p>

</body>

</html>
```

2.4.3 JavaScript

JavaScript adds interactivity and dynamic functionality to websites. It can update content, validate forms, create animations, and more without requiring a page reload.

Example: A button that displays a pop-up message when clicked can be created using JavaScript. Frameworks and libraries like React, Angular, and Vue.js extend JavaScript to build complex, user-friendly applications.



Example

```
<!DOCTYPE html>
<html>
<head>
<title>JavaScript Example</title>
</head>
<body>
<h1 id="greeting">Hello!</h1>
<button onclick="changeGreeting()">Click Me</button>
<script>
function changeGreeting() {
document.getElementById("greeting").innerHTML = "You clicked the
button!";
}
</script>
</body>
</html>
```

Together, HTML provides the structure, CSS enhances the appearance, and JavaScript adds interactivity, forming the foundation of front-end development. These tools ensure that websites are engaging, functional, and accessible to users.

2.5 BASICS OF BACK-END DEVELOPMENT WITH PHP

Back-end development, centers on server-side functionality: how data is stored, processed, and delivered effectively. It's about using the server-side language, like PHP, Python, or Node.js, and the management of the database, including MySQL or MongoDB. It makes features such as user authentication, data submission, and dynamic content generation work.

Back-end development focuses on the server-side of web applications, handling data processing, database interactions and business logic. PHP (Hypertext Preprocessor) is a popular server-side scripting language widely used for building dynamic and interactive websites.



Notes

Overview of Web Development

PHP code is executed on the server, and the result is sent to the browser. You need a server environment like **XAMPP** or **WAMP** to run PHP locally.

- PHP is essential for creating dynamic web applications.
- It integrates seamlessly with databases, processes forms, and manages server-side logic.
- Understanding its basics, like variables, control structures, and database connectivity, is the first step to mastering back-end development.

2.5.1 PHP Syntax

PHP code is written between `<?php` and `?>` tags.

Example:

```
<?php
    echo "Hello, World!";
?>
```

Output:

Hello, World!

2.5.2 Variables and Data Types

PHP variables are declared using the `$` sign.

Example:

```
<?php
    $name = "John";
    $age = 25;
    echo "Name: $name, Age: $age";
?>
```

Output:

Name: John, Age: 25

2.5.3 Control Structures

PHP supports common control structures like `if`, `else`, and loops.



Example (If-Else):

```
<?php
    $number = 10;
    if ($number > 5) {
        echo "Number is greater than 5";
    } else {
        echo "Number is 5 or less";
    }
?>
```

2.5.4 Form Handling

PHP can process form data sent via POST or GET methods.

HTML Form:

```
<form method="POST" action="process.php">
    <input type="text" name="username" placeholder="Enter your name">
    <input type="submit" value="Submit">
</form>
```

process.php:

```
<?php
    $username = $_POST['username'];
    echo "Hello, $username!";
?>
```

2.5.5 Database Connectivity (MySQL)

PHP works well with MySQL to store and retrieve data.

Example:

```
<?php
    $conn = new mysqli("localhost", "root", "", "testdb");
    if ($conn->connect_error) {
        die("Connection failed: " . $conn->connect_error);
    }
    echo "Connected successfully";
?>
```



Notes



INTEXT QUESTIONS 4.2

1. State whether the following are True or False:

- (a) HTML, CSS, and JavaScript are the three foundational technologies used in front-end development.
- (b) The <p> tag in HTML is used to add images to a webpage.
- (c) CSS is responsible for defining the structure of a webpage.
- (d) JavaScript can create animations and validate forms without reloading the page.
- (e) PHP code is executed on the client-side, and the result is sent to the server.

2. Write short answer on following questions:

- (a) What is the purpose of HTML in front-end development?
- (b) Which CSS property is used to change the text color of headings?
- (c) What does JavaScript add to a website?

2.6 SESSION MANAGEMENT

Session management in PHP is a way to store and manage user-specific information across multiple pages of a web application. It allows data to persist between page requests, such as login details, shopping cart contents, or user preferences.

Sessions are server-side storage mechanisms, ensuring data security and privacy as the information is not directly stored on the client's device (unlike cookies).

How Sessions Work in PHP

- 1. A session is started with the `session_start()` function.
- 2. A unique session ID is generated and stored in a cookie on the client's browser.
- 3. Session variables are stored on the server and associated with the session ID.
- 4. The session data is accessible across multiple pages until the session expires or is destroyed.



Example of Session Management in PHP

Step 1: Starting a Session and Setting Session Variables

login.php

```
<?php
// Start a session
session_start();
// Set session variables
$_SESSION['username'] = "JohnDoe";
$_SESSION['user_role'] = "Admin";
echo "Session variables are set!";
?>
```

Step 2: Accessing Session Variables

dashboard.php

```
<?php
// Start the session
session_start();
// Check if the session variables are set
if (isset($_SESSION['username']) && isset($_SESSION['user_role'])) {
    echo "Welcome, " . $_SESSION['username'] . "!";
    echo " Your role is: " . $_SESSION['user_role'];
} else {
    echo "Session variables are not set.";
}
?>
```

Step 3: Destroying a Session

logout.php

```
<?php
// Start the session
session_start();
```



Notes

```
// Destroy the session  
session_unset(); // Remove all session variables  
session_destroy(); // Destroy the session  
echo "You have been logged out.";  
?>
```

Key Functions for Session Management in PHP

- `session_start()`: Starts or resumes a session.
- `$_SESSION`: Superglobal array used to store session variables.
- `session_unset()`: Clears all session variables.
- `session_destroy()`: Ends the session and deletes the session data.

Session management in PHP is a crucial feature for building user-specific and dynamic web applications. By storing data on the server, it ensures security and allows seamless navigation across multiple pages with persistent information.

2.7 INTRODUCTION TO DATABASE

A **database** is an organized collection of data that allows easy storage, retrieval, and manipulation of information. It provides a systematic way of managing data, ensuring it is stored efficiently, securely, and can be accessed quickly when needed. Databases are essential for applications that require data persistence, such as websites, mobile apps, and enterprise systems.

2.7.1 Organized Storage and Database

Databases store data in a structured format, often using tables, rows, and columns. This organization helps with:

- **Efficient storage**: Data is stored in a way that minimizes redundancy and optimizes space.
- **Easy retrieval**: Data can be quickly searched, sorted, and retrieved using queries.
- **Data integrity**: Constraints and relationships between tables ensure the consistency and accuracy of the data.



2.7.2 MySQL

MySQL is one of the most popular relational database management systems (RDBMS) used to manage databases. It stores data in tables that can be linked through relationships. MySQL uses **Structured Query Language (SQL)** to perform operations like inserting, updating, deleting, and querying data.

Key Features of MySQL

- **Open-source:** Free to use and widely supported.
- **Fast and reliable:** Efficient performance even with large datasets.
- **Supports complex queries:** Allows complex data manipulations with ease.
- **Scalable:** Suitable for small websites to large enterprise applications.

Creating a Table:

```
CREATE TABLE users (  
    id INT AUTO_INCREMENT PRIMARY KEY,  
    name VARCHAR(100),  
    email VARCHAR(100)  
);
```

Inserting Data:

```
INSERT INTO users (name, email) VALUES ('John Doe', 'john@example.com');
```

Retrieving Data:

```
SELECT * FROM users;
```

Databases are essential for organizing and managing data efficiently. MySQL, as a popular RDBMS, allows structured storage and easy retrieval using SQL queries, making it a powerful tool for managing data in web applications and beyond.

2.8 DATABASE CONNECTIVITY WITH SQL AND SQL INJECTION

PHP provides functions to connect to databases and execute SQL queries. MySQL is one of the most commonly used databases with PHP for web applications.

Here's how to connect PHP to a MySQL database and interact with it.



2.8.1 Database Connection in PHP

To connect to a MySQL database using PHP, you can use either **MySQLi** (Improved) or **PDO** (PHP Data Objects). Here's an example using **MySQLi**:

PHP Code for MySQLi Connection

```
<?php
// Database credentials
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "testdb";
// Create connection
$conn = new mysqli($servername, $username, $password, $dbname);
// Check connection
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}
echo "Connected successfully";
?>
```

- **\$servername**: Host where the MySQL server is located (usually "localhost").
- **\$username** and **\$password**: Credentials to access the MySQL server.
- **\$dbname**: The database you want to connect to.

2.8.2 Executing SQL Queries

Once connected, you can perform SQL operations like **SELECT**, **INSERT**, **UPDATE**, and **DELETE**. Below is an example of querying the database:

Select Query Example:

```
<?php
$sql = "SELECT * FROM users"; // SQL query
$result = $conn->query($sql); // Execute the query
if ($result->num_rows > 0) {
```



```
while($row = $result->fetch_assoc()) {  
    echo "id: " . $row["id"]. " - Name: " . $row["name"]. "<br>";  
}  
} else {  
    echo "0 results";  
}  
$conn->close(); // Close the connection  
?>
```

2.8.3 Understanding SQL Injection and Attacks

SQL Injection is a type of security vulnerability where an attacker can manipulate SQL queries by injecting malicious SQL code into them. This can allow attackers to:

- Retrieve, modify, or delete data.
- Execute administrative operations on the database.
- Bypass authentication and gain unauthorized access.

Example of SQL Injection Vulnerability

Consider the following PHP code that takes a user input and directly inserts it into an SQL query without validation:

```
<?php  
  
$username = $_GET['username'];  
$password = $_GET['password'];  
  
// Unsafe SQL query  
  
$sql = "SELECT * FROM users WHERE username='$username' AND  
password='$password'";  
  
$result = $conn->query($sql);  
  
?>
```

An attacker could exploit this by inputting the following values:

- **username:** admin' OR '1'='1
- **password:** anything



Notes

This would result in the following SQL query:

```
SELECT * FROM users WHERE username='admin' OR '1'='1' AND password='anything';
```

This query always returns true ('1'='1'), allowing the attacker to bypass authentication and access the system.

2.8.4 Preventing SQL Injection

To prevent SQL injection, use **prepared statements** with parameterized queries. This ensures that user input is treated as data, not executable code.

Secure Code Example Using MySQLi (Prepared Statements):

```
<?php
// Prepare the SQL statement
$stmt = $conn->prepare("SELECT * FROM users WHERE username=?
AND password=?");
// Bind parameters
$stmt->bind_param("ss", $username, $password); // "ss" means both are
strings
// Set the parameters
$username = $_GET['username'];
$password = $_GET['password'];
// Execute the statement
$stmt->execute();
// Get the result
$result = $stmt->get_result();
if ($result->num_rows > 0) {
echo "Login successful!";
} else {
echo "Invalid credentials";
}
$stmt->close(); // Close the prepared statement
$conn->close(); // Close the connection
?>
```

Overview of Web Development

- **Prepared statements:** Ensure that user input is not directly included in SQL queries.
- **Bind parameters:** Specify the data type of the parameters (e.g., ss for two strings).
- **Execute and fetch data:** Run the query in a secure way.

Database Connectivity in PHP allows interaction with databases using libraries like **MySQLi** or **PDO**. **SQL Injection** is a serious security risk where attackers manipulate SQL queries to execute harmful commands.

To prevent SQL injection, always use **prepared statements** and **parameterized queries**, ensuring user input is handled safely.



INTEXT QUESTIONS 2.3

1. Fill in the blank

- In PHP, a session is started using the function.
- The superglobal array is used to store session variables in PHP.
- To destroy a session and clear all session data, use the and functions.
- A unique session ID is stored in a on the client's browser.
- Session management in PHP stores data on the, ensuring security and privacy.



WHAT YOU HAVE LEARNT

- Web development involves creating websites and web applications using tools like HTML, CSS, JavaScript, and programming languages such as Python or PHP.
- Web application architectures are categorized as one-tier, two-tier and three-tier systems.
- Client-side programming runs on the user's browser and is responsible for the design, styling, and interactivity of a website. Technologies like HTML, CSS, and JavaScript are used to create an engaging user experience.



Notes



Notes

Overview of Web Development

- Server-side programming runs on a web server and handles data processing, user requests, and security. Languages like PHP and Python are commonly used for this purpose.
- Client-server interaction occurs when the client sends a request to the server, which processes it and sends back the necessary data. The client-side then displays the data in an interactive and user-friendly manner.
- Front-end development involves creating the visual and interactive elements of a website that users see and interact with.
- Back-end development focuses on server-side functionality, handling data storage, processing, and retrieval.
- A database is an organized collection of data that enables easy storage, retrieval, and manipulation. It ensures efficient storage, quick access, and maintains data integrity through structured organization using tables, rows, and columns.
- MySQL is a widely used relational database management system (RDBMS) that stores data in tables and supports SQL for performing operations like inserting, updating, and querying data.



TERMINAL QUESTIONS

1. What are the three types of web application architectures, and how do they differ?
2. Which technologies are commonly used for client-side programming?
3. What is the role of server-side programming in web development?
4. How do you establish a connection to a MySQL database using PHP? Provide an example using MySQLi.
5. What is the purpose of the CREATE TABLE SQL statement in MySQL, and how would you create a table for storing user data with fields for id, name, and email?
6. What SQL command would you use to retrieve all records from the users table in MySQL?
7. How can you handle SQL injection vulnerabilities when interacting with a MySQL database in PHP?
8. Write an SQL query to update the email of a user in the users table based on their id.



ANSWERS TO INTEXT QUESTIONS



Notes

2.1

- (a) front-end, back-end (b) One-Tier
(c) Application (d) Client-side programming
(e) Server-side

2.2

- (a) True (b) False (c) False (d) True (e) False
- (a) HTML defines the structure and content of web pages using tags.
(b) The colour property.
(c) JavaScript adds interactivity and dynamic functionality.

2.3

- (a) session_start() (b) \$_SESSION
(c) session_unset(), session_destroy() (d) cookie
(e) server

Key Learning Outcomes

- Explain the fundamentals of web development and its core tools.
- Differentiate between client-side and server-side programming, including their roles and technologies.
- Describe database connectivity and characteristics of a DBMS



COMPUTER NETWORKS

In the previous lesson, you learned an overview of database management systems. Today, people use computers in so many places like homes, workplaces, and marketplaces. Modern technology allows computers located in distant places to be interconnected, shared, and interacted with. This is achieved through a computer network, which is a collection of devices connected with communication links. Distributed processing is another characteristic of computer networks, whereby a task is divided and distributed to be carried out by a number of computers instead of depending on one single computer to accomplish the entire work.

This lesson will introduce you to the key concepts of computer networking and data communication. You will learn about the components of networks, such as nodes and communication channels, and explore different types of networks like LAN, WAN, and the internet.



OBJECTIVES

After reading this lesson, you will be able to:

- describe components of computer networks;
- distinguish among Internet, Intranet and Extranet in respect of parameters;
- explain various Transmission modes, Ethernet, and Classification of Transmission Media;
- list and explain various networking devices like Repeaters, Hubs, Bridges, Switches, and routers;
- explain OSI reference model, TCP/IP Model, function of layers;

- explain Port Numbers, Common TCP& UDP Ports;
- explain IPv4 Addressing and Subnet Masking;
- explain RIR, IANA;
- list and explain TCP/IP troubleshooting utilities.



3.1 TYPES OF COMPUTER NETWORKS

In computer networks, LAN, WAN, and MAN refer to different types of networks with size, range, and purpose variance. Such networks are the heart of communication in modern society since they facilitate the transfer of data and the sharing of resources within diverse geographical areas. Each type of network is aimed at fulfilling a specific requirement on the part of the user as per location, scale, or usage.

LAN (Local Area Network)

LAN is a network that connects devices in a small, localized area like home, office, or campus. It facilitates rapid communication among devices and helps users to share files, printers, etc., much more conveniently. Typically, LANs run on technologies using either wires like an Ethernet cable or wirelessly by using technologies such as Wi-Fi. LAN is the best solution for small and medium-sized organizations or even home-based operations because devices are nearby each other; therefore, they are economical and have faster data transfer.

WAN (Wide Area Network)

It covers a geographically larger area than a LAN. It will connect several cities, countries or even continents together. The network of several large LANs using WAN will keep businesses and organizations over a long-distance. Internet itself, the largest network, connects hundreds of thousands and millions of individual networks together through WANs. WANs tend to rely on telecommunication infrastructure, such as leased lines, satellite links, or fiber optics, to carry data long distances, meaning a wider communication range but usually at a higher cost.

MAN (Metropolitan Area Network)

A MAN falls between the scope of a LAN and a WAN, usually spanning a metropolitan area such as a city or a large campus. It links multiple LANs within a defined geographical area that can enable fast communication and sharing of resources. MANs are mostly utilized by cities, large universities, or companies that have many buildings scattered throughout a city. They are constructed using high-



capacity transmission technologies that will enable reliable and efficient data transfer across a larger area than a LAN but without the extensive distances of a WAN.

LAN, WAN, and MAN collectively constitute varying dimensions on which computers can function on scales that need specific provision in terms of connectivity, pace, and provision for sharing by location.

3.2 INTERNET, INTRANET, AND EXTRANET

Internet is a network of networks that connects millions of computers from across the world. The Internet consists of people who use and develop the network and the resources that can be used by any user on the network. No one owns this network but it can be used by anyone.

Intranet is an internal private network built within an organization using Internet. Only employees of that organization can access and share resources in its network as the owner of the network is that very organization. For example, the intranet of NIOS will allow only its employees to access the data and resources.

Extranet is a type of network that allows users from outside to access the intranet of an organization. Its purpose to share information between the members of the organization and some authenticated external users. For example, NIOS has an internal network (called Intranet) that can be accessed only by employees of NIOS. However, access can be given to one of the faculties at a study centre (who is not the regular employee of NIOS) to enter practical marks of students enrolled with that centre, then it becomes an extranet.

3.3 OVERVIEW OF TRANSMISSION MEDIA

Transmission medium is a communication channel that carries the message from sender to receiver. Here electromagnetic (EM) signals can be used to complete data transmission. In data communication, the transmission medium acts as a physical channel between the sender and the receiver.

The transmission media can be classified as **Guided Media** and **Unguided Media**

3.3.1 Guided Media

A physical link between the transmitter and the receiver is provided by **guided media**. There are major 3 types of Guided media:

1. **Twisted Pair:** A twisted pair of wires is made up of two copper wires that are insulated and usually have a thickness of one millimeter. The cables are coiled into a helical configuration. These are often used in telephones lines, LAN etc.



2. **Coaxial Cable:** A rigid copper wire serves as the core of a coaxial cable, which is encased in an insulating substance. Coaxial cable has the advantage of higher data speeds over longer distances. These are mostly used in distribution of cable television signals.
3. **Optical Fiber:** When it comes to data processing and security, this medium is superior. Optical fiber has a light-conductive glass or plastic inner core. It is a transparent, flexible fiber that has been pulled extremely thin and is constructed of silica glass. Because optical fiber is flexible and can be bundled into cables, it may be used as a medium for computer networking and telecommunication. Compared to electrical wires, light travels through the fiber with minimal attenuation, making it particularly beneficial for long-distance talks. These are relatively high compared to other types of cables

3.3.2 Unguided Media

Unguided media transfer electromagnetic (EM) waves without using any physical link. Major types of unguided media are as follows:

1. **Microwave Transmission:** The waves in a **microwave** transmission move straight. These are unidirectional and the transmitting and receiving antennas need to be precisely aligned with one another in order to achieve a significantly greater signal to noise ratio.
2. **Radio Waves:** In order to avoid the need for the transmitter and receiver to be precisely positioned physically, radio waves can be sent in all directions from the source i.e. in an omnidirectional manner. FM Radio, Television are some applications where Radio waves are used.
3. **Infrared Waves:** Short-range communication makes extensive use of **infrared waves**. Infrared communication is carried out by TV, VCR, and stereo remote controls.
4. **Satellite Communication:** **Satellite communication** uses satellites to transmit signals between sender and receiver. In this operation, the signal, which is essentially a beam of modulated microwaves, is transmitted to the satellite. The satellite then amplifies the signal and transmits it to the receiver's antenna on Earth's surface. So, all signal transfer occurs in space. Thus, this sort of communication is referred to as space communication.
5. **Bluetooth:** Bluetooth is a PAN technology. Its radio features include low power, limited range, and medium transmission speed. It successfully exchanges data across small distances.



Notes

6. **Wi-Fi:** WIFI stands for Wireless Fidelity, a wireless technology standard for wireless Internet access. Wi-Fi relies on a high energy input to provide a 100-meter range and substantially faster transmission rates. This speed makes Wi-Fi substantially quicker than Bluetooth and comparable to a high-speed modem. Wi-Fi is better than Bluetooth for transferring large files and getting faster internet access.

3.4 OVERVIEW OF NETWORK DEVICES

Computer network devices are also known as communication devices and they constitute a data communication network. These devices are Ethernet Card, Router, Hub, Switches, Gateways, and Bridges etc. In an Ethernet or WAN network, the data communication cannot be performed without these devices.

Descriptions of these devices are mentioned below:

3.4.1 RJ45 Connector

RJ45 is a type of connector commonly used for Ethernet networking. It looks similar to a telephone jack, but is slightly wider. Since Ethernet cables have a RJ45 connector on each end, Ethernet cables are sometimes also called RJ45 cables. The 'RJ' in RJ45 stands for 'registered jack' since it is a standardized network interface. The '45' simply refers to the number of the interface standard.

3.4.2 Ethernet Card

Ethernet cards are one type of network adaptor which support the Ethernet standard for high-speed network connections over wires. Ethernet cards are also known as network interface cards (NICs). It is the most extensively used LAN technology.



Fig. 3.1: Ethernet Card

3.4.3 Router

Routers are network devices that expand or partition networks by routing packets from one logical network to another. These transmit data packets across

networks. A router connects to at least two networks, usually two LANs or WANs, or a LAN and its ISP's network. It manages traffic between networks by delivering data packets to their intended IP addresses and also allows several devices to share the same Internet connection.



Notes



Fig. 3.2: Router

3.4.4 Hub

A hub is the networking device which links multiple networks and computers together. Unlike a network switch or router, it does not include routing tables or intelligence for determining where to transmit information and broadcasts all network data across each link.

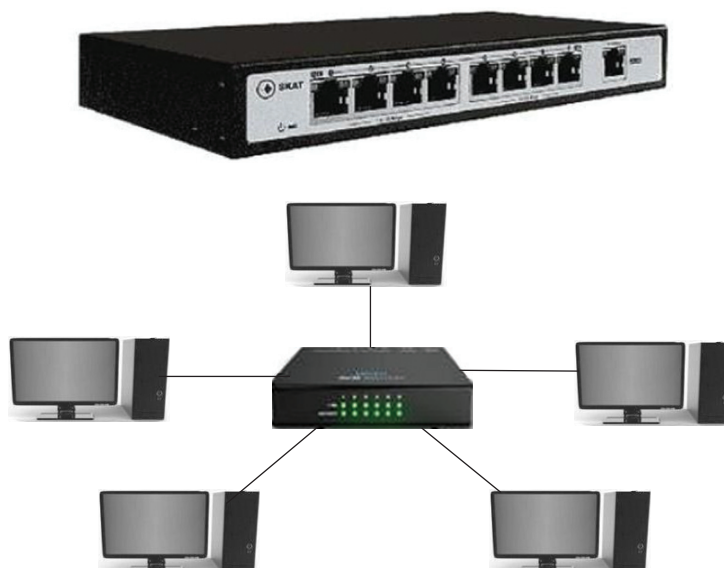


Fig. 3.3: Hub and its Connectivity in Network



Notes

3.4.5 Switch

Switches are a unique form of hub that adds intelligence to simple physical layer repeater hubs. A switch performs essentially the same function as a hub, but more efficiently. By seeing the traffic that passes through it, it may “learn” where specific addresses are. A switch must be able to read the MAC address from each frame it receives. This information enables switches to route incoming data frames only to the specified computer.



Fig. 3.4: Switch

3.4.6 Gateway

Gateways are the network devices which connect two networks with different transmission protocols. They translate the message from one protocol to other. A network gateway can be implemented entirely in software, entirely in hardware, or as a hybrid of the two.



Fig. 3.5: Gateway

3.4.7 Bridges

A bridge is a type of network device that unites several smaller networks into one larger network. It provides connectivity to other networks of computers that use the same protocol. A bridge can be used to connect several LANs (Local Area Networks) together to create a larger LAN.

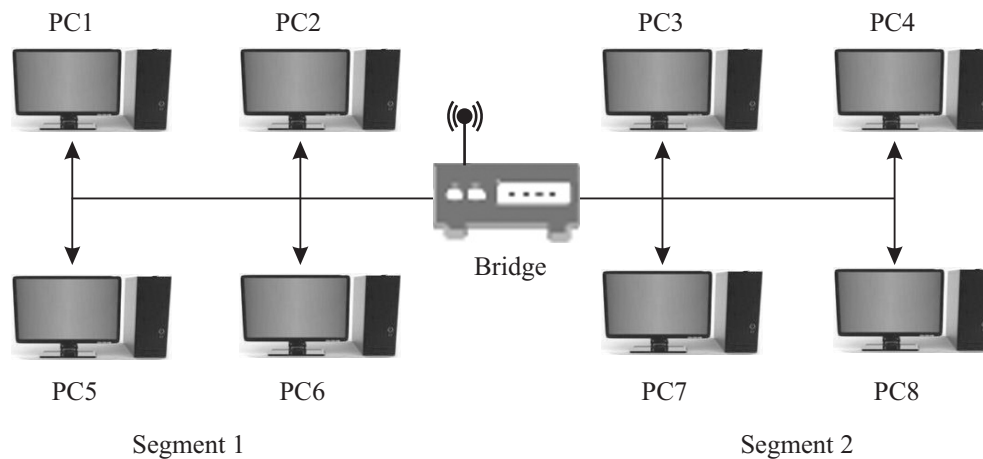


Fig. 3.6: Bridge in the Network

Notes



3.5 OSI REFERENCE MODEL

Computer systems use the **Open System Interconnection**, or OSI, reference model to communicate with one another over a network. The International Organization for Standardization (ISO) created the OSI model in 1984, and it is currently used as an architectural paradigm for communications between computers. It is divided into seven layers that work together to carry out specialized network functions, allowing for a more systematic approach to networking. Each layer is assigned a particular task.

Characteristics of OSI Model

The OSI model is divided into two layers: upper layers and lower layers.

- **The upper layer:** The application-related problems that are mostly handled by the higher layer of the OSI model are limited to software implementation. The layer nearest to the user is the application layer. Software applications are interacted with by both the application layer and the end user. The layer just above another layer is referred to as an upper layer.
- **The lower layer:** The OSI model's lowest layer handles data transport-related concerns. Hardware and software are used to implement the data connection layer and the physical layer. In the OSI model, the physical layer is the lowest layer and the one nearest to the physical media. Information placement on the physical medium is mostly the responsibility of the physical layer.



Notes

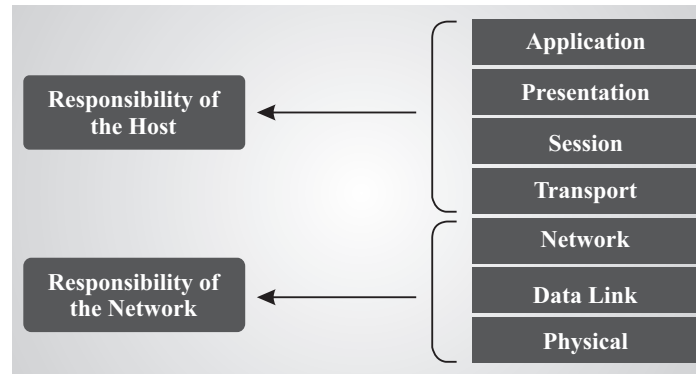


Fig. 3.7: The OSI Reference Model

Layers of OSI Model

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

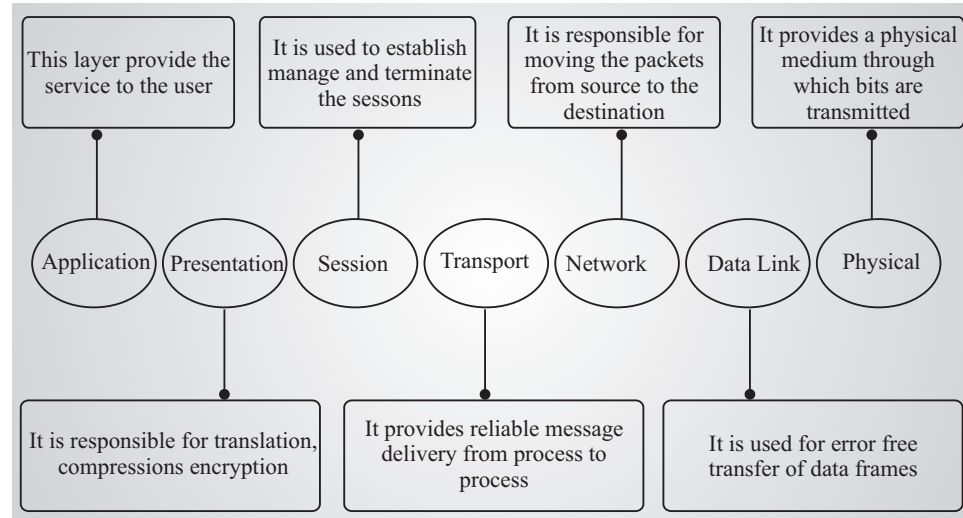


Fig. 3.8: Functions of Layers of OSI Model

3.6 TCP/IP PROTOCOL SUITE

The TCP/IP suite is a set of protocols used on computer networks today (most notably on the Internet). It provides an end-to-end connectivity by specifying how



data should be packetized, addressed, transmitted, routed and received on a TCP/IP network. This functionality is organized into four abstraction layers and each protocol in the suite resides in a particular layer.

The TCP/IP suite is named after its most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP). Some of the protocols included in the TCP/IP suite are:

- **ARP (Address Resolution Protocol):** used to associate an IP address with a MAC address.
- **IP (Internet Protocol):** used to deliver packets from the source to the destination based on the IP addresses.
- **ICMP (Internet Control Message Protocol):** used to detect and report network error conditions. Used in ping.
- **TCP (Transmission Control Protocol):** a connection-oriented protocol that enables reliable data transfer between two computers.
- **UDP (User Datagram Protocol):** a connectionless protocol for data transfer. Since a session is not created before the data transfer without any guarantee of data delivery.
- **FTP (File Transfer Protocol):** used for file transfers from one host to another.
- **Telnet (Telecommunications Network):** used to connect and issue commands on a remote computer.
- **DNS (Domain Name System):** used for host names to the IP address resolution.
- **HTTP (Hypertext Transfer Protocol):** used to transfer files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web (WWW).



INTEXT QUESTIONS 3.1

I. Choose the appropriate answer:

1. Function of Modem is
 - (a) Modulation
 - (b) Demodulation
 - (c) Both of these
 - (d) None of these



Notes

2. The OSI Layer responsible for moving the packets from source to destination

- | | |
|--------------------|-----------------------|
| (a) Physical Layer | (b) Application Layer |
| (c) Network Layer | (d) Session Layer |

II. Fill in the blanks:

1. A of wires consists of two insulated copper wires, typically about 1 mm thickness.
2. In microwave transmission the waves travel in lines.

3.7 COMMON TCP AND UDP PORTS

Transportation layer conventions utilize the idea of ports and multiplexing/demultiplexing to convey information to individual services listening on network nodes. These ports are spoken to by a solitary 16-bit number, implying that they can constitute a range of numbers 0-65535. This range has been separated by the IANA (Internet Assigned Numbers Authority) into several different segments:

- **Port 0** is not used for internet/network traffic, but it's sometimes utilized in communications going down between different programs on identical computers.
- **Ports 1-1023** are alluded to as system ports. These ports speak to official ports for most notable system administrations and many common network services. HTTP usually communicates at port 80, while FTP at port 21.
- **Ports 1024-49151** are known as registered ports. These ports are utilized for a bunch of different network functions and services that probably won't be very frequently used as ones that are on system ports. A genuine case of a registered port is 3306, which is a port that numerous databases tune in on. Registered ports are in some cases formally enlisted and recognized by IANA, yet this is not certain to always be the case. On most operating systems, any client of any entry-level can run a program tuning in on a Registered port.
- Lastly, there is a range of ports from **port 49152-65535**. These are known as **Ephemeral** ports (or **private** ports). Ephemeral ports can't be enlisted with IANA and are commonly utilized for setting up outbound network traffic and connections.



Notes

Table 3.1: Common Network Ports and their Services

PORT	Service	Description	Transport Protocol
7	Echo	Port just echoes whatever is sent to it. This feature can be used in many attacks, such as Smurf/Fraggle.	TCP and UDP
20 /21	File Transfer Protocol (FTP)	Port used by FTP protocol to send data to the client	TCP
22	Secure Shell (SSH)	Used as secure replacement protocol for Telnet	TCP and UDP
23	Telnet	Port used by Telnet to remotely connect to a workstation or server (unsecured)	TCP
25	Simple Mail Transfer Protocol (SMTP)	Used to send E-Mail over internet	TCP
53	Domain Name System (DNS)	Port for DNS requests, network routing, and zone transfers	TCP and UDP
67 /68	Dynamic Host Configuration Protocol (DHCP)	Used on networks that do not use static IP address assignment.	UDP
80	Hypertext Transfer Protocol (HTTP)	Used for browsing web-pages on a browser	TCP
110	Post Office Protocol (POP3)	Port used to retrieve complete contents of a server mailbox	TCP
143	Internet Message Access Protocol (IMAP4)	Internet Message Access Protocol (IMAP4) is a new protocol to read an email with a wider range of operations	TCP and UDP
194	Internet Relay Chat Protocol (IRC)	Allows communication in form of text between multiple parties, one or more clients can connect to a centralized server.	TCP and UDP
443	HTTP with Secure Sockets Layer (SSL)	Port used for secure web traffic	TCP and UDP
3389	Remote Desktop Protocol (RDP)	Port used by remote desktop to remotely manage other windows system	



3.8 NETWORKING COMMANDS

Windows comes with some incredibly useful networking commands that are powerful, yet very easy to use and access from the command prompt, also referred to as cmd

PING

Used for: Troubleshooting network connection issues

Command to enter: ping

The ping command is one of the most widely used utilities and used to test whether one network host is able to communicate with another.

Assuming there is nothing in place to stop the ping reaching its destination, like a firewall or a network problem, the device will respond to the ping with four data packets.

If you receive these packets back, the ping confirms that a working network path exists between you and the destination host.

```
Command Prompt
C:\Users\HP>ping google.com

Pinging google.com [142.250.193.78] with 32 bytes of data:
Reply from 142.250.193.78: bytes=32 time=2ms TTL=115
Reply from 142.250.193.78: bytes=32 time=4ms TTL=115
Reply from 142.250.193.78: bytes=32 time=2ms TTL=115
Reply from 142.250.193.78: bytes=32 time=2ms TTL=115

Ping statistics for 142.250.193.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 2ms

C:\Users\HP>^S
```

IPCONFIG

Used for: Quickly finding your IP address

Command to enter: *ipconfig*



IPConfig is one command that provides a lot of useful information.

Simply, the IPConfig command displays basic IP address configuration information for the Windows device you are working on.

IPConfig has a few switches associated with it to provide additional information as well as perform certain actions:

- IPConfig /all – Displays additional information for all network adapters
- IPConfig /release – Releases the IP address you are currently using
- IPConfig /renew – Renews an IP address on your device
- IPConfig /flushdns – Flushes the DNS cache
- IPConfig /? – Displays help for IPConfig and its switches

```
Command Prompt
C:\Users\HP>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : Dlink
    Link-local IPv6 Address . . . . . : fe80::8fd0:8c40:adde:df2b%12
    IPv4 Address. . . . . : 192.168.5.168
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::7a98:e8ff:fe21:5e81%12
                                192.168.5.1

Wireless LAN adapter Wi-Fi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : Dlink

Wireless LAN adapter Local Area Connection* 9:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```



GETMAC

Used for: Quickly finding your MAC address

Command to enter: getmac

In order to be compliant with the IEEE 802 standards, each device must have a unique MAC (Media Access Control) address.

The getmac command provides an easy way to find the MAC address of your device. If you see more than one MAC address for your device, it will have multiple network adapters

As an example, a laptop with both Ethernet and Wi-Fi will have two separate MAC addresses

```
Command Prompt
C:\Users\HP>getmac

Physical Address    Transport Name
=====
5C-60-BA-A2-00-C2   \Device\Tcpip_{9547DCC3-203E-4367-B6CD-A20F01D83006}
AC-50-DE-D2-1B-2B   Media disconnected
AC-50-DE-D2-1B-2C   Media disconnected
```

ARP

Used for: Troubleshooting network connection issues

Command to enter: arp

ARP stands for Address Resolution Protocol and the command is used to map an IP address to a MAC address.

It is easy to assume that communication over a network takes place using just IP addresses, but this is not the case. The delivery of packets is ultimately dependent on the MAC address of the device's network adapter, not the IP address.

By using the arp command, you can display and modify the Address Resolution Protocol cache; useful for resolving address resolution problems



```
C:\Users\HP>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          Displays current ARP entries by interrogating the current
            protocol data. If inet_addr is specified, the IP and Physical
            addresses for only the specified computer are displayed. If
            more than one network interface uses ARP, entries for each ARP
            table are displayed.

-g          Same as -a.

-v          Displays current ARP entries in verbose mode. All invalid
            entries and entries on the loop-back interface will be shown.

inet_addr   Specifies an internet address.

-N if_addr  Displays the ARP entries for the network interface specified
            by if_addr.

-d          Deletes the host specified by inet_addr. inet_addr may be
            wildcarded with * to delete all hosts.

-s          Adds the host and associates the Internet address inet_addr
            with the Physical address eth_addr. The Physical address is
            given as 6 hexadecimal bytes separated by hyphens. The entry
            is permanent.

eth_addr    Specifies a physical address.

if_addr     If present, this specifies the Internet address of the
            interface whose address translation table should be modified.
            If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a .... Displays the arp table.
```

HOSTNAME

Used for: Quickly finding your hostname

Command to enter: hostname

The hostname command provides you with an easy way of identifying the hostname that has been assigned to your Windows device.

There are ways of being able to find this through Windows, but using the command line is much quicker.

Simply type hostname into the command prompt and it will present you with the local computer name of your device.

```
C:\Users\HP>hostname
DESKTOP-70AS7GT
```



NSLOOKUP

Used for: Troubleshooting network connection issues

Command to enter: nslookup

NSLookup is useful for diagnosing DNS name resolution problems.

By typing nslookup into the command prompt, you will be presented with the name and IP address of your device's DNS server.

For you at home, this will more than likely be your router, but in enterprise environments, this will probably be a dedicated DNS server.

NSLookup can be used to find the IP address of a device, find the domain name of an IP address and find mail servers for a domain.

```
C:\Users\HP>nslookup
Default Server:  UnKnown
Address:  fe80::7a98:e8ff:fe21:5e81
```

The hostname command provides you with an easy way of identifying the hostname that has been assigned to your Windows device.

There are ways of being able to find this through Windows, but using the command line.

NBTSTAT

Used for: Troubleshooting NetBIOS issues

Command to enter: nbtstat

As you now know from using the hostname command, each device running Windows will be assigned a computer name.

Often, there will be either a domain or workgroup that is also assigned and that the device is a member of. For you at home, your device is likely to be within its own workgroup.

The technical term for the computer name is the NetBIOS name, which is where the nbtstat command comes into play.

Nbtstat-n will show the NetBIOS names that are in use by a device, whereas the nbtstat-r command shows how many NetBIOS names a device has recently been able to resolve.



```
C:\Users\HP>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
          [-r] [-R] [-RR] [-s] [-S] [interval] ]

-a (adapter status) Lists the remote machine's name table given its name
-A (Adapter status) Lists the remote machine's name table given its
                        IP address.
-c (cache)           Lists NBT's cache of remote [machine] names and their IP addresses
-n (names)           Lists local NetBIOS names.
-r (resolved)        Lists names resolved by broadcast and via WINS
-R (Reload)          Purges and reloads the remote cache name table
-S (Sessions)        Lists sessions table with the destination IP addresses
-s (sessions)        Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
-RR (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh

RemoteName  Remote host machine name.
IP address   Dotted decimal representation of the IP address.
interval    Redisplays selected statistics, pausing interval seconds
             between each display. Press Ctrl+C to stop redisplaying
             statistics.
```

NET

Used for: Displaying available Net switches

Command to enter: net

The net command is definitely a versatile one, allowing you to manage many different aspects of a network and its settings such as network shares, users and print jobs.

These include accounts to set password and logon requirements, file to show a list of open files and sessions to list, or even disconnect, sessions on the network.

If you are ever in doubt as to what task each switch performs, run net help and I'm sure you'll find the answer.

```
C:\Users\HP>net
The syntax of this command is:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
  HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
  STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

NETSTAT

Used for: Displaying network statistics

Command to enter: netstat

Viewing network statistics is a great way to troubleshoot any problems you are experiencing on your network and may well point you in the direction of the root



Notes

Computer Networks

cause. It will describe the protocol being used, the local address, the foreign address, and the connections state.

```
C:\Users\HP>NETSTAT

Active Connections

Proto Local Address          Foreign Address         State
TCP   127.0.0.1:49674         DESKTOP-70AS7GT:49675  ESTABLISHED
TCP   127.0.0.1:49675         DESKTOP-70AS7GT:49674  ESTABLISHED
TCP   127.0.0.1:60480         DESKTOP-70AS7GT:60481  ESTABLISHED
TCP   127.0.0.1:60481         DESKTOP-70AS7GT:60480  ESTABLISHED
TCP   127.0.0.1:60482         DESKTOP-70AS7GT:60483  ESTABLISHED
TCP   127.0.0.1:60483         DESKTOP-70AS7GT:60482  ESTABLISHED
TCP   192.168.5.168:7680      ManishTyagi-1547:51112 ESTABLISHED
TCP   192.168.5.168:49416    20.198.118.190:https   ESTABLISHED
TCP   192.168.5.168:50796    104.26.9.169:https     TIME_WAIT
TCP   192.168.5.168:50799    172.67.156.179:https   ESTABLISHED
TCP   192.168.5.168:50847    199.232.21.229:https   ESTABLISHED
TCP   192.168.5.168:50875    172.64.152.89:https    TIME_WAIT
TCP   192.168.5.168:50876    192:https              ESTABLISHED
TCP   192.168.5.168:50912    207.65.33.78:https     ESTABLISHED
TCP   192.168.5.168:50914    211:https              ESTABLISHED
TCP   192.168.5.168:50927    87:https              ESTABLISHED
```

NETSH

Used for: Displaying and configuring network adapters

Command to enter: netsh

Netsh is another very powerful command, allowing you to view and configure almost all of the network adapters in your device in much greater detail compared with some other commands.

To check all of the available netsh contexts, run netsh /?

To inspect all of the wireless network drivers on your device and their attributes, for instance, run the **netsh wlan display drivers** command.

```
C:\Users\HP>netsh wlan show interfaces

There is 1 interface on the system:

Name               : Wi-Fi
Description        : Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter
GUID               : b3e0bd4b-97b6-42ff-a363-600f971bc43f
Physical address   : ac:50:de:d2:1b:2b
Interface type     : Primary
State              : disconnected
Radio status       : Hardware On
                   : Software On

Hosted network status : Not available
```



TASKKILL

Used for Ending processes

Command to enter: taskkill

I'm sure you are familiar with being able to end a process using the Task Manager, but did you know it is also possible from the command line?

Well, you certainly can, and you have the option to kill a task or process using either the process ID or by the file name.

```
C:\Users\HP>taskkill /IM mspaint.exe
SUCCESS: Sent termination signal to the process "mspaint.exe" with PID 4036.
```

PATHPING

Used for Troubleshooting network connection issues

Command to enter: *pathping*

pathping combines that best of both ping and tracert into a single utility. Enter pathping followed by a hostname into the command prompt and it will initiate what looks like a regular old tracert command.

```
C:\Users\HP>pathping 192.168.5.168

Tracing route to DESKTOP-70AS7GT.DLink [192.168.5.168]
over a maximum of 30 hops:
 0  DESKTOP-70AS7GT.DLink [192.168.5.168]
 1  DESKTOP-70AS7GT.DLink [192.168.5.168]

Computing statistics for 25 seconds...
Hop  RTT      Source to Here   This Node/Link   Address
     Lost/Sent = Pct Lost/Sent = Pct  Lost/Sent = Pct  Address
 0                               0/ 100 = 0%      DESKTOP-70AS7GT.DLink [192.168.5.168]
 1    0ms      0/ 100 = 0%      0/ 100 = 0%      DESKTOP-70AS7GT.DLink [192.168.5.168]

Trace complete.
```

SYSTEMINFO

Used for : Displaying system information

Command to enter: systeminfo

This command will poll your device and display the most important information in a clean, easy to read format.



```
C:\Users\HP>systeminfo

Host Name:                DESKTOP-70AS7GT
OS Name:                  Microsoft Windows 11 Pro
OS Version:               10.0.22621 N/A Build 22621
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         HP
Registered Organization:
Product ID:                00330-50000-00000-AADEM
Original Install Date:     4/26/2023, 3:43:12 PM
System Boot Time:         12/28/2023, 9:48:25 AM
System Manufacturer:       HP
System Model:              HP ProOne 440 23.8 inch G9 All-in-One Desktop PC
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 151 Stepping 2 GenuineIntel ~1400 Mhz
BIOS Version:              HP U13 Ver. 02.07.00, 12/15/2022
Windows Directory:         C:\WINDOWS
System Directory:           C:\WINDOWS\system32
```

3.9 IPV4 ADDRESSING

A 32-bit string of numbers separated by periods is an **IPv4 address**, or Internet Protocol version 4. It gives a device's network interface a unique identity. IP address is a component of the TCP/IP (Transmission Control Protocol/Internet Protocol) family of protocols, which serves as the main set of guidelines for online communication. For devices like printer, PCs, printers, routers, switches, etc. to be able to communicate with one another within the network and over the Internet, they must be assigned an IP address.

IPv4 Address Format

A dot is used to separate each set of four decimal integers that make up an IPv4 address also called as “**dotted decimal format**.” Because each set is made up of eight bits, it is referred to as a “**octet**.” Each octet in the IP address 192.168.10.100 is displayed in binary format in the picture below:

Format	1 st Octet	2 nd Octet	3 rd Octet	4 th Octet
Dotted Decimal	192	168	10	100
Binary	11000000	10101000	00001010	01100100

Fig. 3.9: IPv4 Address Format

An octet's value can be anything between 0 and 255. As a result, the entire range of IPv4 addresses is 0.0.0.0 to 255.255.255.255. The network part and the host part are the two components of an IPv4 address. It uses a subnet mask to identify these components.



Network Part

The left side of the IP address represents the **network part** of an IPv4 address. It identifies the specific network that the IPv4 address is assigned to. The IP address class of the IPv4 address is also identified by the network component of the address.

For instance, we have a /24 subnet mask and the IPv4 address 192.168.10.100.

/24 indicates that the network component of the IPv4 address is the first 24 bits, beginning on the left side. The host component consists of the final 8 bits out of the 32 bits.

Format	1 st Octet	2 nd Octet	3 rd Octet	4 th Octet
Dotted Decimal	192	168	10	100
Binary	11000000	10101000	00001010	01100100
Network				Host

Host Part

Network's device or interface is uniquely identified by the **host part** of its IPv4 address. Direct communication between hosts with the same network segment is possible; traffic does not need to be routed.

IPv4 Address Allocation

Hosts and interfaces can have their IP addresses assigned to them either dynamically or manually.

- **Static:** On the device, a **static IP** address is manually configured. Setting static IP addresses on servers and network equipment like routers and switches is recommended practice.
- **Dynamic:** Dynamic Host Configuration Protocol (DHCP) allows a device to be automatically assigned a **dynamic IP** address. It is recommended to use dynamic IP addresses on endpoints, like PCs.

Types of IPv4 Addresses

Public and private IP addresses are the two categories of IP addresses that exist.

- **Public IP address:** used for Internet traffic routing. This is distributed to clients by Internet Service Providers (ISPs) and used on the Internet.
- **Private IP address:** utilized for LAN internal traffic in private networks. The Internet cannot route private addresses.



3.10 RIR

An entity that oversees the distribution and registration of Internet number resources in a particular geographic area is known as a **regional Internet registry (RIR)**. Autonomous system (AS) numbers and IP addresses are examples of internet number resources.

As the regional Internet register system developed, it was finally divided into five regions, with a registrar responsible for each. The unincorporated Number Resource Organization (NRO), a coordinating entity to act on topics of global concern, serves as the informal conduit for communication between the regional Internet registries.

Five regional registries

1. The African Network Information Centre (AFRINIC) serves Africa.
2. The American Registry for Internet Numbers (ARIN) serves Antarctica, Canada, parts of the Caribbean, and the United States.
3. The Asia Pacific Network Information Centre (APNIC) serves East Asia, Oceania, South Asia, and Southeast Asia.
4. The Latin America and Caribbean Network Information Centre (LACNIC) serves most of the Caribbean and all of Latin America.
5. The Réseaux IP Européens Network Coordination Centre (RIPE NCC) serves Europe, Central Asia, Russia, and West Asia.

Internet Assigned Numbers Authority (IANA)

The Internet Number Registry System, which is outlined in IETF RFC 7020—IETF being an acronym for the Internet Engineering Task Force—includes regional Internet registries. The RIRs, which in turn follow their regional policies to allocate resources to their clients, which include Internet service providers and end-user organizations, get Internet resources from the Internet Assigned Numbers Authority (IANA). As a group, the RIRs take part in the Number Resource Organization (NRO), which was established to represent their interests collectively, carry out cooperative projects, and coordinate their efforts internationally. In order to form the Address Supporting Organization (ASO), which coordinates global IP addressing policy within the ICANN framework, the NRO and ICANN have entered into an agreement.



3.11 TCP/IP TROUBLESHOOTING UTILITIES

Like any craftsman, network engineers too require tools to complete their tasks. Network engineers require tools and network utilities to enable them to perform their duties effectively, whether they are building, testing, monitoring, or troubleshooting. But just like at your neighborhood hardware shop, there are a bewildering array of tools and services available for networks these days.

TCP/IP tools are crucial since they will enable you to diagnose the majority of TCP/IP issues and start working on solutions, in addition to helping you on your networking examinations.

Wireshark (free, open source)

The packet detail moving across the network is the primary source of the majority of performance and security issues with networks. Nearly a million downloads of Wireshark, the industry standard tool for gathering and interpreting this data, occur each month.

Engineers can rapidly deconstruct a problem to its packet level with the help of Wireshark. This enables them to ascertain the cause of the problem promptly, be it the network, server, service, or client.

Nmap (free, open source)

On today's networks, maintaining security is essential, and it doesn't just happen. Engineers must constantly scan and monitor networks for illegal devices and open ports in order to keep ahead of invasions and vulnerabilities that could be exploited by potential hackers.

Nmap offers tools to find hosts on the network, ports on those hosts, operating systems and firewalls that are active, and much more. Engineers can identify problematic devices and open sockets with its ability to scan entire subnets and TCP port ranges.

iPerf3 (free, open source)

To debug any network issue, it is crucial to validate throughput and packet loss in a comprehensive manner. It is not a guarantee that we are obtaining 1Gbps of bandwidth just because a circuit or connection is described as such.

Notes

Engineers may monitor network throughput, packet loss, and jitter with iPerf3. iPerf3 can assist in identifying and fixing several problems, such as traffic



congestion, link-level failures, packet loss caused by shifting latency, and throughput concerns. These metrics aid in determining whether or not the network is to blame for the performance issue.

Cisco Packet Tracer (free)

For network engineers, network simulation is essential, particularly during the design phase. In order to assist engineers in simulating and testing network settings prior to their deployment to the enterprise, Cisco created the Packet Tracer tool.

Since these tools don't require expensive hardware to build and test huge setups, they're very useful for industry certification examinations preparation..

Putty (free, open-source)

Putty gives the ability to access and configure network devices. Even if automation is becoming more and more prevalent and sophisticated new technologies are hitting the market, basic setup and troubleshooting still require professionals to have direct access to the infrastructure. Putty remains the preferred tool for command line access for the majority of users.

Netstat (free, command line, multiple operating systems)

The majority of operating systems provide Netstat (Network Statistics), a command-line utility that shows the current state of TCP and UDP communications. When determining server load, connecting connections to a particular process, or keeping an eye on the security of a system that is being attacked, this data is quite useful.

Angry IP Scanner (free, open-source)

Though it is comparable to Nmap, the Angry IP Scanner simplifies things and speeds up the process. To find out if the device is alive, the program only pings each IP address in the configuration list. If necessary, it can also resolve the hostname, find the MAC address, and run a port scan. These scans' output results can be exported to Excel or a number of other formats.



INTEXT QUESTIONS 3.2

I. Write the full form of following terms:

- | | | |
|----------|---------|---------|
| (a) HTTP | (b) UDP | (c) ARP |
| (d) ICMP | (e) DNS | |



II. State whether the following statements are true or false:

1. The Network portion of the IPv4 address uniquely identifies the device or the interface on your network.
2. ICMP is used to detect and reports network error conditions



WHAT YOU HAVE LEARNT

- A collection of interrelated computers that help in the exchange and sharing of information is referred to as a computer network.
- A hub is used within a network as a common connecting point, where multiple devices can connect and communicate with one another.
- Modem is the device converts digital data to analog signals and vice versa to allow communication over different types of transmission media.
- A bridge is a networking device that connects two or more network segments within a single logical network, thereby enhancing the overall performance and efficiency of the network.
- The Open Systems Interconnection (OSI) model is a reference framework that consists of seven distinct layers, each of which has a specific function in the network communication process.
- The TCP/IP suite is a collection of protocols designed to provide end-to-end connectivity by defining how data should be packetized, addressed, transmitted, routed, and received across a TCP/IP network.
- Multiplexing and demultiplexing processes are enabled by different TCP/UDP ports, allowing information to be conveyed to individual services operating on network nodes, such as FTP, Telnet, and DHCP.
- Networking commands, which can be easily accessed from the command prompt, include utilities such as ping, ipconfig, and getmac, providing essential functionality for network management and troubleshooting.
- An Internet Protocol version 4 address consists of a 32-bit string of numbers separated by periods that uniquely identifies a device on a network.
- A Regional Internet Registry (RIR) is an organization that distributes and registers Internet number resources around the world to ensure effective allocation and management of these resources.



Notes



TERMINAL EXERCISE

1. What is the use of Netstat utility?
2. Explain Transmission media and their types?
3. Write a short note on RIR and IANA
4. What is OSI model? How many layer does it has? Name them.
5. Write a short note on TCP/IP protocol suite.
6. Mention number of bits used for IPV4 addressing? Explain its address format
7. Why networking commands are useful? Enlist commands and their use?



ANSWERS TO INTEXT QUESTIONS

3.1

- I.** 1. (c) 2. (c)
- II.** 1. twisted pair 2. straight

3.2

- I.** (a) **HTTP:** Hyper Text Transfer Protocol
(b) **UDP:** User Datagram Protocol
(c) **ARP:** Address Resolution Protocol
(d) **ICMP:** Internet Control Message Protocol
(e) **DNS:** Domain Name System
- II.** 1. False 2. True

Key Learning Outcomes

- Describe the various transmission modes and the classification of transmission media
- Analyze the functions of different layers in the OSI and TCP/IP
- Explain about different networking devices like repeaters, hubs, and routers.
- Compare common TCP/UDP ports used by services like FTP and HTTP



4

WEB APPLICATION AND SECURITY

Web applications are integral to our online experience, enabling us to do everything from shopping to socializing. Developers should understand how web applications are developed and how they should be secured. The Internet is a network of connected systems that are incredibly complex, and the nature of cyberattacks is growing increasingly sophisticated. For this reason, there should be robust security measures in place for valuable information as well as ensuring the correct functionality of web systems.

In the last lesson, you learned about computer networks and their role in device communication. In this lesson, you will learn about secure web applications ensuring the safety of your web applications.

One may think of networks as the infrastructure of digital communication and web applications as the instruments we use to view and interact with information. This lesson will teach you about securing web applications, highlighting the vital link between network protocols and application security.



OBJECTIVES

After reading this lesson, you will be able to:

- state and describe Web application terminologies;
- explain Web Application protocols;
- describe basic HTML tags;
- differentiate between HTTP and HTTPS;
- explain Browser security & Email Security.



Notes

4.1 WHAT IS A WEB APPLICATION?

A web application, also referred to as a “web-based application,” is the software that runs on web servers and is accessed through web browsers over the internet. Unlike desktop applications, which must be installed on specific devices, web applications offer a platform-independent experience. That is, users do not require specific configurations to run the application and hence they can access its features using a web browser on different devices, such as computers, tablets and smart phones.

Web applications are designed to function with the client-server model, as demonstrated in Fig. 4.1, where the user’s device, referred to as the client, sends requests to a remote server for data access and submission. The client-server model allows for dynamic and interactive functionality. Many people use online banking systems, social media platforms, e-commerce sites, and even Google Docs, which are examples of web applications.

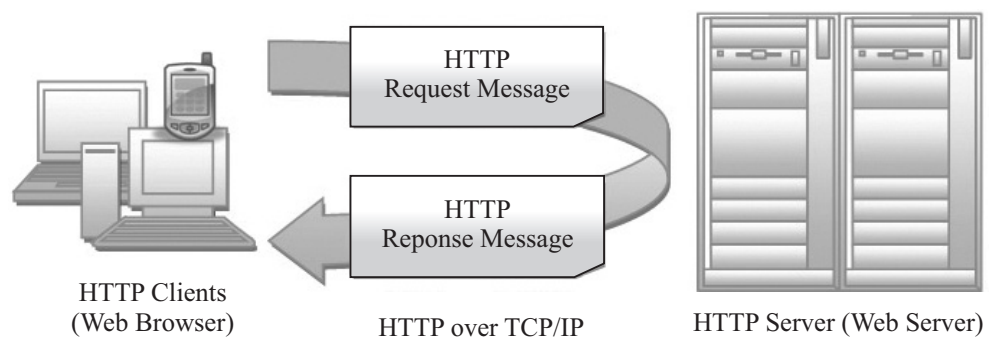


Fig. 4.1: Client Server Architecture

Web applications are built using a variety of programming languages, tools, and technologies. The frontend part is that portion which interacts with the user, whereas the backend performs server-side processes and includes data storage in addition to business logic.

With the advancement of technology and fast internet speeds, web applications have become popular, changing the way people access and use software services.

4.2 WEB APPLICATION TERMINOLOGIES

“Web application terminology” refers to the specialized terms and concepts used in web development and management. These terms are essential for developers, designers, and anyone involved in building and maintaining web-based applications. Understanding this terminology ensures effective communication and collaboration in the web development field.



Following are the most used terminologies in web based application:

1. **Client-Server Architecture:** Describes the relationship between the user's device (client) and the remote server where the web application is hosted, defining their respective roles in data processing and presentation.
2. **Frontend:** The user interface and user experience components of a web application that users interact with directly. It includes elements like web pages, forms, and visual design elements.
3. **Backend:** The server side of a web application responsible for handling data storage, business logic, and server side processing. It interacts with the frontend to deliver a seamless user experience.
4. **API (Application Programming Interface):** A set of rules and protocols that allows different software applications to communicate with each other. In the context of web applications, APIs enable interaction between the frontend and backend components.
5. **MVC (Model View Controller):** An architectural pattern commonly used in web development that separates the application into three interconnected components Model (data and business logic), View (user interface), and Controller (handles user input and updates the model).

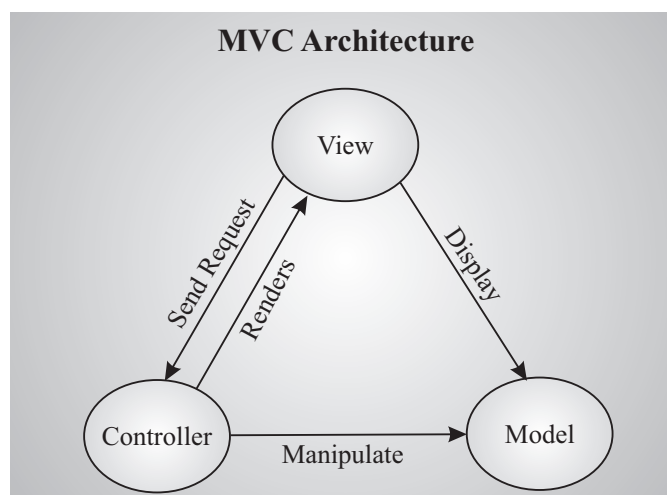


Fig. 4.2: Model View Controller Architecture

6. **HTTP (Hypertext Transfer Protocol):** The fundamental protocol for data communication on the World Wide Web. It defines how messages are formatted and transmitted, allowing for the retrieval of linked resources (such as HTML pages, images, etc.) from servers.



Notes

Web Application and Security

7. **Cookies:** Small pieces of data stored on the user's device by the web server through web browser. Cookies are used to retain user specific information, such as login credentials or user preferences, across multiple sessions.
8. **Session Management:** A session is a temporary connection between the client and server, kept active to track user activities. It gets started once a user logs in to a networked application and terminates due to log off session expiry or the user disconnection. Session Management is the process of securely handling user sessions, typically involving the use of tokens or cookies to keep track of a user's interactions with the web application during a particular visit.
9. **URL (Uniform Resource Locator):** A web address that specifies the location of a resource on the internet. It is used by browsers to retrieve specific web pages or data from servers.
10. **IPAddress:** An IP Address is an Internet Protocol Address assigned to every device on a network so that devices can communicate with each other over the internet or a local network. It's a virtual address through which data can be sent and received between devices like computers, smartphones, and servers.

IP addresses are of two versions: IPv4 and IPv6. IPv4 has a 32-bit address format, written as dotted decimal for example, such as 192.168.1.1 and IPv6 has a 128-bit address represented in hexadecimal form, such as 2001:0db8:85a3:0000:0000:8a2e:0370:7334. IP addresses are important for routing information across networks so that the data packets get to the correct destination.

11. **Port Number:** Port numbers are essential components of the networking architecture that facilitate the organization and management of network communication. In the context of the Internet Protocol (IP), a port number is a 16bit unsigned integer, thus ranging from 0 to 65535. It serves as a way to differentiate between different services or processes running on a single device.



INTEXT QUESTIONS 4.1

1. Fill in the blank

- (a) Web applications are programs or software applications that run on a web



- (b) Web applications use technologies to provide dynamic and interactive experiences for users.
- (c) The frontend of a web application is responsible for the user
- (d) Web applications have become integral components of our digital landscape, providing functionalities such as online and social networking.

4.3 WEB APPLICATION PROTOCOLS

Web application protocols are the basic rules that enable computers to communicate and share information between the user's computer and the server. They are highly important in making sure that websites work efficiently. One of the most significant protocols is known as HTTP (Hypertext Transfer Protocol) as shown in fig 4.2. It enables your web browser to obtain text and links from a website's server, such as reading an article or clicking on a link. HTTP dictates how the information is sent and received, and thus you see things like web pages, pictures, and videos.

To add more security to this, there's HTTPS (Hypertext Transfer Protocol Secure). It is like the version of HTTP that has been upgraded. It adds protection by encrypting the information sent. This is an added layer that keeps all the important stuff, such as your login details and financial transactions, safe from potential spying or meddling. Thus, it ensures that the channel for sending sensitive information is secure.

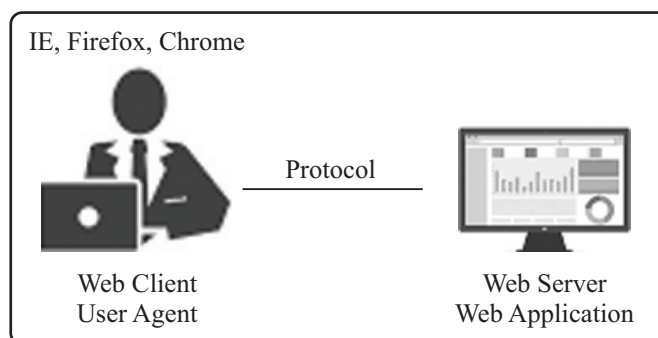


Fig. 4.3: Protocol Structure

In addition to HTTP and HTTPS, other protocols include FTP (File Transfer Protocol), which is used in transferring files within web applications, SMTP (Simple Mail Transfer Protocol), which allows email communications in web applications, IMAP (Internet Message Access Protocol), used for accessing Internet messages, and POP3, which is short for Post Office Protocol version 3.



Notes

Web Application and Security

Indeed, as development in web design evolves, all these protocols form the basis upon which developers make their web applications robust, efficient, and safe.

Web application protocols are sets of rules and conventions that govern the communication and data exchange between different components of a web application. The most commonly used web application protocols are:

1. **HTTP (Hypertext Transfer Protocol):** The foundation of any data exchange on the web, HTTP is used for transmitting hypertext (text with links) and is the protocol behind the transfer of data between a user's browser and a web server.
2. **HTTPS (Hypertext Transfer Protocol Secure):** An extension of HTTP that adds a layer of security through encryption. It uses SSL/TLS protocols to secure the data transmitted between the client and the server, safeguarding against eavesdropping and tampering. SSL (Secure Socket Layer) and TLS (Transport Layer Security) are protocols that encrypt data to ensure secure communication over the internet. TLS is the successor of SSL, which provides stronger encryption and improved security.
3. **WebSocket:** A communication protocol that provides communication channels. WebSockets enable real time communication between the client and the server, allowing for more interactive and dynamic web applications.
4. **FTP (File Transfer Protocol):** FTP is often used for the transfer of files between a client and a server. It's commonly employed in web development for uploading files to a web server.
5. **SMTP (Simple Mail Transfer Protocol):** Specifically designed for email transmission, SMTP is used for sending emails from a client to a server or between servers.
6. **IMAP (Internet Message Access Protocol):** IMAP is an important tool for emails. It helps you check and handle your emails in a flexible way on different devices. With IMAP, your emails stay on the email server, and it keeps everything in synchronization. This is great for people who want to use their emails easily on different gadgets.
7. **POP3 (Post Office Protocol version 3):** POP3, which stands for Post Office Protocol version 3, is a common way to get emails from a mail server to your computer or phone. With POP3, your emails are usually taken from the server and stored on your device. Once they're downloaded, they're often removed from the server.



While POP3 is a simple way to get your emails on one device, it has a drawback. It doesn't work well for people who want to check their emails on different devices because it doesn't keep everything in sync. That's why many modern email systems, especially for people using different gadgets, prefer the more advanced IMAP (Internet Message Access Protocol).

8. **PPP (Point to Point Protocol):** PPP is like a language that two devices use to talk directly to each other. Initially, it was made for connecting computers over the phone, but now it's used in various kinds of networks, such as fast internet and Virtual Private Networks (VPNs). PPP is excellent at sending data between two devices by putting a cover around it so that it can go through various kinds of connections.
9. **TELNET (Terminal Network):** Telnet is a way to control a computer or device from far away. It lets you act like you're right there, typing commands on the machine. Telnet works by connecting your device to the remote one over the network. You can give commands and get information just like you're using the computer directly.

Telnet sends everything in plain text, so it's not very secure. That means if you use Telnet, someone could easily see your usernames and passwords. Because of this security risk, people now prefer using more secure methods like SSH (Secure Shell) for remote control, especially when dealing with sensitive information. Even though Telnet used to be popular for managing computers from a distance, its use has gone down because of these security concerns. Modern practices suggest using encrypted protocols like SSH for better protection during remote connections.

10. **SSH (Secure Shell):** SSH, or Secure Shell, is a cryptographic network protocol that provides a secure way to access and manage network devices and servers over a potentially insecure network. SSH encrypts the communication between the client and the server, ensuring the confidentiality and integrity of the transmitted data.



INTEXT QUESTIONS 4.2

1. State whether the following are True or False:
 - (a) HTTP (Hypertext Transfer Protocol) is a secure protocol for transmitting data between a user's browser and a website's server.
 - (b) IMAP (Internet Message Access Protocol) is primarily used for retrieving messages from a mail server to a local email client.



Notes

Web Application and Security

- (c) Telnet is a secure protocol for remote access, encrypting data to protect against unauthorized access.
- (d) In HTTPS, the “s” in “https://” indicates a secure connection, signifying the use of encryption.
- (e) Point-to-Point Protocol (PPP) is commonly used in networking to establish connections between multiple devices.

4.4 DIFFERENCE BETWEEN HTTP AND HTTPS

HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) are like special rules for how your web browser talks to a website’s computer. HTTP is the basic one, but it sends information in a way that others could read it while it’s traveling through the internet. This means someone might see things like your login details.

Now, HTTPS is like the upgraded version. It uses something called SSL (Secure Sockets Layer) to turn the information into secret code when it goes between your computer and the website. This secret code keeps your important stuff, like logins and personal details, safe as it travels through the internet.

You can tell if a website is using HTTPS because its web address starts with “https://” instead of just “http://”. This is important for websites, especially when you’re doing things like buying stuff online. Using HTTPS makes sure your communication with the website is super secure, protecting you from potential online dangers. Search engines also like websites that use HTTPS, so it helps them show up better in search results.

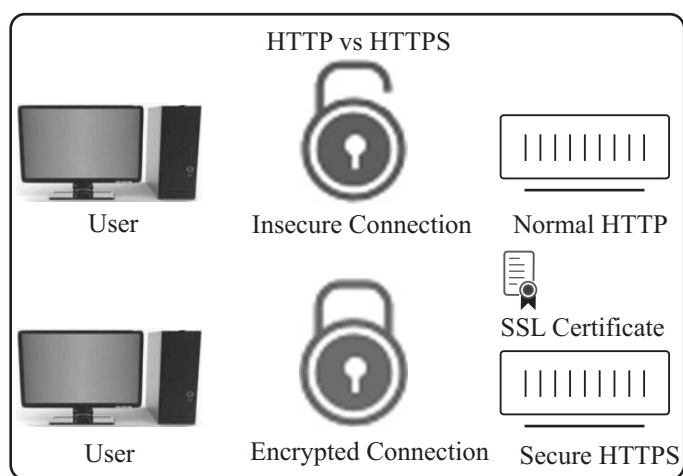


Fig. 4.4: HTTP and HTTPS



Here are the key differences between HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure):

Table 4.1: Difference between HTTP and HTTPS

Aspect	HTTP	HTTPS
Security	Not secure. Data transmitted in plain text, vulnerable to eavesdropping and interception.	Secure. Uses SSL/TLS protocols to encrypt data, ensuring confidentiality and protection against unauthorized access.
Data Transmission	Plain text transmission, readable if intercepted.	Encrypted transmission, even if intercepted, data remains unreadable without the decryption key.
Port Number	Operates on port 80 by default.	Operates on port 443 by default. Different port for secure traffic.
URL Indicator	URL begins with “http://” in the address bar.	URL begins with “https://”. “s” indicates a secure connection.
Certificate Requirement	No SSL/TLS certificate required.	Requires an SSL/TLS certificate from a Certificate Authority (CA) for authenticity and secure communication.
SEO Consideration	Search engines may penalize HTTP websites due to security concerns.	HTTPS is favored by search engines, and having a secure connection can positively impact search rankings.

4.5 BROWSER SECURITY

Browser security is a critical aspect of ensuring a safe and trustworthy online experience for users. Web browsers, the gateways to the internet, implement various security measures to protect users from potential threats and vulnerabilities. Features such as secure socket layers (SSL) protocol are integral components that enable encrypted communication between the browser and websites, safeguarding sensitive data like login credentials and personal information. Browser security also involves regular updates and patches to address identified vulnerabilities, ensuring that users are protected against the latest security threats. Phishing and malware protection security policies further contribute to the overall security posture of modern web browsers, creating a more resilient and secure environment for users as they navigate the vast landscape of the internet.



4.5.1 Components of Browser Security

Browser security involves a combination of components and features designed to protect users from various online threats. Here are key components of browser security:

1. **HTTPS (Hypertext Transfer Protocol Secure):** HTTPS is a fundamental component that ensures secure communication between the user's browser and the websites they visit. It employs encryption protocols like SSL/TLS to safeguard data during transmission, reducing the risk of eavesdropping and data interception.
2. **SSL/TLS Protocols:** Secure Socket Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols that provide the foundation for secure communication on the internet. They establish encrypted connections, protecting sensitive information such as login credentials and financial transactions.
3. **Phishing and Malware Protection:** Modern browsers incorporate mechanisms to detect and block phishing attempts and malicious websites. These features warn users or prevent access to sites known for phishing activities, thus reducing the likelihood of users falling victim to scams or malware.
4. **Browser Updates and Patch Management:** Regular updates and patches are crucial for addressing identified vulnerabilities in browsers. Browser developers release updates that include security fixes, ensuring that users are protected against the latest threats. Timely updating is a critical component of browser security.
5. **Security Sandbox:** Sandboxing prevents malicious code from affecting the entire system by confining it to a restricted environment within the browser.
6. **MultiFactor Authentication (MFA):** Some browsers support multifactor authentication, adding an extra layer of security beyond traditional passwords. MFA requires users to provide multiple forms of identification, reducing the risk of unauthorized access, even if login credentials are compromised.
7. **Privacy Controls:** Browsers offer privacy controls such as incognito or private browsing modes that limit the storage of browsing history, cookies, and other data. Additionally, features like tracking protection enhance user privacy by preventing websites from collecting unnecessary data.



8. **Network Security Measures:** Browsers often integrate with network security measures, such as firewalls and intrusion detection systems, to provide an additional layer of protection against external threats.

By integrating these components, browsers aim to create a robust security environment that protects users from various online threats, ensuring a safer and more secure internet browsing experience.

4.6 EMAIL SECURITY

Email security refers to the set of measures and practices implemented to protect email communication from various cyber threats and ensure the confidentiality, integrity, and availability of sensitive information exchanged through email channels. With email being a primary means of communication for individuals and organizations, email security is of paramount importance. This security encompasses a range of technologies and protocols designed to guard against threats such as phishing attacks, malware, unauthorized access, and data breaches. Key components of email security include encryption to protect the content of emails, authentication mechanisms to verify the legitimacy of senders, antiphishing measures to identify and block malicious attempts, spam filtering to reduce unwanted and potentially harmful emails, and data loss prevention to control the inadvertent or intentional disclosure of sensitive information. Robust email security measures are critical for maintaining trust, preventing unauthorized access, complying with regulations, and safeguarding against the diverse array of cyber threats that can exploit vulnerabilities in email communication.

4.6.1 Why Email Security?

Email security is crucial for several reasons, reflecting the central role that email plays in personal and business communications. Here are key reasons why email security is important:

1. **Confidentiality of Information:** Emails often contain sensitive and confidential information, including personal details, financial data, and business communications. Ensuring the confidentiality of this information is paramount to prevent unauthorized access or data breaches.
2. **Protection Against Phishing Attacks:** Phishing attacks, where attackers attempt to trick individuals into revealing sensitive information or downloading malicious content, are commonly carried out through email. Effective email security measures help identify and block phishing attempts, protecting users from falling victim to scams.
3. **Prevention of Data Loss:** Email security helps prevent unintentional or malicious data loss by implementing measures such as encryption and data



Notes

Web Application and Security

loss prevention (DLP). This ensures that sensitive information does not fall into the wrong hands, either through accidental disclosure or intentional theft.

4. **Business Continuity:** Email is a critical tool for communication in business environments. Email security safeguards against disruptions caused by malware, ransomware, or other cyber threats that could compromise the availability and functionality of email services.
5. **Protection from Malware and Viruses:** Email attachments and links are common vectors for spreading malware and viruses. Robust email security includes scanning for malicious content, preventing the delivery of infected files, and protecting users from inadvertently downloading harmful material.
6. **Maintaining Trust and Reputation:** Individuals and organizations rely on email for professional and personal communication. A security breach, such as unauthorized access to email accounts, can damage trust and harm an individual's or business's reputation. Email security measures help maintain the integrity of communication channels.
7. **Compliance with Regulations:** Many industries and regions have regulations and compliance requirements governing the protection of sensitive information, especially in sectors like finance, healthcare, and government. Adequate email security measures help organizations comply with these regulations and avoid legal consequences.
8. **Preventing Unauthorized Access:** Unauthorized access to email accounts can lead to identity theft, unauthorized transactions, or the compromise of sensitive information. Strong authentication mechanisms, multi factor authentication, and secure access controls are integral to preventing unauthorized access.
9. **Mitigating Business Email Compromise (BEC):** BEC attacks involve impersonating trusted entities to deceive individuals into transferring funds or revealing sensitive information. Email security measures, including anti-phishing techniques, are essential to mitigating the risks associated with BEC.
10. **Protecting Intellectual Property:** For businesses, email often contains intellectual property, trade secrets, and proprietary information. Email security safeguards these assets and prevents them from being exposed to competitors or malicious actors.

Email security is essential for safeguarding sensitive information, maintaining trust, ensuring business continuity, and complying with regulations. As email continues to be a primary means of communication, securing this channel is critical to protect individuals, businesses, and their assets from a variety of cyber threats.



4.6.2 Components of email Security

Email security involves a combination of components and practices aimed at safeguarding email communication from various cyber threats. Here are key components in email security:

1. **Encryption:** Encryption ensures that the content of emails is secure during transmission. It involves encoding the information so that only authorized recipients with the decryption key can access and understand the message.
2. **Authentication Mechanisms:** Authentication mechanisms help verify the authenticity of email senders, preventing email spoofing and phishing attacks.
3. **Anti-Phishing Measures:** Anti-phishing technologies are critical components that identify and block phishing attempts. These measures include link analysis, email content inspection, and real-time threat intelligence to detect and prevent users from falling victim to phishing scams.
4. **Spam Filtering:** Robust spam filters are essential for filtering out unwanted and potentially malicious emails. These filters use various techniques, including pattern recognition, blacklists, and heuristics, to identify and block spam emails.
5. **Multi-Factor Authentication (MFA):** Multi-Factor Authentication adds an extra layer of security beyond passwords. By requiring users to provide additional verification, such as a code sent to their mobile device, MFA helps prevent unauthorized access to email accounts.
6. **Secure Email Gateways:** Secure email gateways act as a protective barrier between an organization's internal email server and external networks. They scan incoming and outgoing emails for malware, viruses, and other malicious content, preventing threats from reaching users.
7. **Data Loss Prevention (DLP):** DLP solutions monitor and prevent the unauthorized sharing of sensitive information in emails. These systems can identify and block the transmission of confidential data, helping organizations maintain control over their sensitive information.
8. **Regular Software Updates and Patch Management:** Keeping email servers and email clients up to date with the latest security patches is crucial for addressing vulnerabilities that could be exploited by attackers. Regular updates help maintain the security of the email infrastructure.
9. **Email Retention Policies:** Establishing email retention policies helps manage the storage of emails, reducing the risk associated with prolonged storage of



Notes

sensitive information. Regularly deleting outdated or unnecessary emails mitigates the impact of potential data breaches.

By integrating these components, organizations can create a robust email security strategy that protects against a wide range of threats and vulnerabilities, ensuring the confidentiality, integrity, and availability of their email communication.



INTEXT QUESTIONS 4.3

Fill in the blank:

- (a) is a secure version of HTTP that uses encryption to protect the data transmitted between a user's browser and a website's server.
- (b) In browser security, a is a small data file stored on the user's device that helps websites remember user preferences and login information.
- (c) A strong policy helps protect against unauthorized access to email accounts by requiring users to create complex passwords and change them regularly.
- (d) Email is a method of filtering and blocking unsolicited and potentially harmful emails from reaching a user's inbox.



WHAT YOU HAVE LEARNT

- A web application is software that runs on web servers and is accessed via web browsers, offering a platform-independent experience. It follows a client-server architecture where the user's device (client) communicates with a remote server to access or submit data.
- Web applications rely on protocols like **HTTP** for data transmission and use **cookies** and **session management** for user data storage and interaction tracking.
- HTTP transmits data in plain text, whereas HTTPS encrypts data using SSL/TLS protocols for secure communication. HTTPS improves website security, protecting against eavesdropping and data interception, while also boosting SEO rankings.
- Web browsers use HTTPS, SSL/TLS protocols, phishing and malware protection, and regular updates to secure online activities.
- Browser security features like multi-factor authentication (MFA) and privacy controls help safeguard user information.

Web Application and Security

- Email security ensures confidentiality, protects against phishing attacks, prevents data loss, and maintains business continuity.
- Regular updates, secure email gateways, and data loss prevention (DLP) strategies are crucial in maintaining robust email security.



Notes



TERMINAL QUESTIONS

1. What is a web application, and how does it differ from traditional desktop applications?
2. Explain the significance of HTTPS in web application security.
3. Discuss the importance of browser security features.
4. What is the role of protocol in web applications?
5. Explain client server relationship in terms of web applications



ANSWERS TO INTEXT QUESTIONS

4.1

- | | |
|---------------|---------------------|
| (a) Browser | (b) Web development |
| (c) Interface | (d) Shopping |

4.2

1. (a) False (b) True (c) False (d) True (e) False

4.3

- | | |
|--------------|--------------------|
| (a) HTTPS | (b) cookie |
| (c) password | (d) spam filtering |

Key Learning Outcomes

- Identify and describe key terms used in web application development and management.
- Explain the protocols used in web applications.
- Compare HTTP and HTTPS, explaining their differences in terms of security and use in web browsing.
- Understand the security measures in web browsers and email systems.



5

EMPLOYABILITY AND COMMUNICATION SKILLS

In today's competitive job market, only technical expertise is not sufficient for any employee.. Equally important are the employability skills that help individuals perform well in their professional journeys. These skills, including effective communication, IT proficiency, 21st-century competencies, work ethics, and traits like adaptability and dependability, are essential for navigating the modern workplace. Employability skills provide the means through which individuals effectively interact with colleagues, customers, and other stakeholders to foster good relationships that would help in an organization's success. They are as important as technical skills in determining job performance and career growth.

Additionally, self-management skills, including flexibility and responsibility, are critical to adapt to the changing work environment. These skills, besides strengthening the growth and reputation of companies, pave the way for entrepreneurial ventures.

This lesson will focus on the significance of employability skills and how they contribute to the success of the individual and organization as well.



OBJECTIVES

After reading this lesson, you will be able to:

- describe importance of employability skills;
- describe 21st-century skills and their importance;
- illustrate verbal and nonverbal communication skills;



- illustrate effective communication;
- identify business opportunities;
- identify different types of financial products and service;
- compute income and expenses;
- describe importance of maintaining safety and security in financial transactions;
- explain different legal rights and laws;
- operate digital devices and applications safely and securely;
- interpret types of customers and their needs;
- describe process of application for a job and interview preparation.

5.1 EMPLOYABILITY SKILLS

An employee is a person who works for a salary. Employability skills are imperative skills which ensure one performs better in any workplace. These consist of both hard and soft skills, and these consist of key personal attributes much prized by employers. Employability skills are needed if one is to deliver effectively on the job and to continue resilient and effective in their careers.

Hard skills, or technical skills, are learned at school, in training, or through on-the-job experience. They are specific to a job and can be measured and taught.

Soft skills, being the most important skills, are generalized traits that can be applied in any job and any industry. The transferable or interpersonal skills such as communication, teamwork, attitude, and adaptability have been known as soft skills. Soft skills are essential to the success of professionals because they allow employees to thrive in any environment.

Employers not only seek technically skilled individuals but also value those who can make a broader contribution to the organization. Organizations look for people with the following qualities:

1. **Good oral and written communication skills:** Good oral and written communication are needed to communicate effectively with people and customers.

Oral communication aims to effectively convey information through clear and concise vocal words. It fosters interaction, relationship building and facilitates collaboration among individuals.



Notes

Employability and Communication Skills

Written communication relies on written words whereas oral communication involves direct interaction between individuals through spoken words. These skills enable employees to articulate ideas, collaborate with colleagues and present their thoughts convincingly to employers or clients. Written communication skills are crucial for crafting professional documents such as emails, reports, presentations and cover letters.

2. **Leadership Qualities:** It is said that Leaders are not born but they are made. Leaders provide direction, vision, motivate and inspire others and help in creating a conducive environment. Leadership skills are highly sought after by employers as they involve dealing with people, taking responsibility and initiative.

McKinsey is an American multinational strategy and management consulting firm which is the oldest and largest of the “Big Three” management consultancies has reported the analysis of academic literature as well as a survey of nearly 200,000 people in 81 organizations all over the world, there are four types of behavior that account for 89 percent of leadership effectiveness:

- being supportive
- operating with a strong results orientation
- seeking different perspectives
- solving problems effectively

3. **Critical thinking and Problem solving:** Problems in any organization range from the simplest to the most complex and should be approached constructively and equitably. To this end, critical thinking and problem-solving individuals are indispensable. They analyze a situation, apply knowledge, and make appropriate decisions. An organization needs people who can take up problems based on facts, data, and knowledge.

Organizations would want those people who can deal with issues independently or make meaningful contributions as a team member. They don't need individuals who can take the initiative and provide solutions. The perfect employee would be able to critically think and come up with unique ideas, communicate knowledge, make proper judgments, and make wise decisions. Critical thinking would therefore entail making sense of available information, asking questions, and developing reasonable conclusions for solving problems better and making informed decisions in the workplace.

4. **Positive attitude:** “You can often change your circumstances by changing your attitude.” –Eleanor Roosevelt



A positive attitude towards work can bring positive changes for you in an organization. People with a positive attitude are focussed towards work, support their colleagues, they work in collaboration and are compassionate. People with a positive attitude never complain but are always with a solution.

5. **Time Management and Organizational Skills:** Good time management and keeping organized are some of the most significant things employers seek in employees. It lets one be able to meet deadlines, balance priorities, and reduce stress. For example, a project manager with several tasks will have to organize their schedule, allocate time for each task, and avoid procrastination. This ability ensures that projects are completed efficiently and deadlines are met without compromising quality.

Organization, then, is not only time management but also a clean working environment, structured tasks and responsibilities, and the right systems for tracking progress. Be it a meeting, project timeline, or even emails, employees who are organized can make workflow smoother and help prevent bottlenecks in processes.

6. **Teamwork and Collaboration:** Employees who can work well with others contribute to a positive and productive work culture. Teamwork involves more than working with others. It requires understanding the dynamics of the group, respecting diverse perspectives, and working towards a shared goal. For instance, in a marketing campaign, a team that collaborates well can brainstorm ideas, divide tasks, and support one another in delivering the project successfully.

Collaboration is communication and compromise. When the ideas are shared and people listen to one another, there is a higher likelihood of solving any conflicts that might arise and even strengthens working relationships. Employers hire people who work well with other diverse teams, manage group dynamics effectively, and contribute to a collective goal.

7. **Adaptability and Flexibility:** Adaptability and flexibility are the most important employability skills in the fast-paced work environment. Organizations often change in terms of technology, market conditions, or business goals. Therefore, they expect employees to adjust accordingly. For example, in the pandemic era of COVID-19, employees had to rapidly shift from being in a work environment to being at home. Those employees flexible enough managed to adapt to this transition by setting up a home office and learning some communication tools with minimal disruption.



Being adaptable means openness to new ideas and changes in the workplace. It involves continuous learning of new skills and keeping updated in the modern trends of the industry and embracing change as an opportunity for growth. In dynamic work environments, the most valuable assets are those employees who can adapt to a given situation and remain productive.



INTEXT QUESTIONS 5.1

I. Fill in the blanks:

1. Rohan has completed his graduation in economics, he has developed his skills.
2. and are needed to communicate effectively with people and customers.
3. is the process of understanding information available, seeking answers and coming to a justified conclusion.
4. provide direction, vision, motivate and inspire others, and help in creating a conducive environment.
5. A is someone who works for a salary.

II. Multiple choice questions:

1. Employability skills are
 - (a) Skills for good communication
 - (b) Skill to be a good employee
 - (c) Interpersonal Skill
 - (d) None of the above
2. Which of the following is not an employability skill
 - (a) Excellent communication skill
 - (b) Positive attitude
 - (c) Sales and marketing
 - (d) Leadership qualities
3. Which are the skills needed for career growth

(a) Technical skills	(b) Soft skills
(c) Communication skills	(d) All of the above



4. An employee is someone
 - (a) Who is hired for work
 - (b) Who will paid for the job
 - (c) Both a and b
 - (d) None of the above
5. Meaning of employability skill is
 - (a) IT skills
 - (b) Skills for good communication
 - (c) To make successful at workplace
 - (d) None of the above

5.2 ENVIRONMENTALLY SUSTAINABLE PRACTICES AND THEIR IMPORTANCE

The smartest move one can make as a professional is to embrace sustainability. The 2030 Agenda for Sustainable Development, adopted by all United Nations Member States in 2015, is a step ahead for peace and prosperity for people and the planet, now and into the future.

Environmentally Sustainable Practices and their Importance: The 17 Sustainable Development Goals are a call for urgent global action from both developed and developing nations. These goals are set in place to try and address an assortment of the critical issues that prevail; these are poverty, health, education, inequality, and economic growth and include environmental conservation.



Fig. 5.1

<https://global.unitednations.entermediadb.net/assets/mediadb/services/module/asset/downloads/preset/assets/2015/09/22525/image1170x530cropped.jpg>



Notes

Employability and Communication Skills

These will only be achievable with global cooperation and individual responsibility. As citizens, we should actively contribute towards the attainment of these sustainable objectives. The development of sustainability skills broadens our knowledge but also enhances our professional skill set, ultimately fostering career growth while making a positive impact on the world.

- **Quality Education:** Education is the most powerful tool to change the world. We aim to provide quality education to each and every individual. All boys and girls should complete free primary and secondary schooling by 2030. Vocational education is mandatory as per NEP 2020. This will help an individual with necessary skills and knowledge to succeed in their chosen career paths
- **Gender Equality:** Gender equality is not only a fundamental human right, but a necessary foundation for a peaceful, prosperous and sustainable world. There has been progress over the last decades. We need to ensure that there should be equal pay for men and women.
- **Decent work and economic Growth:** There should be decent work conditions for employers. The employers should feel safe and secure in their workplace. Decent conditions To promote inclusive and sustainable economic growth, employment and decent work for all.
- **Industry, innovation and infrastructure:** Innovation and infrastructure are crucial drivers of economic growth and development. The companies are now promoting innovations and advancement in technology. They look forward to having better and smart solutions to the problems. Entrepreneurs are bringing positive change in the current scenario, they are promoting new solutions, products and services. As we are witnessing positive changes in the infrastructure of our Country in rural as well as urban areas. Using renewable sources of energy such as wind, solar, hydro and geothermal not only helps in climate change but also in stopping air pollution and improving health conditions. Promoting sustainable industries and investing in scientific research and innovation are ways to facilitate sustainable development.
- **Reduced inequalities:** We are seeing a positive change in our society as men and women are now getting equal opportunities at workspace. Earlier there had been discrimination in terms of gender, caste, religion or economic status. If each and every individual is treated the same, this will bring amazing change in our society. The world will prosper and will end discrimination.
- **Peace, Justice and strong institutions:** This goal is about promoting peaceful and inclusive society. It aims for access to justice for all and building



effective, accountable and inclusive institutions at all levels. People should feel safe and far away from all violence and hatred. We need to bring harmony for the development, progress and happiness of the countrymen.

- Partnership for the Goals: The world is more interconnected than ever. Improving access to technology and knowledge is an important way to share ideas and foster innovation. Stronger partnership will contribute to environment protection and sustainable development. The agenda also promotes support for developing nations. The aim is to manage their debt, promote investment for the growth and development of the country.



INTEXT QUESTIONS 5.2

I. Fill in the blanks:

1. There are Sustainable Development Goals (SDGs), which are an urgent call for action by all countries.
2. By year the United nation has set a target for achieving Sustainable Development goals.
3. We need to give equal opportunity to men and women at workspace.
4. goal ensure equal pay for men and women.
5. Use of energy will help in climate change.

II. Multiple choice questions:

1. Which of the following stands correct for SDGs
 - (a) Improve Education
 - (b) Eradicate poverty
 - (c) Gender equality
 - (d) All of the above
2. The 2030 Agenda for Sustainable Development, adopted by all United Nations Member States in
 - (a) 2014
 - (b) 2017
 - (c) 2015
 - (d) 2020
3. What are the main objectives of sustainability?
 - (a) Improve environment
 - (b) Improve education
 - (c) Improve health
 - (d) All of the above



Notes

4. Sustainable goals addresses to
 - (a) Developing countries
 - (b) Developed countries
 - (c) Poor countries
 - (d) All countries
5. Pillars of sustainable development
 - (a) Society, Economy, Environment
 - (b) Peace, harmony, justice
 - (c) Entrepreneur, stock market
 - (d) None of the above

5.3 21ST-CENTURY SKILLS AND THEIR IMPORTANCE

The entire world has witnessed an era of intense transformation in digital technology, global trade, science, economy, education and innovations. The development of a society, a nation and the world go hand-in-hand with the development of an individual. When a society, nation or world develops, this has a direct impact upon the development of an individual and vice-versa.

21st Century skills : 21st Century Skills are the most essential skill in today's time. These skills are important for better professional, work habits, and character traits that are believed to be critically important to succeed in today's world. They are required to enable an individual to face the challenges of the 21st century world that is globally-active, digitally transforming, collaboratively moving forward and creatively progressing.

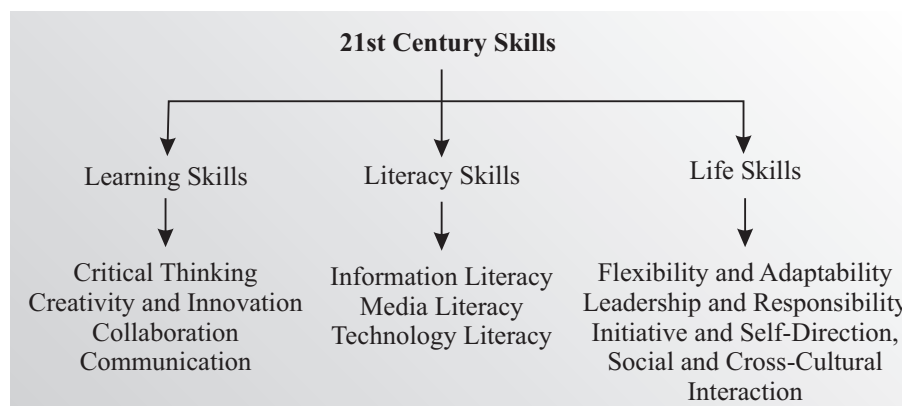


Fig. 5.2: 21st Century Skills

Learning Skills: The most popular 4 C's are part of 21st Century skills.

- **Critical thinking:** Critical thinking is when you find solutions to problems. In critical thinking you question, analyze, interpret, evaluate and come to a solution on your own.



- **Creativity:** Creativity is generating new solutions or ideas of a problem. It is thinking out of the box
- **Collaboration:** Collaboration is working in a team. Collaboration increases productivity and efficiency of work.
- **Communication:** Communication is a way of expressing our thoughts, beliefs. Effective communication is sharing our thoughts, ideas to others and in return get positive feedback or results.

Literacy Skills

- **Information Literacy:** With millions of websites today, there is a lot of information on the internet. Information literacy is the ability to locate, evaluate, use and communicate information efficiently and effectively. Information literate people use information for their learning and growth.
- **Media Literacy:** There are various forms of media through which we get information about the world. Different forms of media are print media, internet media and broadcast media. Media literacy is helpful in assessing and evaluating the information.
- **Technology skills:** This is the most relevant skill of today's time. A person should know the basics of computer, word processing, presentation and spreadsheets softwares. They should know how to search for appropriate information and should be able to work effectively with emails etc. There should be awareness on do's and don'ts of using social media.

Life Skills

- **Flexibility & adaptability:** Adaptability is the capacity to adjust, evolve and succeed in response to changes at the workplace. The faster you adapt yourself at the workplace, the faster your growth starts. You need to understand the working culture and environment. Flexibility is how you change in certain conditions or circumstances at any given point of time. It is how you handle problematic situations, and come out of it with proper solutions.
- **Leadership and responsibility:** Leader is someone who guides, influences, motivates others for the common purpose. Leader takes the responsibility for actions and directions of a team. If a certain assignment was successful, a good leader credits his team. But, he takes the ownership, if in any case there was failure in delivering the assignment.



Notes

Employability and Communication Skills

- **Initiative and self direction:** Initiative is taking charge to solve a problem. It is a quality of an individual to achieve the goals and take the responsibility. Self direction is your inner desire to make your own decisions and organize your own work. Self-direction is achieving the goal with managing time and effort.
- **Social and cross cultural Interaction:** There will be people from different backgrounds and countries. It is the company's effort to ensure that people can work in a diverse environment. Cross cultural interactions open doors for new businesses and job opportunities worldwide.



INTEXT QUESTIONS 5.3

I. Fill in the blanks:

1. Information literacy, media literacy and technology literacy are skills.
2. Working together in a team is
3. Taking charge to solve a problem is taking
4. Generating ideas or new solutions to a problem is
5. Different forms of media are and

II. Multiple choice questions:

1. The 4Cs of 21st century refers to
 - (a) Communication
 - (b) Collaboration
 - (c) Communication, Critical thinking,
 - (d) Creative
2. People from different backgrounds and countries work together in unison is
 - (a) Diverse environment
 - (b) Social and cross cultural interaction
 - (c) Social Interaction
 - (d) Cultural Interaction



3. Flexibility is how you
 - (a) Change in certain circumstances or conditions
 - (b) Handle problematic situation
 - (c) Both a and b
 - (d) None of the above
4. 21st century skills are classified into
 - (a) Learning skill
 - (b) Life skill
 - (c) Literacy skill
 - (d) All of the above
5. A person who guides or motivates its employees is called
 - (a) Leader
 - (b) Manager
 - (c) Boss
 - (d) Colleague

5.4 COMMUNICATION SKILLS

Communication is essential in life. It helps us to connect with others. Just as we need basic facilities such as food, water, shelter, and other basic resources to survive, we need the communication process to succeed in life. We use it to build relationships, share information, and resolve conflicts. Communication is more than just a way to express our thoughts and feelings. It helps us to learn things better. Communication is very important in the workplace or in business. It is very essential to communicate with colleagues, customers and other people we meet.

There are 5 elements of communication:

- **Sender:** Sender is one who initiates the communication process
- **Receiver:** Receiver is who receives the message from the sender.
- **Message:** Message is what is to be communicated.
- **Channel:** Channel is a medium of communication.
- **Feedback:** Response of receiver to the sender.

We communicate with each other by speaking, writing, facial expressions, body language, gestures, using symbols etc. There are two types of communication: verbal and nonverbal.



Notes

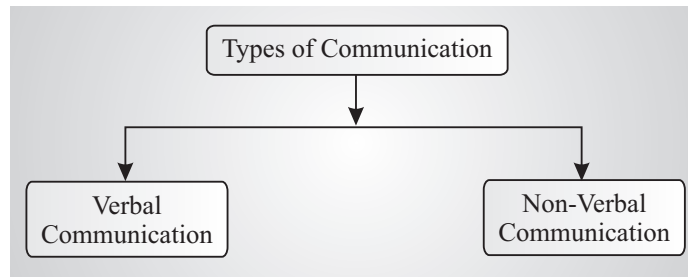


Fig. 5.3: Types of Communication

Verbal Communication: The term ‘verbal’ means by using words and language. Verbal communication is sharing our ideas, information, suggestions, thoughts and feelings either in oral or written.

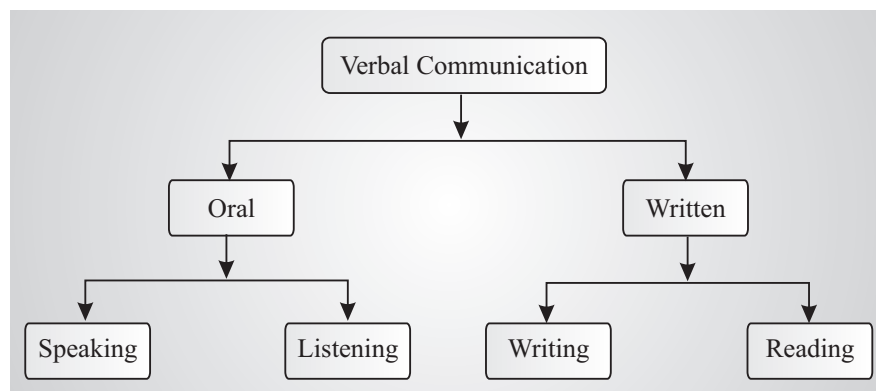


Fig. 5.4: Verbal Communication

- **Oral:** To communicate orally one should possess good command in language. There should be clarity in voice and a person should be able to express ideas clearly and effectively. Oral communication is of two types:
 - **Speaking:** Face-to-face conversations in meetings, group discussions, seminars, presentations, video conferencing, telephonic conversations etc.
 - **Listening:** Active listening can help you to understand what others are saying in conversations and meetings. Look at the speaker and nod or smile that you are listening. Evaluate the conversation and if required ask questions.
- **Written:** Written communication is an important aspect of today's communication. Exchange of information can be either printed or handwritten. Well maintained written records are permanent evidence for the future and at any point of time for reference. It promotes uniformity in policies and procedures.



- **Writing:** Written communication can be done through letters, emails, messages, contracts, forms, quotations etc.
- **Reading:** Reading is a process of constructing meaning from the written text either printed or through digital media. It can be in the form of books, magazines, graphs, charts, websites, emails etc.

Non-Verbal Communication: Non verbal communication is communicating without using words or language but with body language, gestures, eye contact, facial expression etc. To communicate effectively using Non-Verbal communication, one should:

- Maintain eye contact
- Modulate voice tone
- Maintain Proper distance
- Smile when required
- Maintain good body posture
- Physical appearance



INTEXT QUESTIONS 5.4

I. Fill in the blanks:

1. Body language is type of communication.
2. A person who initiates the communication process is
3. is just a way to express our thoughts and feelings.
4. It is preferable not to interrupt someone while
5. Email is a type of communication.

II. Multiple choice questions

1. The process of exchanging information between individual or a group is
 - (a) Transmission
 - (b) Communication
 - (c) Formal communication
 - (d) Informal communication
2. Which of the following is an example of non-verbal communication
 - (a) Speaking
 - (b) Listening
 - (c) Reading
 - (d) Body Posture



Notes

3. Active listening is
 - (a) Paying attention to the speaker
 - (b) Asking questions
 - (c) Using mobile phone
 - (d) Avoiding eye contact
4. Written communication is
 - (a) Communication over video call
 - (b) Sending an email
 - (c) Attending meeting
 - (d) Telephonic conversation
5. Which communication skill requires a voice tone and clarity
 - (a) Listening skill
 - (b) Reading skill
 - (c) Verbal communication
 - (d) Non-verbal communication

5.5 JOB AND BUSINESS OPPORTUNITIES

5.5.1 Identify Business Opportunities

The first and most important step in the entrepreneurship journey is identifying a business opportunity. Starting your own business requires lots of hard work, dedication, commitment, and focus. There are many areas where one can look for potential business opportunities. Some of the areas where some significant domains exist are as follows:

- **Environment:** Opportunities with respect to sustainability, renewable energy, and eco-friendly products or services
- **Education:** New ideas of teaching methodologies, online courses or educational tools
- **Import/Export:** In International Trade, it involves importing foreign products or exporting the local product into foreign markets
- **Technology:** Any new advancements related to software or hardware, also newer technologies are AI, Blockchain, IoT etc.
- **Health:** Medical healthcare innovations, wellness products or services to take care of human beings' health and well-being.
- **Transport:** Logistic and other environment-friendly transportation and delivery services



- **Services:** Those services will be provided which would cater to the customers' requirements like personal grooming, domestic or home upkeep services, and even business consultation
- **Digital Products:** Digital products may include making an application or building a web service, selling media content.

5.5.2 Identify Different Types of Financial Products and Service

Financial services refer to the mobilization and allocation of funds to sectors that require them. These services are essential in boosting economic growth and development since they support investment, facilitate domestic and international trade, and ensure the smooth flow of capital. Some of the key areas within financial services include:

- **Banking:** This is providing financial services such as saving accounts, loans, and credit facilities to individuals and businesses.
- **Insurance:** Covers risks and uncertainty of financial nature through different kinds of insurance policies.
- **Investment Services:** Provides people and businesses with avenues to invest and manage finances in a number of asset classes.
- **Real Estate:** Involves buying, selling, or renting residential or commercial properties.
- **Financial Products** are instruments through which individuals and businesses can invest, borrow, or save money. These products are issued by banks, financial institutions, governments, or companies. Some common financial products include:
 - **Shares:** Ownership stakes in companies that are bought and sold on stock exchanges.
 - **Mutual Funds:** Investment vehicles that pool funds from multiple investors to invest in a diversified portfolio of stocks, bonds, or other assets.
 - **Fixed deposits:** investment products supplied by banks for depositing money for a period of time at an agreed-on interest rate .
 - **Consumer loans:** loans given to customers for personal use. There include the loans used by customers to purchase their cars or to renovate their houses.



Notes

- **Credit cards:** financial services that enable individuals to borrow up to a specified amount to buy goods and repay borrowed funds.

Together, financial services and products offer the core infrastructure for all economic activities by ensuring that all aspects of financial life are well-managed.

5.5.3 Compute Income and Expenses

Computation of total income refers to the sum of all money received from business activities.

Any money incurred to run a business is known as expense.

Net income is total income reduced by total expenses.

Gross income = Sum of all money earned

Gross Expense = Sum of all money spent

Net income = Gross income - Gross expense

5.5.4 Maintaining Safety and Security in Financial Transactions

It is very important to maintain safety and security in financial transactions. Now a days people are doing most of the financial transactions online. We need to be careful while doing any transaction online. As due to our negligence we might lose our hard earned money during online transactions. To maintain safety and security in financial transactions one should:

- (a) Install Antivirus and antispyware software.
- (b) Create a strong password.
- (c) Don't share passwords with anyone and don't keep it on the web.
- (d) Do transactions only on Secure websites
- (e) Do not use public wifi.

5.5.5 Different Legal Rights and Laws

Law is an official rule of a country or state that says what people may or may not do.

Rights are the actions which are allowed to any person to do in state or country (jurisdiction of the law). Rights are social, ethical or legal. There are various kinds of rights provided to citizens in our country like fundamental rights, constitutional rights, human rights, civil rights and legal rights. These are recognized and protected by law.



Rights which are legally protected by any law are known as legal rights. Legal rights are enjoyed by the citizens of the country to freedom without fear or favor. Some legal rights are valid for each countrymen but some legal rights are valid for particular states. Various legal rights enjoyed by the citizens are:

- **The Equal Remuneration Act 1976:** It is the duty of employers to pay equal remuneration to men and women workers for the same work or work of similar nature. There should be no discrimination while recruiting men and women workers.
- **Civil Rights:** This right is given to an individual for freedom of speech, religion, assembly and other fundamental liberties.
- **The Right to a fair trial:** Under our Indian constitution, the right to get a fair trial is a basic fundamental human right. He has the right to defend himself.
- **Inheritable and non-inheritable rights:** A right is inheritable if it survives even after the person dies. A right is non-heritable if a person dies.
- **Proprietary and personal rights:** Proprietary rights includes a persons assets and his property. Proprietary rights are valuable and have monetary value. Personal rights are merely elements of well being .

5.5.6 Operate Digital Devices and Applications Safely and Securely

- While using any digital device such as Mobile phones, laptops, computers, tablets etc, make sure it is password protected. The password should be strong and difficult to crack.
- The online transaction applications such as UPI, Paytm, Google Pay, Phone pay etc. should be opened by entering a password or using fingerprint.
- Anti virus and anti spyware softwares should be installed to remove viruses and unwanted adverts.
- Wifi should be password protected. Abstain yourself from using public wifi.
- Avoid storing sensitive details on the cloud.
- Beware of suspicious mails and do not open it or an attached file .
- Lock your device when you are away from it.

5.5.7 Types of Customers and their Needs

Customer is one who buys something in exchange for money or for something else. Customers play an important role in the business. There are various ways to deal with different types of customers. Various types of customers are:



Notes

1. **New Customer:** New customers make their first purchase and initiate a relationship with the company. Adding new customers is very important for the growth and expansion of a company. If they are satisfied with the product or the services, their association starts with the company.
2. **Potential Customer:** Potential clients are those who are likely to buy a product or avail a service. The company should try by different means to make him a customer.
3. **Loyal Customers:** Loyal customers are those who have built faith and are satisfied with the company. They buy or avail service as and when required.
4. **Impulsive customers:** Impulsive customers are those who buy without planning for the same. They are quick decision makers.
5. **Discount Customers:** Discount customers are one who always look for discounts to make a purchase. They are reluctant to buy without discounts.
6. **Need Based Customers:** Need based customers are those who purchase if they really need it.
7. **Knowledgeable Customer:** Knowledgeable customers are those who have complete knowledge of the product or service and do not need guidance or motivation for the purchase.
8. **Angry Customer:** Angry customers are those who are unhappy with the product or service.

5.5.8 Process of Application for a Job and Interview Preparation

Process of Application for a Job: There are various things you have to keep in mind before applying for a job through newspapers, job portals, links from family and friends etc.

- **Self assessment:** It is a tool to reflect your career progress, achievements, accomplishments, skill development. It helps in identifying your skills, strengths, interest and personal value. This will help in choosing the right job.
- **Preparation of resume:**
 - Choose the best format for your resume.
 - Brief summary about yourself.
 - Add complete personal details.
 - Include all educational details.



- Add professional details
 - List the relevant skills
 - List the work experience in descending order.
 - Highlight the achievements or awards.
- **Drafting a cover letter to a resume:** A cover letter is a document submitted with the job application showing interest in the open position.

Interview Preparation: To walk for an interview one should keep following things in mind.

- Review the job profile.
- Research about the company.
- Prepare the key points about yourself to communicate to the interviewer.
- Dress professionally.
- You should know your strengths.
- Be punctual.
- Enter with a positive attitude and smile and be confident.
- Listen carefully to the interviewer's questions and then answer them.



INTEXT QUESTIONS 5.5

I. Fill in the blanks:

1. The financial that are made available to sectors in need.
2. A customer is likely to buy a product or avail a service.
3. It is not advised to do transactions using public wifi.
4. Right to pay equal remuneration to men and women is
5. One who sets his own business is called an

II. Multiple choice questions:

1. Resume should include
 - (a) Work experience
 - (b) Relevant skill
 - (c) Educational qualification
 - (d) All of the above.



Notes

Employability and Communication Skills

2. A person who does not need any guidance for buying a product is
 - (a) Need based customer
 - (b) Knowledgeable customer
 - (c) Impulsive customer
 - (d) None of the above
3. On finding suspicious mail
 - (a) Open it at once
 - (b) Open the attached file
 - (c) Delete it immediately
 - (d) None of the above
4. Which one is a “Do’s” for interview
 - (a) Nervousness
 - (b) Be confident
 - (c) Dress casually
 - (d) Excessive gesture
5. A person who is associated of starting a business is
 - (a) Executive
 - (b) Manager
 - (c) Entrepreneur
 - (d) Employer



WHAT HAVE YOU LEARNT

- Employability skills are the essential skills that enable you to thrive in any workplace. It is a combination of soft and hard skills.
- Organizations look for people with Good oral and written communication skills, Leadership Qualities, Critical thinkers & Problem solvers, Positive attitude etc.
- Sustainable Development, adopted by all United Nations Member States in 2015, is a step ahead for peace and prosperity for people and the planet, now and into the future. There are 17 Sustainable Development Goals (SDGs), which are an urgent call for action by all countries - developed and developing - in a global partnership.
- Sustainable development goals related to employability skills are Decent work and economic Growth, Industry, innovation and infrastructure, Quality Education, gender equality, Peace, Justice and strong institutions and partnership for the goals.
- 21st Century Skills refer to the skills that are required to enable an individual to face the challenges of the 21st century world.

Employability and Communication Skills



Notes

- 21st century skills are broadly classified into learning Skills, literacy Skills and life Skills.
- Most popular 4 C's are part of 21st Century skills are Critical thinking, Creativity Collaboration and Communication.
- Communication is of two types, verbal communication and non verbal communication.
- Verbal communication is sharing our ideas, information, suggestions, thoughts and feelings either in oral or written. It is of two types: oral and written.
- Non verbal communication is communicating without using words or language but with body language, gestures, eye contact, facial expression etc.
- Business opportunity is an idea or a set of circumstances that make it possible to develop a profitable and sustainable business.
- Financial services refers to mobilizing and allocating services. These funds are made available to sectors in need like Banking, Insurance, Investment Services, Real estate etc.
- Financial Products is an instrument in which a person can make an investment, borrow or save money for example Shares, Mutual funds, Fixed deposits, Consumer Loans, Credit cards etc.
- Maintaining safety and security in financial transactions is very important. Follow some safety measures when doing transactions online.
- Law is an official rule of a country or state that says what people may or may not do. Rights are the actions which are allowed to any person to do in state or country. Rights which are legally protected by any law are known as legal rights for example The Equal Remuneration Act 1976, The Right to a fair trial, Civil rights, Inheritable and non- inheritable rights, Proprietary and personal rights etc.
- Job interview is an opportunity to present your skills, knowledge and experience to the interview panel. Be calm and confident and carry a positive attitude.



TERMINAL EXERCISE

1. Why are employability skills important?
2. What are sustainable development goals?



Notes

Employability and Communication Skills

3. Explain 4 C's of 21st century skills?
4. Write the difference between verbal and non verbal communication.
5. What is a business opportunity?
6. Who is an entrepreneur?
7. Explain any two legal rights in brief.
8. List the important points for creating a resume.
9. How are technology skills important for us?
10. Who is a potential customer?
11. What is media literacy?
12. What are the benefits of oral communication?
13. How is positive skill important for employees?
14. What are soft skills?
15. How are new customers beneficial for us?
16. Explain different elements of communication?
17. What can we do to make secure online transactions?
18. Explain The Equal Remuneration Act 1976.



ANSWERS TO INTEXT QUESTIONS

5.1

- I.**
- | | |
|----------------------|--|
| 1. Hard | 2. Good oral and written communication |
| 3. Critical Thinking | 4. Leader |
| 5. Employee | |

- II.**
- | | | | | |
|--------|--------|--------|--------|--------|
| 1. (b) | 2. (c) | 3. (d) | 4. (c) | 5. (c) |
|--------|--------|--------|--------|--------|

5.2

- I.**
- | | | |
|----------------------------------|---------|--------------------|
| 1. 17 | 2. 2030 | 3. Gender equality |
| 4. Decent work & Economic growth | | |
| 5. Renewable sources | | |

Employability and Communication Skills



Notes

- II.** 1. (d) 2. (c) 3. (d) 4. (d) 5. (a)

5.3

- I.** 1. Literary skill 2. Collaboration
3. Initiative 4. Creativity
5. Print media/ internet media / broadcast media

- II.** 1. (d) 2. (b) 3. (c) 4. (d) 5. (a)

5.4

- I.** 1. non-verbal 2. sender 3. communication
4. speaking 5. Written

- II.** 1. (c) 2. (d) 3. (a) 4. (b) 5. (c)

5.5

- I.** 1. Services 2. potential 3. online
4. The Equal Remuneration Act 1976
5. Entrepreneur

- II.** 1. (a) 2. (b) 3. (c) 4. (b) 5. (c)

Key Learning Outcomes

- Explain the significance of employability skills in the workplace and career development.
- Describe 21st-century skills and their importance
- Illustrate effective communication
- Identify different types of financial products and services



6

FUNDAMENTALS OF CYBER SECURITY

Technology has penetrated in every sphere of our life. Computers, laptops, mobile phones, and other digital devices have changed the way we lead our personal and professional lives. On the positive side, it has improved communication, business, education, entertainment, governance, and many more for us but on the other side, it has also made us vulnerable to a wide range of cyber crimes. As the world around us is adapting to new forms of technology, every individual or organization should take measures to protect their personal information, identity, and finances from potential cyber crimes or threats. Online threats or cyber threats include data breaches, malware, viruses, and other malicious activities that can lead to financial loss or reputational damage. Therefore, it is crucial for all of us to understand what cyber security is, why it is important, and how we can protect ourselves from potential cybercrimes.

Cyber security is the combination of technologies and practices that keep the digital devices, networks, programs, and data safe from unauthorized access or any kind of malicious attack. Cyber security helps to protect against such threats and risks by using various protection measures:

- Hardware security measures such as firewalls
- Software security measures such as antivirus
- Encryption techniques that can help protect data from unauthorized access.
- Authentication protocols, access control systems, and monitoring tools
- User education programs that educate people about cyber hygiene, that refers to some best practices to keep oneself safe online.



OBJECTIVES

The learner will be able to:

- define Cybercrime
- identify Information Security concepts like CIA, Authentication and Authorization.
- recognize computer ethics
- distinguish between ethical and unethical behaviour.
- distinguish among Internet, Intranet and Extranet
- explain malware, its types and prevention
- categorize various cyber attacks
- define plaintext and ciphertext
- explain cryptography and its types

6.1 CYBERCRIME

Cybercrime is an unlawful act that is committed or facilitated using digital device(s) and/or a network including Internet. The digital device may be used for the execution of the crime, may be a target, or may be used to spread malware to other machines on the network. A cybercrime may be committed by individual(s) or organization(s) with financial gain as the primary motive. However, it is also done to damage someone's reputation or for political gains. Each one of us should understand that when we are online, any one of us can be potential target, and so we should take adequate measures to protect ourselves.

6.2 INFORMATION SECURITY

A cyber-attack may disrupt the normal flow of work, cause financial losses or damage to reputation of an individual or a company. Information Security (abbreviated to Infosec), are the practices and tools that an individual or an organization must implement to protect print, electronic, or any other form of confidential, private, or sensitive information from unauthorized access, use, alterations, destruction, disclosure, or disruption. The data, such as customer account details, financial details or even any type of intellectual property must be protected when it is stored or when it is being transmitted from one location to another. Information Security encompasses a wide range of fields, from network and information security to testing and auditing. The policy settings that are made



Notes



Notes

to prevent unauthorized people from accessing data also comes under Information security. The organizations must understand the importance of information security and must take steps to detect, respond to, and proactively prevent any type of cyber-attack.

6.2.1 Principles of Information Security

The basic principles or tenets of information security are confidentiality, integrity, and availability. Together, they are known as **CIA** triad. Every element of information security program must make sure to implement these principles.



Fig. 6.1: Principles of Information Security

<https://www.google.com/url?q=https://www.geeksforgeeks.org/the-cia-triad-in-cryptography/&sa=D&source=docs&ust=1712824883689688&usg=AOvVaw0RSnKwBdJVzwcwjkr2xnddE>

- **Confidentiality:** This principle ensures that confidentiality of data is maintained. The personal information is kept private and is made visible or accessible to only those people who are authorized to access. Therefore, to ensure confidentiality, we need to identify who is authorized to access data and block the attempts made by any unauthorized person or organization. The methods used to ensure confidentiality are allocating user ids and passwords, encrypting data, authentication, etc.
- **Integrity:** The principle of integrity ensures that data is always accurate and is not incorrectly modified. Any kind of incorrect modification may be done accidentally or with malicious intent. Practices such as frequent backups can help to restore and verify the data integrity.
- **Availability:** This principle of information security makes sure that software systems and data are available to users who have permission to access data. Also, the data should be available as per the requirement at any time. Availability is the mirror image of confidentiality. While the former makes the



data accessible to only authorized users, the latter makes sure that the information is kept private from unauthorized users. By ensuring data availability, a good backup policy is also ensured.

Ideally, data should always be kept confidential, in the correct state, but at the same time, it should be always available to authorized users. However, depending on the type of data, emphasis may be given to one or more principles of information security. For example, any one's medical information must be kept confidential while in case of financial data, both confidentiality and integrity of data have to be given equal importance.

6.2.2 Authentication and Authorization

Authentication and authorization are two very commonly used words in information and cyber security. Authorization and authentication work together so that the system knows who is accessing and what information is being accessed.

Authentication is the act of validating a user's identity on a network or a device. It is the first step in any security process that ensures that the person trying to gain access is the same that he/she is claiming to be. The authentication by server is done by using username and passwords, access cards, retina scans, voice recognitions, fingerprints, etc. Sometimes, a one-time pin or OTP is used to grant access to only one session or transaction. Authentication only confirms the identity of the user. It does not ensure the tasks a user can do or the data that he/she can access. As per the type of application to be accessed and the security levels that are to be applied, there are following types of authentication factors:

- **Single-Factor Authentication:** This is the simplest way of authentication and just needs a username and password to access any device or network.
- **Two-Factor Authentication:** This is a two-level security authentication process. Therefore, it needs two-step verification to authenticate a user. In addition to user name and password, it also requires additional information that is known only to that specific user. This can be done by sending OTP to the user's registered mobile number or email address or by asking specific questions such as the first vehicle's registration number, pet name, mother's year of birth, first company, etc.
- **Multi-Factor Authentication:** This is the most secure type of authentication. It requires two or more than two levels of security that may be related to each other or may be independent. It is usually used at places that store highly sensitive or confidential data such as in government agencies, banks, and other financial institutions. In this type of authentication, username and password, OTP, security questions, and biometrics may be used to verify the user.



Notes

Some of the commonly used authentication techniques are:

- (i) **Password based authentication:** In this technique, the user is successfully authenticated if the username and password match the system's database.
- (ii) **OTP Based authentication:** The user gets an OTP or link in her/his registered mobile number or email address. The user is successfully authenticated if the correct OTP is entered.
- (iii) **Two-Factor or Multi-Factor Authentication:** In this technique, in addition to username and password, either an OTP or correct answer to certain specific security questions is required to authenticate a user.
- (iv) **Single Sign-On:** It allows authentication to multiple applications with a single sign in. For example, you may sign in just once to Google to access your mail, drive, photos, etc.
- (v) **Social Authentication:** This authenticates the user with existing credentials available on the social network. For example, you may login to an application with your Facebook account.

Authorization is the process of checking whether the user has valid permission to access a specific resource or not. Basically, it defines what data and information a user can access. For example, permission to download a particular file from the server or providing administrative access to a user in an organization. However, some data on the Internet, such as maps, government policies, legal provisions, employment status, etc., can be accessed without any authorization. Such type of data is available for all. But the data that is specific to an organization must be authorized both for viewing and editing. Some of the commonly used authorization techniques are as follows:

- **Role-Based Access control (RBAC):** Using this technique, each user is given access according to his/her role or profile in the organization. For example, a student is given access to only his/her result but a teacher is given access to the result of all students in the class.
- **JSON Web Token (JWT):** It is an open standard in which the users are verified and authorized using private/public key pairs. It is used to securely transmit data between two parties who have to login using a valid key pair to access and use a particular resource.
- **Security Assertion Markup Language (SAML):** In this open standard authorization technique, the authorization credentials are provided to the service providers. These credentials are exchanged through digitally signed XML documents.



- **OpenID Authorization:** This technique is used to verify the identity of end-users based on any type of authentication.
- **OAuth:** This technique uses an authorization protocol that enables the API (Application Programming Interface) to authenticate and access the requested resources. For example, WhatsApp is given permission to access photos from your device.

For complete information security, authorization must follow authentication. The users should first prove their identities and then the administrators of the organization check the permissions to access the requested resource or data.



Fig. 6.2: Authentication and Authorization

Table 6.1: Difference between Authentication and Authorization

Authentication	Authorization
Process of identifying a user to give him/her access to the network or device.	It is the process of giving permission to access the resources or data
Both user and server are verified	The server verifies whether the user is allowed through the defined policies and rules.
It is performed before authorization	It is usually done after successful authentication
It requires login details of the user such as user id, password, finger prints, face id, etc. Mostly, these details can be changed by the user.	This defines what all types of access a user can be given. For example, permission to view data or to modify data. Authorization permissions cannot be changed by the user. It is the manager of the organization who can change the authorizations.
Example: To access the portal of an organization after entering valid user id and password	Example: After the employee logs in, what all files they can access for viewing or editing.



6.3 COMPUTER ETHICS

Computer ethics are a set of moral values and practices that address the ethical issues and constraints that arise from the use of technology. The digital devices, especially on a network, should be used without damaging or violating the moral values and beliefs of any other individual or organization. Computer ethics lay down such behaviour and approach that should be followed by all netizens. The core issues surrounding computer ethics are based on software piracy, privacy, copyright and trademark infringement, and social interaction with users over the websites and related services. Further, it also includes that people who are building technology, such as computer programmers, should work in public interest with due regard to security, privacy, environment, and public health.

Another term that is closely related to computer ethics is Internet Ethics, that is the acceptable behavioural code that should be followed when using the Internet. In simple terms, it is the manual code of conduct that is acceptable on the web. The Internet should not be used as a tool to favour or defame a particular person or a section of society, especially by the developers and administrators of the Internet. With the increased use of technology including Internet, social media, and artificial intelligence, following ethical concerns have arisen and need due attention by all of us:

- **Cybercrime:** It includes hacking, identity theft, theft of intellectual property, injecting malware, such as viruses, worms, trojans, etc. and much more.
- **Privacy and Security:** Online privacy is one of the most common concerns among the users. This includes stealing personal, confidential, or sensitive data and using it for malicious purposes. The act of tracking someone's online activity, cyber bullying, or cyber stalking, is also a rising ethical concern among the netizens. On the larger perspective, the collection and usage of big data affects various decision-making processes such as insurance claims, stock market updates, and even political announcements. Therefore, such data must be handled with safety and integrity. That is why the netizens want to be aware about why and how their data is being collected by various organizations.
- **Intellectual Property:** Enormous amount of digital content of all types is available on the Internet. With almost all art forms being digitized and shared online such as paintings, literary works, software codes, movies, music, protection of original work is a cause of concern for digital users.
- **Net Neutrality:** The people and organizations who are responsible for development and functioning of the Internet should allow the information on



the Internet to flow freely. They should not encourage or emphasize a particular content. Similarly, the people responsible for collecting and analysing big data should use such data ethically and with integrity. Therefore, maintaining neutrality of the Internet is also an ethical concern these days.

6.3.1 Ethical Behaviour on the Internet

While using any digital device online, it is important to respect privacy, intellectual property, and digital rights of other users. Following are some of the ethical practices that should be followed by all netizens:

- Respect the privacy of all users and policies governing intellectual property.
- Request for permission before using any other user's device or resources.
- Do not use your device to harm others or to steal someone's intellectual property such as music, photographs, software codes, etc.
- Each user should be responsible enough to safeguard their personal information.
- The people with technical expertise should always act with integrity, and in the best interest of their client, organization, and society at large.
- Report illegal or unethical activities to the appropriate authorities.

6.3.2 Common Unethical Behaviour on the Internet

Although the guidelines have been laid down for ethical usage of technology, certain unethical practices are not uncommon. Some of these include identity theft, software piracy, financial theft, intellectual theft, etc. We will learn about these in the due course of chapter.



INTEXT QUESTIONS 6.1

A. State whether the following statements are true or false:

1. A cyber crime is committed only for financial gain.
2. The principle of integrity in CIA Triad ensures that personal information is made visible to only authorized users.
3. Authentication defines what data and information can a user access.
4. JWT is an open standard in which the users are verified and authorized using private/public key pair.
5. A piece of music posted online is an example of intellectual property of the composer.



Notes

B. Mention which of the following behaviour on the Internet is ethical/unethical.

1. Requesting for permission before using any other user's device or resources.
2. Posting your best friend's photograph without her consent.
3. Downloading and using videos after taking permission from the creator.
4. Stealing data from your colleague's pen drive and posting it on social media.

6.4 MALWARE

Malware or Malicious Software is an umbrella term that describes any program or code that is meant to harm the digital devices in any manner. The cyber criminals develop malware with an intention to steal, encrypt, or delete data, to disable or destroy digital devices and networks, or even to spy on any user's digital activity. Some of the common examples of malware include viruses, worms, trojan horse, spyware, adware, and ransomware.

These days, as most of the malware is embedded through the Internet, anyone who is online, is vulnerable to malware attacks. Some of the actions by which a malware can quietly penetrate to the victim's device are:

- surfs through hacked websites
- clicks on any pop-up ad in the browser
- clicks on any malicious link that comes in the email
- opens a malicious email attachment
- downloads infected files
- installs software and apps from unfamiliar websites
- plugs in infectious USB drive

Although one needs to have a sharp eye to detect a malware on his/her system but many times, a malware lies undetected in your device, keeping track of your activity. Still, the following signs may signal a malware attack on the device and hence should never be ignored.

- The computing device slows down.
- Problems with shutting down or starting up the computer.



- Frequent and annoying pop-up ads coming up on the screen.
- The system crashes suddenly.
- Mysterious loss of disk space.
- Sudden increase in the system's Internet activity.
- Change in browser settings that have not been done by you.
- The browser automatically takes you to websites that you do not intend to use.
- Antivirus stops working and it cannot be turned on.
- You are unable to access the files or any of the resources on your device.

6.4.1 Types of Malwares

Certain common types of malwares are:

1. **Virus:** A virus is a program code that is embedded or attached to a file. Once the infected file is downloaded, the virus also gets downloaded. But it will remain dormant until the host file is opened on the infected device. A virus is programmed to disrupt the normal functioning of the computer, hence causing significant data loss or damage to the system. Some of the common types of virus are:

Boot Sector virus: It affects the master boot record of the digital device. This gives rise to problems such as inability to boot or start the system, unable to locate the hard disk or poor system performance. Examples of boot sector viruses are disk killer and stone virus.

Macro virus: It affects spreadsheets, documents, and other data files by inserting malicious codes in the macros associated with the development of these software. These corrupt data, insert words and pictures, move text, or even format hard drives. Melissa virus is a common example of a macro virus.

Memory Resident virus: It is one that lives in primary memory or RAM and gets activated as soon as the system is switched on and the operating system is loaded in the primary memory. All the files that are currently running on the desktop are affected. Common examples are Randex and Meve.

Web Scripting virus: This type of virus breaches the inbuilt security of a web browser and injects the malicious code to alter some browser settings. It mostly affects the social networking sites and spreads with the help of pop-up ads on web pages. Some examples are DDoS and JS.fortnight.

2. **Worm:** A worm is a type of malware that generally affects the devices on a network. These multiply and disperse at an exponential rate but they do not need any host program to spread the infection. Due to overload, the network



Notes

Fundamentals of Cyber Security

resources are depleted thereby affecting the efficiency of the network considerably such that the server has to be shut down. They may also lead to damage or loss of data. Some examples of worms are Code Red, ILOVEYOU, and Morris.

3. **Trojan Horse:** A trojan horse, or simply trojan is a malicious program that is disguised as a helpful program but it harms the system. Once the user downloads the trojan, it can modify or destroy files, gain access to confidential data, or even crash the device. Unlike viruses and worms, trojans cannot self-replicate. The users are tricked into clicking on malicious links and attachments that are disguised to appear as genuine. Examples of trojans are ProRat, Beast and Zeus.
4. **Ransomware:** This is a type of malware that gains access to confidential and important information from a digital device. Thereafter it encrypts that data and the victim can only open it by using the mathematical key known only to the attacker. Hence, the attacker demands ransom or money, usually in bitcoins, to decrypt and release the data back to the victim. A ransomware gets downloaded when one clicks a fraudulent link that may be part of a phishing email. This is one of the most profitable malware, and hence is rapidly gaining popularity. Some examples of ransomware are BitPaymer, Maze, and DarkSide.
5. **Spyware:** A spyware is a malicious software that secretly runs on the victim's device without his/her explicit knowledge, and is used to steal personal and financial information of the victim. Although it is used by law enforcement agencies and security organizations for investigations, it is also used by cyber criminals to steal sensitive information. It keeps track of the user's activity on the browser to gain sensitive information such as usernames and passwords. Keylogger is a common type of spyware that records keystrokes on your system to record passwords and personal information.
6. **Adware:** An adware is a malicious software that tracks the user's browsing activity and then pops up unwanted blinking ad pop-ups when the user is online. Generally, an adware does not harm the system but they can redirect the user to fraudulent websites that can contain trojans and worms. An adware may slow down the victim's system.
7. **Fileless Malware:** This is the latest form of malware that uses legitimate programs to infect a device. It operates from the victim's computer's memory and not from the hard drive. The fileless malware leaves no digital footprints – no files to scan or no malicious process to detect. Hence these are very difficult to detect and remove. Further, the malware disappears when the victim's system is rebooted. DNSMessenger is an example of fileless malware



6.4.2 Prevention of Malware

The netizens can prevent their device from a potential malware attack by following some simple tips:

- Always keep the operating system and all other applications updated. The cyber criminals look out for vulnerabilities in the old and outdated systems while planning an attack.
- Never click on any link in the pop-up window that appears in the browser. Simply click on the 'X' button on the top right corner of the pop-up.
- Use a limited number of apps on your device. Install only those apps that are being used and uninstall all others.
- Always use strong passwords that cannot be guessed easily by anyone.
- Enable multi-factor authentication to safeguard your accounts.
- Back up your data regularly.
- Make sure all devices – computers, laptops, or mobile devices, have an updated antivirus installed on them. Preferably, enable firewall protection as well. Run virus and security scans regularly.
- Do not lend your device to anyone or leave it unattended for any reason. If your device settings have changed or any of your apps have mysteriously disappeared, it might be a sign that some malware has been installed.
- Avoid clicking on unknown links – it may be posted via a simple text message, an email, or any social networking application.
- Visit only trusted sites and avoid websites that give freebies, such as free screensavers.
- Beware of emails requesting personal information. Even if an email comes from your bank asking to click on the given link to change your password or any other setting, do not do it. Go to the official banking site, verify the request, and then do the needful from that trusted site only.
- Always download software and apps from official app stores or only from official trusted sources.
- Do not open an email attachment unless you know what it is about, even if it comes from your known ones.
- Check your bank account and credit card statements regularly



Notes

- Stay informed and educate others about potential online threats and the preventive measures to protect from such threats.

In a nutshell, we can say that malware prevention requires vigilance. The practices listed above ensure the safety of personal information, financial assets, and sensitive and confidential data.

6.5 CYBERATTACKS

A cyberattack is an intentional effort to steal, modify, damage, or destroy data or any other resource on the network. With the advancement of technology, the cyber criminals are becoming more and more creative with their attacks. As a netizen, one should be aware of all prevalent cyberattacks. The knowledge of these attacks is the best means to protect ourselves. Some of the common forms of cyber-attacks include the following:

6.5.1 Hacking

Hacking is one of the most common forms of cybercrime. The persons who commit the crime of hacking are known as hackers. As we know, a computing device stores a lot of sensitive and personal information of an individual or an organization. In fact, these days much of the data is virtually stored on the cloud as well. Hackers gain access to systems or networks without necessary permissions and authentications. They then cause data theft, system disruptions, and even injection of malware. This is done for monetary benefits or to settle business or political rivalries. The Swachh City platform, an initiative associated with Swachh Bharat Mission was hacked in September 2022, putting data of its 16 million users at risk. The database was then put on sale on the dark web.

6.5.2 Malware Attacks

A malware attack is a software-based attack where any form of malware – viruses, worms, trojans, ransomware, adware, spyware, or fileless malware can be used to harm a digital device or a network. We have studied malware and its types in the previous section of this chapter.

6.5.3 Denial-of-Service (DoS) Attacks

A Denial-of-Service (DoS) attack is one in which the attacker blocks the access to data and/or resources for the owner of the computing system, network, or resource.

A **Distributed Denial-of-Service (DDoS)** attack is a type of cybercrime that is committed to bring down a complete system, server, or a network. It tries to make



an online-services unavailable for its users by spamming with numerous connection requests. The huge network traffic leads to complete exhaustion of bandwidth such that the service becomes inoperable. To bring back normalcy, the cyber attackers may demand money, usually in bitcoins. Sometimes, such types of attacks may also be used as a distraction to commit some other crimes. IoT (Internet of Things) devices are used to carry out such attacks. These types of attacks are becoming increasingly common. According to a report, 16 lakhs DDoS attacks were attempted on the G20 website in the year 2023.

6.5.4 Phishing, Vishing, and Smishing

These are the types of attacks in which the user is coerced to give its own personal and confidential information such as bank account details, ATM PINs, credit/debit card details, etc. to the attacker. Phishing is a type of cyberattack in which fraudulent emails and websites that appear to be legitimate are used to trick individuals into revealing personal information. The phishing emails may contain infectious attachments or links to malicious websites, or they may directly ask to reveal confidential information. Spear Phishing is a type of phishing in which the employees of an organization are targeted through emails that seem to come from a trusted source, such as the CEO or IT Manager of the organization.

Vishing is an attempt by cyber criminals to seek personal information through phone calls. They entice the person by luring them into a good deal, a lottery, or some prize money and then winning their confidence. Thereafter, the victims themselves divulge their personal information that is then used by attackers for malicious purposes.

Smishing is a type of cyberattack that tricks people by sending text messages that contain either a fraudulent number for the victim to respond back or link to a fraudulent website or to download malicious software via phone or web.

6.5.5 Spoofing

Spoofing is a type of cyberattack in which the attacker pretends to be a trusted entity and motivates the victim to do something that is beneficial for the attacker. This disguise may be done to steal money, steal data, spread malware, or gain access to the systems. The attackers usually encash on human vulnerabilities such as fear, greed, or lack of technical knowledge. There can be various kinds of spoofing attacks such as text message spoofing, email spoofing, website spoofing, caller id spoofing, etc.

6.5.6 Identity-Based Attacks

Identity Based attacks are those attacks in which the personal identification details of a person are stolen and used for malicious purposes. The details may be financial,



Notes

medical, personal or any other such confidential information. Such identity theft may be used to commit crimes in the victim's name or may lead to unauthorized purchases, loans, and many more fraudulent activities.

Some of the common types of identity theft are:

- **Financial Identity Theft:** In this type of identity theft, the personal details are stolen for monetary benefits of the attacker.
- **Account Takeover Theft:** In this case the attacker uses the stolen details to get access to the victim's existing account and steal money.
- **True to Name Theft:** In this type of identity theft, the criminal steals personal details of the victim and then creates a new account on that very name. For example, a fraudster may open a bank account in the victim's name after stealing his/her personal details. Thereafter that bank account may be used for performing some illegal transactions.
- **Medical Identity Theft:** In this type of identity theft, the medical records, health claims, or insurance records of the victim are stolen to make some false financial claims on behalf of the victim.
- **Synthetic Identity Theft** – In this type of identity theft, the criminal steals personal information of multiple people. Portions of information from these multiple sources are then combined to create a new identity which is then used to get a debit/credit card, sim card, etc.
- **Child Identity theft** – This happens when personal details of a child such as his Aadhar card number are stolen and then used for malicious purposes. Generally, such details are not used instantly and so are difficult to catch.
- **Criminal Identity Theft** – When the attacker gives a stolen identity as his own identity in the police station and then commits crimes using that very stolen identity, it is criminal identity theft. As a result, the police approach the victim instead of the actual offender.

6.5.7 Insider Attacks

An insider attack is a type of cyberattack that is committed due to negligent or malicious employees, third party agents such as contractors and consultants, or business partners who have inside information about an organization. Such information includes sensitive data, security measures, and the authentication process of an organization. With an insider threat attack, there can be theft of



confidential or commercially valuable information, intellectual property, and trade secrets. With knowledge of the organization's security systems, it can also be an entry point for cyber criminals to launch a malware attack on the organization.

In these types of attacks, the insiders have legitimate access to the information and systems in the organization, and they misuse their legitimate access intentionally or accidentally, so it becomes very challenging to detect these threats. There are various types of insider threats. These include:

- **Intentional:** This is when an insider purposely and knowingly causes harm to an organization. This may be due to frustration, lack of recognition, or not getting due monetary benefits.
- **Unintentional:** This happens when the threat occurs due to human error or negligence. Sometimes, an employee is negligent and keeps weak passwords that are cracked easily, ignores software updates and security patches, or misplaces portable storage devices. This gives an opportunity to the attacker to commit the crime. Some other acts of negligence include sending business information to the wrong email address, clicking malicious links, opening malicious email attachments, or failing to delete sensitive information carefully.
- **Third Party Threats:** Any person or organization that is not an employee, but is connected with the organization due to business is a third party. For example, contractors, consultants, vendors, business partners, etc. The threats that arise due to negligence or malicious activity by any of these are known as third party threats.
- **Collusive Threats:** These are caused when one or more types of insider threats work together to cause harm to an organization.

6.5.8 IoT – Based Attacks

The Internet of Things (IoT) is a network formed by connecting multiple devices over the Internet. The devices that can be connected to the IoT are known as IoT devices. These include smart locks, vehicles, lighting systems, cameras, fitness trackers, home appliances such as air conditioners, washing machines and many other types of gadgets. Huge amounts of data is collected through these multiple devices, which makes the IoT devices very vulnerable to cyber attacks such as data theft, phishing attacks, spoofing, or Denial of Service (DoS) attacks.

Although there are quite a few advantages of IoT, the security aspects of IoT devices need due attention. The built-in sensors attached in the IoT devices pass on sensitive information through the Internet. Any security breach can cause theft of sensitive data.



Notes

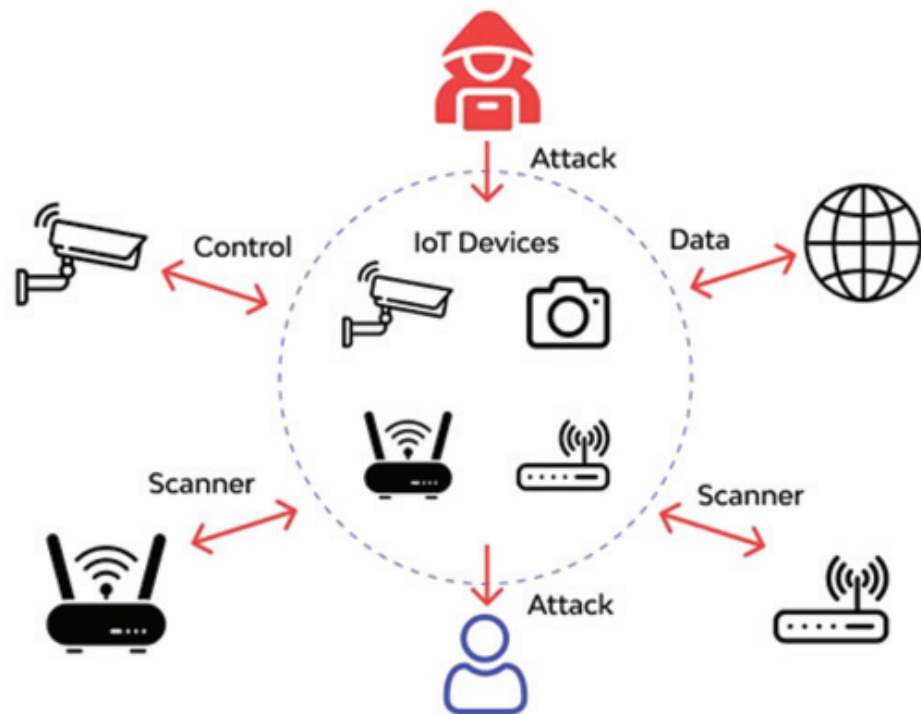


Fig. 6.3: IoT – Based Attacks

https://assets.website-files.com/5ff66329429d880392f6cba2/623d9a4f3d2b8fef4fc8af48_IoT%20world.jpg

Some of the reasons for IoT based attacks are as follows:

- **Outdated hardware and software:** The gadgets and digital devices, once installed, are not updated on time. This gives an opportunity to the cyber criminals to gain access to these devices and their data. The network ports that are used to connect these devices are also insecure as they do not use proper security protocols.
- **Use of default passwords:** Most gadgets, especially security cameras, home locks, routers, light control systems, etc. are installed with default passwords that are not changed by the user. This makes it easy for cyber criminals to compromise such gadgets.
- **Unsafe communication:** The messages sent over the Internet through IoT devices are not encrypted, hence, they can be easily comprehended by hackers.
- **Personal Information Leaks:** If the cyber criminals get hold of the IP address of the IoT devices, they can easily reveal the user's precise location, residential or permanent address.



- **Automation:** With the increase in the use of artificial intelligence and automation in the program codes, our lives have become convenient but at the same time, we have become increasingly dependent on technology. If cyber criminals get access to these codes, they can get control of the automation and do anything they want to. In one of the examples of the Milwaukee Couple case, the hackers compromised their smart home and took control of security cameras, played vulgar music, and pushed the room temperature to 90 degrees.

Another famous IoT based attack is the Mirai Bot attack. In 2016, an IoT botnet was used to execute a massive DDoS attack that brought several websites, such as CNN, Twitter, and Netflix, offline. The default usernames and passwords were used to log in to various gadgets in the IoT network and spread the malware.

IoT users should be aware of cyber security practices. One should always get services from a reliable IoT vendor and ensure that all their products use proper security measures in their product design. The smartphone controlling the IoT devices should also be well protected with a firewall or a dedicated monitoring tool. The notifications sent to the smartphone by the IoT devices should be read carefully.

6.5.9 Juice jacking

This is a type of cyberattack where an infected USB charging port is used to compromise a digital device. A mobile device can be charged using the same USB cable that is used to transfer data. If the phone is charged through a USB port that is compromised, the hackers either copy data or inject malware into the charging device in such a manner that it is not even noticed. Hence, one should never charge their phones at public places such as railway stations, cafes, metro stations, airports. Although most of the juice jacking attacks have occurred on mobile phones, all digital devices that are charged using USB are prone to this type of attack.

To prevent Juice jacking attacks, avoid public USB charging stations. Instead, use a power cable or carry your power bank. Still, if there is absolute necessity to charge using a USB port, then:

- disable automatic transfer of data option
- lock the device once it connects with the charging station, so that it is prevented from synching or transferring data.
- If a prompt appears to “Trust this computer”, deny the permission. This is a clear signal that the charging port is compromised.



Notes



Fig. 6.4: Juice Jacking

<https://iconscout.com/illustration/phone-juice-jacking-attack-5376385>

6.5.10 Man-in-the-middle (MITM) Attacks

A Man-In-The-Middle or MITM attack is a type of cyberattack where the attacker positions himself/herself between the two communicating entities (user and application) in a communication channel. This may be done to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of data is happening. None of the entities whether they are logging in, sending emails, texting, or chatting on a video call, are aware that an attacker is present in their conversation and is stealing their data. The attackers collect personal credentials and login information.

Consider a courier delivery service, where the courier delivery person opens the confidential packet, copies the personal details, seals the packet back and then delivers it. MITM attack works in the same manner where the attacker is the courier delivery person who steals confidential data.

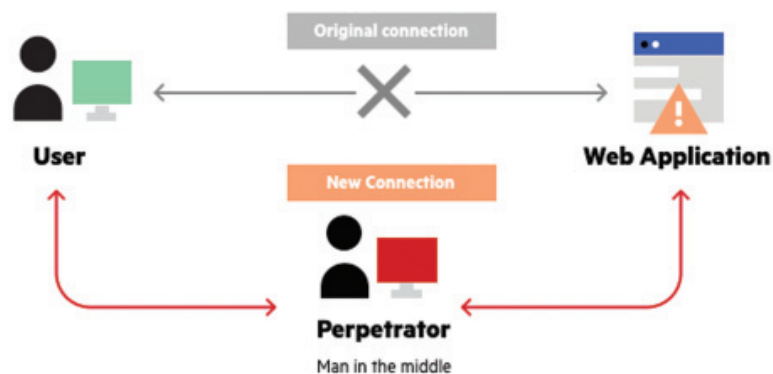


Fig. 6.5: Man in the Middle Attack



The aim of the attack is to steal personal data such as credit card numbers, passwords, login ids, etc. For example, if a user is logging in to an e-commerce site, the attacker positions himself/herself in between the e-commerce platform, to steal the user id and password is visible to the attacker. Other than e-commerce websites, financial and other applications where logging in is required, are targeted for MITM attacks. Information so obtained is used for identity theft, unapproved fund transfers or illicit password change. One of the warning signs of an MITM attack is unexpected and frequent disconnections from service and getting links of strange URLs in the browser window.

To avoid MITM attacks one must follow the following cyber security practices:

- Update and secure home Wi-Fi routers with strong passwords.
- Use a virtual private network (VPN) while connecting to the Internet.
- Use an updated antivirus software
- Avoid using public Wi-Fi, especially while performing financial transactions
- Do not visit unsecured websites

6.5.11 Password Attacks

A password attack is one when the attacker attempts to steal the password for any application. It is increasingly becoming common these days. The username and password are one of the most used authentication techniques. The attackers target the weak passwords, especially if that is the only authentication method used for logging in the network. The weak passwords are easily guessed as they are too generic or are already compromised. However, passwords may be stolen by installing a keylogger on the victim's device or through an MITM attack. The different types of password attacks are:

- Brute Force Attack:** In this type of attack, a hacker uses a computer program to try all possible letters, numbers, symbols in multiple combinations, character by character, until it gets the correct combination to form the correct password. This is done systematically using an automated program, starting with most common passwords. That is why weaker passwords such as 12345 or "abcdef", are easy to crack. c
- Phishing Attacks:** This is one of the most common types of attack. A hacker sends a phishing email which looks as if it is coming from a trustworthy source, such as a bank. The email usually contains a link that asks for the



Notes

sensitive information on the pretext of locking the account, or winning a prize, or gift transactions, etc. Once the victim is lured and gives the credentials to the hacker, he/she has the access to the victim's account. Further, if the same password is used across multiple accounts of the victim, the hacker has access to all the victim's accounts. Hence, a phishing attack relies on human error to be successful.

- (iii) **Credential Stuffing attacks:** This type of attack exploits the human tendency to reuse passwords. The hacker tries various combinations of stolen usernames and passwords, with the hope of gaining access to an account where the victim has reused the compromised password in any of the accounts. Such compromised passwords can be easily obtained from the dark web.
- (iv) **Dictionary attacks:** These are a type of brute force attacks but in this case, the hacker uses a common list of words, phrases, names, or certain other details that are personalized to a specific user. For example, it is very easy to find one's mother's name, date of birth, or your pet's name. The attacker tries to use these to gain access to the victim's account.
- (v) **Password Spraying Attacks:** Many times, the same password is used against multiple accounts in the same application. For example, one single username and password is used to login to all applications associated with google mail, such as google drive, google docs, google slides, etc. A password spraying attack is a type of brute force attack where the hacker uses one commonly used or default password to get access to multiple accounts of an application. As this process is automated, it can target millions of users at once. That is why the name of this attack is password spraying. To prevent this attack, a user is locked out after making certain failed login attempts.
- (vi) **Keylogger Attacks:** Keyloggers are malicious codes that record everything one types on the keyboard. Generally, such type of malicious software is downloaded and installed into the victim's device by phishing mails or along with free downloads from fraudulent sites. Once keyloggers have infected a system, they are almost impossible to detect, that is why prevention is the best defence for these types of attacks.

To avoid being the victim of password attacks:

- Use strong passwords and change them regularly.
- Wherever possible, use multi-factor authentication, wherever possible.
- If Possible, enable a biometric authentication
- Always use an updated antivirus software.



6.5.12 Cyber Bullying and Cyber Stalking

Cyber bullying and cyber stalking is becoming a growing concern among young internet users. In case of cyber bullying, digital devices along with the Internet are used to threaten, intimidate, or harass a person to such an extent that it becomes a trauma and distress for the victims.

Cyberstalking is an act of following a person online or making repeated attempts to contact the victim through text, audio, or video messages on a social media platform. This is done despite a clear indication of disinterest by the victim. The stalker sends lewd comments and attempts to seek personal attention.

6.5.13 Cyber Grooming

With the increase in Internet usage by children, and too without proper parental supervision, the children are becoming easy victims to cybercrimes. Cyber grooming is an act when a person, usually an adult, befriends a child through social media platforms. He/she subsequently gains trust of the child generally, with an intention of sexual abuse or any other such activity. The child may be forced to meet the attacker in person without the knowledge of parents or guardians. Such children may be abused or forced to perform illegal tasks.

6.5.14 SIM Swap

A SIM (Subscriber Identification Module) card is the only identity of a particular mobile phone. It identifies the phone to a specific mobile network and allows the user to use its features. SIM Swap is a type of cyberattack in which the criminal fraudulently manages to get a new SIM card issued from the mobile service provider against an already existing registered mobile number. Once the new SIM card is issued, all notifications, alerts, OTPs, that are required for making financial transactions through the victim's bank account are received to the criminal instead of the victim.

6.6 INTELLECTUAL PROPERTY THEFT

With increase in Internet usage, all kinds of creative work such as paintings, music, poems, blogs, research papers, software codes, etc. is made available to all around the world. But that does not mean that anybody can download and use any intellectual property without the consent of the creator. If anyone does the same, he is committing a criminal offence of intellectual property theft. Therefore, the following acts are included in intellectual property theft:



Notes

- **Software Piracy:** This is an act of copying a software and using or distributing it without the consent of the original creator.
- **Plagiarism:** This is an act when the offender copies someone else's work and presents it as his/her own work.
- **Copyright infringement:** A copyright is the right of an intellectual work given to its original creator. The right to use, distribute, reproduce, or display lies with the copyright holder. Any act by the offender that is done without seeking permission from the copyright holder is copyright infringement.
- **Trademark Infringement:** A trademark is a unique symbol or text that identifies the company and its products. If anyone tries to use a similar symbol or logo such that there are chances of deception by the consumers, then such an act is termed as trademark infringement. The figure shows two most popular trademark infringements.



Fig. 6.6: Intellectual Property Theft

<http://www.colormatters.com/images/brand-tm/mcdonald-3-rights.png>



Fig. 6.7

<https://legalupanishad.com/wp-content/uploads/2021/11/Registration-of-shape-of-goods-as-trademarks-5.png>



INTEXT QUESTIONS 6.2



Notes

A. State whether the following statements are true or false:

1. Anyone who is online is vulnerable to malware attacks.
2. A malicious code can only be hidden in a text file.
3. Melissa virus is an example of a boot sector virus.
4. Trojans cannot self-replicate but a worm can.
5. A fileless malware does not leave any digital footprint.
6. Cyber Bullying and Cyber Stalking refer to the same type of cyber crime.

B. Fill in the blanks:

1. A user's device may be infected with a if there is mysterious loss of disk space on the user's device.
2. A is a type of malware that multiplies at an exponential rate on the network but does not need any host program to spread the infection.
3. The persons who commit the crime of hacking are known as
4. is an attempt by cyber criminals to seek personal information through phone calls.
5. The is a network formed by connecting multiple devices over the Internet.
6. A is a unique symbol or text that identifies the company and its products.

6.7 STRIDE THREAT MODELLING

STRIDE Threat modelling is one of the commonly used and most effective tools that can help find threats, rank them in terms of how serious they are, and develop plans to counter them. It was developed by Microsoft to assess the system from the perspective of a potential attacker. Thereafter, the model selects appropriate controls to reduce the risks of such attacks.

STRIDE is an acronym for six threats - Spoofing identity, Tampering with data, Repudiation threats, Information Disclosure, Denial of service, and Elevation of Privileges. Examples of each of these categories are:



Notes

Fundamentals of Cyber Security

Name of Threat	Violated Property	Explanation	Example
Spoofing Identity	Authenticity	Pretending to be a valid user	Illegally accessing someone's username and password
Tampering with data	Integrity	Unauthorized changes made to the data in the storage media or during transmission	One of the many employees of an organization, tampers with integrated checking mechanisms
Repudiation Threats	Non-repudiability	users deny any action performed by them when other users have no means to identify them.	Committing an act under false identity
Information Disclosure	Confidentiality	release of information to the unauthorized parties	A user reads a file that that they were not granted access to
Denial-of-Service	Availability	Deny service to valid users	Intended users are not allowed access to a web server
Elevation of	Authorization	Unprivileged user gets sufficient access to compromise or harm the system	Malicious code is used to access permissions and authorizations

The developers can use STRIDE threat model to spot threats during the design phase of any application or software for offline or online computing. It aims to ensure that the app or software fulfills the CIA triad of Confidentiality, Integrity, and Availability. The model can also be used to find and repair threats in IoT devices as well. STRIDE threat modelling helps the experts to be prepared for future threats.

6.8 PLAINTEXT AND CIPHERTEXT

Plain text (or Clear text) refers to original readable data that is in its natural form. Examples of plaintext include phrases, poems, software codes in programming languages such as Python, C, C++, etc. Majority of applications such as browsers, word processors, emails, etc. prefer plaintext. However, the data in plain text is vulnerable to cyberattacks, especially those that contain passwords or any other sensitive information. This is because plain text is presented in a format that is accessible, not encrypted, and hence is usable without the need for any decryption



tools. The data stored in plaintext in a digital device should be protected from theft, disclosure or transmission as its contents are fully visible. In case of exposure or attack, the third parties should not be able to easily read or interpret the data. That is why both storage medium and device should be protected and safeguarded against potential thefts. Further, it is advised to encrypt sensitive data before it is stored or transmitted, so that it cannot be easily comprehended by the hackers.

The plaintext data, whether stored as hardcopy or soft copy, is insecure when used and stored. Ciphertext is an encrypted version of a plaintext message. It is the data in plaintext that has been changed to make it non-readable to hackers. It can only be read by intended receivers. Ciphertext looks like a string of random characters. Even if hackers manage to breach the security layers and get access to data, they won't be able to understand the encrypted data. This adds another layer of protection to the data.

6.8.1 Cryptography

Cryptography is the process in which the algorithms convert plaintext to ciphertext and vice versa. To protect sensitive data from unauthorized users, cryptography is used in practically all operations. Plaintext and ciphertext are two fundamental concepts in the world of cryptography.

A cryptographic system or an encryption algorithm takes plain text as input, executes the algorithm on this plaintext data, and generates ciphertext as output. The process of converting plaintext to ciphertext is known as **encryption** and the reverse process of converting the encrypted text back to plaintext is known as **decryption**. The process of encryption involves scrambling the original message and making it unreadable, using a secret encryption key. In the reverse process, the decryption algorithms use that very secret key (known as decryption key), to transform ciphertext back into plaintext, that can be read and understood by the recipient. The encryption or decryption key is known as a **cypher (or cipher)**. A cipher can be individual characters, pairs or triplets of characters, or any other combination. These cyphers replace a specific sequence and a pattern of conversion is maintained throughout the conversion process. The strength of a cipher is a critical factor in ensuring the security of encrypted data. However, encryption protects data from unauthorized access but it cannot protect data from modification or deletion from someone who has access to it.

Cryptography is often used by healthcare, e-commerce, banking applications, defence and diplomatic establishments, and other platforms that use confidential data.



Notes

6.8.2 Symmetric and Asymmetric Cryptography

Symmetric cryptography is one where algorithms use a single key to encrypt and decrypt information. The strength of the algorithm depends on how complex this single key is. The sender uses a secret key to encrypt the data and the recipient uses the same key to decrypt and read the encrypted data. Therefore, the secret key is to be shared across all entities that are authorized to decrypt the message. Also, the key must be shared in such a secure manner that any kind of exposure can be avoided. All entities receiving the key should be trustworthy and responsible. All this makes security a major concern in case of symmetric cryptography.

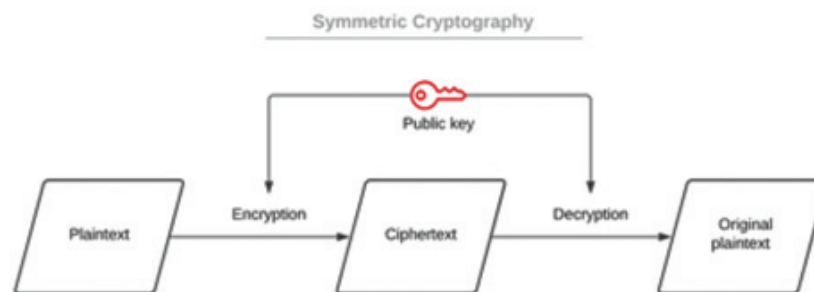


Fig. 6.8: Symmetric Cryptography

<https://www.baeldung.com/wp-content/uploads/sites/4/2021/06/Blank-diagram.svg>

Asymmetric Cryptography is one in which two separate keys – one public and other private are used to encrypt and decrypt data. The public key is used to encrypt the message and is publicly shared. The private key is used to decrypt data. It should be securely stored and never be transferred. However, both keys are mathematically connected. The private key is calculated based on the public key.

As far as security is concerned, only the recipient is responsible for the security of the private key. The asymmetric ciphers are more secure than symmetric ciphers. Hence, it is much more secure as compared to symmetric cryptography. This method of cryptography is widely used in digital signatures.

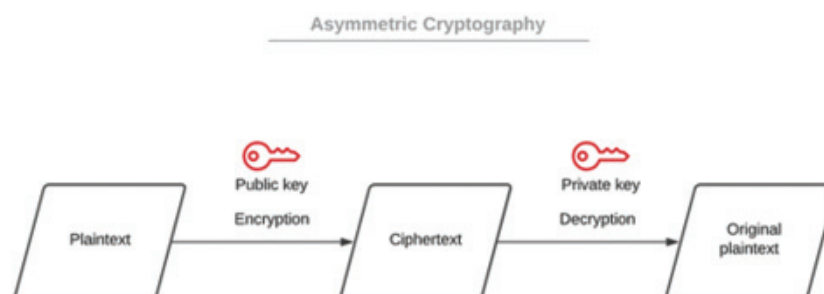


Fig. 6.9: Asymmetric Cryptography

<https://www.baeldung.com/wp-content/uploads/sites/4/2021/06/Blank-diagram-Copy-of-Page-1-1.svg>



Asymmetric cryptography is slower than symmetric cryptography. Therefore, sometimes hybrid approaches are used. A fast symmetric cipher is used for the encryption of an entire message while slow asymmetric encryption is used only for encrypting the key. This process is very efficient, especially for large amounts of data.

Some of the examples, in real life, where cryptography is used are:

- **End-to-end encryption in Messaging Apps:** Messaging apps such as WhatsApp, Signal, and Telegram use end-to-end encryption to secure their conversations. When a message is transmitted on the app, it is encrypted first and then it is only decrypted on the recipient's device. This prevents anyone, including the service provider, from intercepting and reading the messages in the chat.
- **Secure communication in Online Banking:** When the user accesses the bank's website or mobile app, the process of encryption ensures that the login credentials, personal information, and financial transactions are transmitted securely over the Internet. This protects the user from eavesdropping and data theft.
- **Two-Factor Authentication (2FA) :** Many online banking services use encryption to secure the delivery of one-time codes for 2FA. This ensures that only the authentic user can access his/her account, even if someone may have stolen the password.

6.9 ENCRYPTION STANDARDS AND ALGORITHMS

There are various encryption standards available that can be used to secure data being stored or transmitted.

6.9.1 Data Encryption Standard(DES)

Data Encryption Standard (DES) is a historic encryption algorithm developed in 1977. This symmetric data encryption standard divides the plaintext into two parts and then encrypts each part individually. The **56-bit security key** is used to encrypt data in blocks of size of 64 bits each. That means 64 bits of plaintext is taken as input and it generates 64-bits of encrypted text as output. The same algorithm and key are used for encryption and decryption, but with minor differences. One of the applications of DES is to generate random numbers. It has played a significant role in data security but with advancements in computing power, DES has become vulnerable to hacking. That is why it is deployed where strong encryption is not needed. But DES has been used to develop Triple DES (3DES), which provides much more data security.



Notes

6.9.2 Advanced Encryption Standards(AES)

In 2001, US National Institute of Standards and Technology (NIST) established a standard specification for the encryption of electronic data and in 2003, it became the default and publicly accessible encryption algorithm for protecting classified information. Today, AES is widely implemented throughout the world to encrypt sensitive data, in both hardware and software. AES puts the data through multiple encryption rounds and splits it into smaller blocks of 128 bits each. This means, it takes 128 bits (16 bytes) of input and gives 128 bits (16 bytes) of encrypted data as output. Since it is a symmetric encryption algorithm, it uses the same secret encryption key to encrypt and decrypt data. Therefore, this key should be known to both sender and receiver.

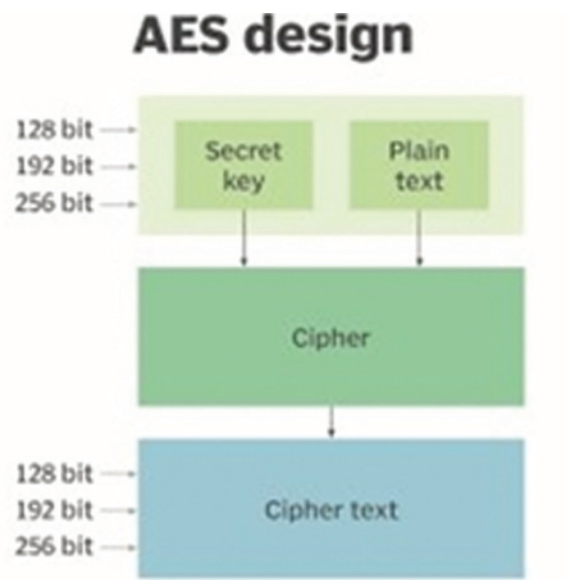


Fig. 6.10: AES Design

https://cdn.ttgtmedia.com/rms/onlineImages/security-aes_design.jpg

AES uses multiple cryptographic keys that could be of 128-bit, 192-bit or 256-bit. Each key goes through 10, 12, and 14 rounds of encryption respectively, to ensure confidentiality and integrity of data. The more the rounds, the harder it becomes to crack the information.

AES is used for a wide range of encryption applications for both government and commercial use such as electronic communication apps, programming libraries, internet browsers, wireless networks, login credentials including passwords, virtual private networking, etc. The classified government or military information is protected using 192-bit or 256-bit security keys.



6.9.3 Triple Data Encryption Standard (3DES)

Triple Data Encryption Standard (3DES) is a symmetric encryption algorithm that is based on the original Data Encryption Standard (DES). However, it utilizes three different keys to encrypt the 64-bit blocks of plaintext, three times. It supports variable security key sizes that range from 128 bits to 192 bits but the same key is used both for encryption and decryption.

Firstly, the plaintext is encrypted with one key, **K1** to generate an intermediate ciphertext. This intermediate ciphertext is decrypted using another key, **K2** and then the final encryption is done using the third key, **K3**. The outcome of this three-step process is a highly secure ciphertext representation of the original plaintext. During the decryption process, the reverse process is followed. That is decrypting with **K3**, then encrypting with **K2** and finally decrypting with **K1**.

3DES is robust and very resistant against modern computational threats. That is why it is widely used with many encryption standards and protocols. Some of the common application areas of 3DES are:

- Secure the financial transactions that take place during net banking, credit card payments, etc.
- Protect sensitive data that is stored in servers of government and military organizations
- Secure the communication between remote locations and virtual private networks.
- Verify the authenticity of digital signatures and digital documents.

The advantages of 3DES are:

- It provides increased security as compared to DES.
- It is compatible with the original DES making the transition of algorithms easy.
- It is widely supported and integrated into various applications, protocols, and hardware.
- Over the decades, it has proved to be very reliable and trustworthy.

However, 3DES is slower in implementation and processing as compared to AES and DES. It also requires management of multiple keys which is quite complex and time consuming as compared to other algorithms.



Notes

6.9.4 Hashing Algorithms

In computing, the data (usually of variable length) is transformed into a fixed size string of characters. This transformed string, which is typically a sequence of numbers and letters, is known as **hash value** or simply **hash** and the process is known as **hashing**.

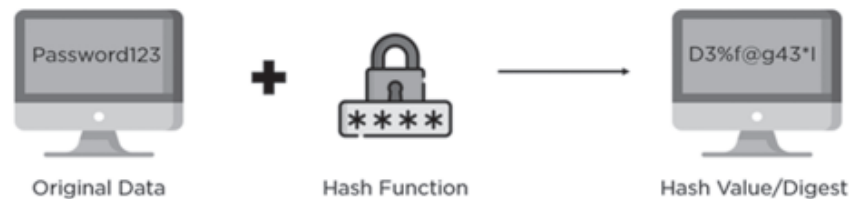


Fig. 6.11: Hashing

https://www.simplilearn.com/ice9/free_resources_article_thumb/md5hashing.PNG

It uses an algorithm, known as **hash function** to create a unique hash value for each specific input data. This set of hash values is known as **hash digest** (or simply **digest**). The hash function generates a different hash even if one character in the input message changes. The main difference between hashing and encryption is that hashing is one-way. Once the data is hashed, it cannot be decrypted unless a brute force attack is used.

Two commonly used hash functions are MD5 and SHA.

Message Digest Algorithm(MD5)

Message Digest Algorithm (MD5) is a cryptographic hash function algorithm that takes input messages of any length and converts it into a fixed length hash or digest of **128 bits (16 bytes)**. It is commonly used for file authentication and for securing passwords of users.



Fig. 6.12: MD5 Algorithm

It is faster, simple and requires relatively low memory to integrate. But, as it generates the same hash function for different inputs, it is considered to be an insecure algorithm.

**Secure Hash Algorithm(SHA)**

Secure Hash Algorithm (SHA) is also a set of cryptographic hash functions that ensure integrity and security of data. It always gives the same hash value for the same input. This property ensures consistency in verifying data integrity and authentication. It is highly improbable that two different data inputs will produce the same hash value. This feature is known as **collision resistance** and is crucial to prevent substitution of one message with another.

SHA is effectively used to safeguard passwords and digital signatures. The server side just keeps track of the user's hash value, rather than the actual password. So, even if the attacker hacks the database, he/she will only find the hashed values and not actual passwords.

SHAs are also used to detect tampering of data that is stored or transmitted. This is because even a slight change to the original text, changes its hash value, making the tampering noticeable.

**INTEXT QUESTIONS 6.3****A. State whether the following statements are true or false:**

1. A STRIDE model is used to anticipate potential threats during the design phase of an application.
2. Plain text can be read only by intended receivers.
3. Sensitive data must be transmitted in encrypted form.
4. A cipher can consist of only individual letters.
5. Messaging apps do not use encryption of data.
6. Hashing and encryption are the same.

B. Fill in the blanks:

1. The S in STRIDE stands for
2. is an encrypted version of a plaintext message.
3. The process of converting plaintext to ciphertext is known as
4. The encryption or decryption key is known as
5. cryptography is one where algorithms use a single key to encrypt and decrypt information.
6. uses three different keys to encrypt data three times.



Notes



WHAT HAVE YOU LEARNT

- Information security focuses on protecting digital data, while cyber ethics involves following ethical guidelines for online behavior.
- The basic principles of information security, known as the CIA triad, are **Confidentiality** (ensuring authorized access to data), **Integrity** (maintaining accurate and unaltered data), and **Availability** (ensuring data is accessible to authorized users when needed).
- Malware is malicious software designed to harm digital devices, steal or encrypt data, and disrupt networks, with common types including viruses, worms, trojans, spyware and ransomware. To prevent malware attacks, users should keep their systems updated, avoid clicking on suspicious links, use strong passwords, enable multi-factor authentication, and regularly back up their data.
- Cyberattacks are intentional efforts to steal, modify, or damage data and systems, with common types including hacking, malware attacks, DDoS, phishing, spoofing, identity theft, insider attacks, IoT-based attacks, and juice jacking.
- Intellectual property theft involves unauthorized use or distribution of creative works, including software piracy, plagiarism, copyright infringement, and trademark infringement.
- STRIDE threat modeling is a tool developed by Microsoft to assess and mitigate potential threats by identifying, ranking, and developing countermeasures for risks.
- It focuses on six threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges, ensuring that software or IoT devices meet the Confidentiality, Integrity, and Availability (CIA) triad.
- In symmetric cryptography, a single secret key is used for both encryption and decryption, with the strength of the algorithm depending on the complexity of the key. The key must be securely shared among trusted entities, which raises security concerns if the key is exposed.



TERMINAL EXERCISE



Notes

1. Define the following:
 - (a) Cybercrime
 - (b) Information Security
 - (c) Malware
 - (d) Spoofing
 - (e) Plagiarism
 - (f) Cryptography
2. Expand the following:
SHA, 3DES, AES
3. Explain CIA Triad with respect to Information Security.
4. Name any three authentication and any three authorization techniques.
5. Explain the ethical concerns that have arisen because of technology.
6. Differentiate between Internet, Intranet, and Extranet.
7. Give any five tips that would protect your device from a potential malware attack.
8. Name any three types of Identity theft attacks.
9. What are IoT based attacks? Why are such attacks caused?
10. Explain briefly MITM attacks.
11. Write a short note on STRIDE threat modelling.
12. Give one example each of:
 - (a) Boot Sector Virus
 - (b) Ransomware
 - (c) Fileless Malware
 - (d) Spyware
 - (e) Hash Function
13. Differentiate between:
 - (a) Authentication and Authorization
 - (b) Virus and Worm
 - (c) Phishing and vishing
 - (d) Symmetric and Asymmetric Cryptography
 - (e) 3DES and AES



Notes



ANSWER TO INTEXT-QUESTIONS

6.1

- A. 1. True 2. False 3. False 4. True 5. True
B. 1. Ethical 2. Unethical 3. Ethical 4. Unethical

6.2

- A. 1. True 2. False 3. False 4. True 5. True
6. False
B. 1. malware 2. worm 3. hackers 4. Vishing
5. Internet of Things (IoT) 6. trademark

6.3

- A. 1. True 2. False 3. True 4. False 5. False
6. False
B. 1. Spoofing 2. Identity 3. Ciphertext 4. encryption 5. cipher
6. Symmetric 7. 3DES

Key Learning Outcomes

- Explain key concepts in information security, including the CIA triad.
- Identify different types of malware (e.g., viruses, worms, ransomware)
- Categorize common cyberattacks and describe their implications on system security and data protection
- Compare and contrast symmetric and asymmetric cryptography, explaining their advantages and limitations



7

INTRODUCTION TO NETWORK SECURITY

While discussing how our digital data is protected, the network security has to be ensured before data transmission. To get started with network security, it is important to know about the computer networks and their protocols. A computer network refers to the association of interconnected computers and other devices that may interact with one another. The main purpose of a computer network is to share information and resources among the devices connected to it. Computer networks can be classified into LAN, MAN, and WAN depending on their size and geographical extent.

A computer network consists of various network devices, including bridges, switches, routers, gateways, firewalls, modems, repeaters, and access points. These devices communicate using network protocols that include TCP/IP, UDP, HTTP, HTTPS, and FTP as you learned about in chapter 6. This lesson will thus cover network security and its involved protocols, how to implement and configure firewalls on Windows and Linux and delve into wireless networks and their safety and involved protocols.



OBJECTIVES

After reading this lesson, you will be able to:

- figure out the working of network security protocols;
- configure and create firewall rules in windows and Linux based environment;
- understand the basics of wireless network security.



7.1 NETWORK SECURITY PROTOCOLS

The purpose of network security is the secure transmission of information between devices or computers. These protocols are designed to ensure the confidentiality, integrity, and authenticity of data when it travels between devices or systems. The main purpose of these protocols is to secure the communication channel and prevent the data from unauthorized access, interception, or tampering.

Here are some common network security protocols which works at different layers of TCP/IP protocol stack:

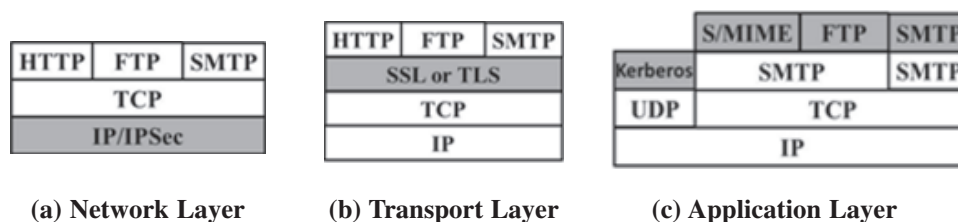


Fig. 7.1

Few important network security protocols are :

1. Secure Sockets Layer (SSL) / Transport Layer Security (TLS)
2. IPSec
3. User Authentication and Kerberos:
4. Virtual Private Network (VPN) Protocols

Let's discuss these protocols in detail:-

7.1.1 Secure Sockets Layer (SSL) / Transport Layer Security (TLS)

SSL is a protocol created by Netscape in 1994, which was later managed by IETF and renamed SSL as TLS and has various versions, TLS 1.3 is the latest version. The Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), are cryptographic protocols that play an essential role in securing communication channels over computer networks. These protocols provide a secure layer for data transmission, ensuring confidentiality, integrity, and authenticity in online interactions. This protocol is generally used for securing web browsing (HTTPS), email (SMTPS/IMAPS), and other applications.

It encrypts data to provide confidentiality and ensures the integrity of the communication. Let us understand how SSL protocol works. There are 4 SSL layer protocols as mentioned below :

- SSL record protocol
- SSL Handshake protocol
- SSL Change-cipher spec protocol
- SSL Alert protocol



Notes

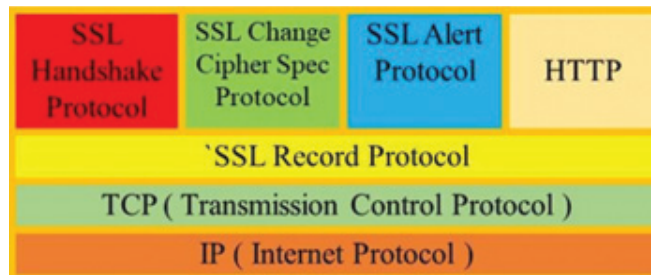


Fig. 7.2: SSL Architecture (SSL Protocol Stack)

In the above figure we can see the SSL protocol stack. Let's understand the purpose and working of all the protocols.

(i) SSL record protocol

In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then an encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended to the fragment. After the data is encrypted, an SSL header is appended to the data.

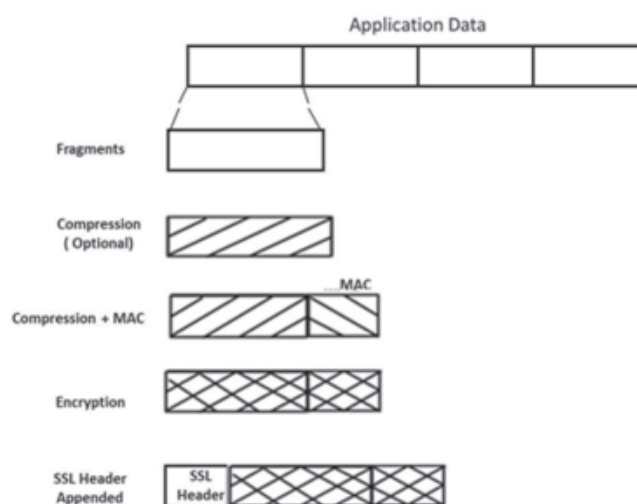


Fig. 7.3: SSL Record Protocol Operation



The SSL record protocol provides the following two services to SSL connection:

- Confidentiality
 - By using symmetric encryption with a shared secret key defined by Handshake Protocol.
 - Provide encryption using algorithms like DES-40, DES, 3DES
 - The message is compressed before encryption.
- Message integrity
 - By using a MAC with shared secret key
 - Similar to HMAC (Hash-based Message Authentication Code) but with different padding.

(ii) SSL Handshake protocol

SSL/TLS uses a handshake process to initiate a secure connection between a client and a server. This involves several steps, including the negotiation of cryptographic algorithms and the exchange of digital certificates. Digital certificates, issued by trusted Certificate Authorities (CAs), validate the authenticity of the server, assuring the client that they are communicating with the intended and legitimate entity. SSL handshake protocol allows server & client to:

- authenticate each other
- to negotiate encryption & MAC algorithms
- to negotiate cryptographic keys to be used

The handshake protocol comprises a series of messages in four phases to complete the handshake process.

- Phase-1: During this stage, both the Client and Server transmit hello message to one another. In this phase, the cipher suite, which includes the set of algorithms and the protocol version, is shared for security reasons.
- Phase-2: After phase 1, The server transmits its certificate along with the Server-key-exchange. The server concludes phase-2 by dispatching the Server-hello-end packet.
- Phase-3: In this phase, The client responds to the server by providing their certificate along with the Client-exchange-key.
- Phase-4: In Phase-4 The change-cipher suite is implemented, signalling the conclusion of the Handshake Protocol.



Notes

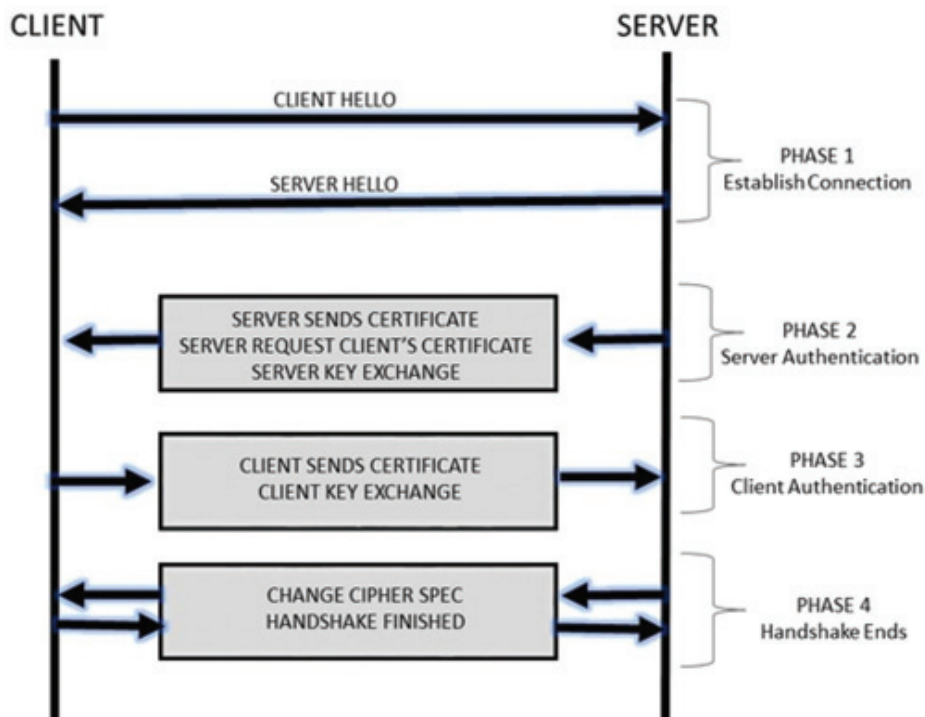


Fig. 7.4: SSL handshake protocol

(iii) SSL Change-cipher spec protocol

The ChangeCipherSpec protocol is an essential message communicated during the TLS handshake. It acts as an indication that both the client and server are prepared to move from unencrypted communication to a secure mode, utilizing the newly agreed-upon cryptographic parameters, including encryption keys and cipher suites. This message is independently sent by each party following the key exchange phase and prior to the commencement of actual application data transmission. By sharing this message, both the client and server confirm they are in alignment to enable the secure communication channel, ensuring the confidentiality and integrity of the data exchanged thereafter.

(iv) SSL Alert protocol

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.

The different versions of SSL with their year of release:

SSL 1: Never publicly released due to significant security vulnerabilities.

SSL 2: Released in 1995 as an initial attempt to secure online communication, but later deprecated due to security flaws.



Notes

SSL 3: Released in 1996, an improvement over SSL 2, but also eventually deprecated due to vulnerabilities like the “POODLE” attack.

TLS 1.0: Released in 1999, marking a significant step forward with improved security features and becoming the de facto standard for secure communication.

TLS 1.1: Released in 2006, addressing some of the security issues in TLS 1.0.

TLS 1.2: Released in 2008, a major enhancement with stronger encryption algorithms and improved security features.

TLS 1.3: Released in 2018, the latest version with significant improvements in performance, security, and privacy.

7.1.1.5 Characteristics of SSL

The SSL protocol has several important characteristics or advantages that make it a reliable solution for securing online transactions:

- **Encryption**
 - Employs strong encryption algorithms (like AES) to scramble data during transmission.
 - Prevents eavesdropping and data theft by malicious actors.
- **Authentication**
 - Verifies the identity of the website or server.
 - Ensures users are communicating with the genuine entity and not a fraudulent one.
- **Data Integrity**
 - Utilizes message authentication codes (MACs) to detect any alterations to the data during transit.
 - Guarantees that the received information matches the original data sent.
- **Non-Repudiation**
 - Difficult for the sender to deny having sent the information, enhancing accountability.
 - Crucial for legal and financial transactions.
- **Public-Key Cryptography**
 - Enables secure key exchange between client and server.
 - Allows for secure communication without the need to pre-share secret keys.



- **Session Management:**
 - Allows for the reuse of established secure connections.
 - Reduces latency and improves performance for subsequent interactions.
- **Trusted Certificate Authorities (CAs):**
 - Issue digital certificates that vouch for the authenticity of websites.
 - Provide users with confidence in the trustworthiness of the website they are interacting with.

In essence, SSL provides a robust framework for secure online communication by establishing trust, confidentiality, and data integrity between the client and server.

7.1.2 Internet Protocol Security (IPsec)

This network security protocol works at the internet layer of the TCP/IP protocol stack. It provides secure communication at the internet layer including virtual private network (VPN) connections. It encrypts and authenticates IP packets, ensuring secure and private communication. You have learned about the internet protocol (IP) and IPv4 header in chapter 3.

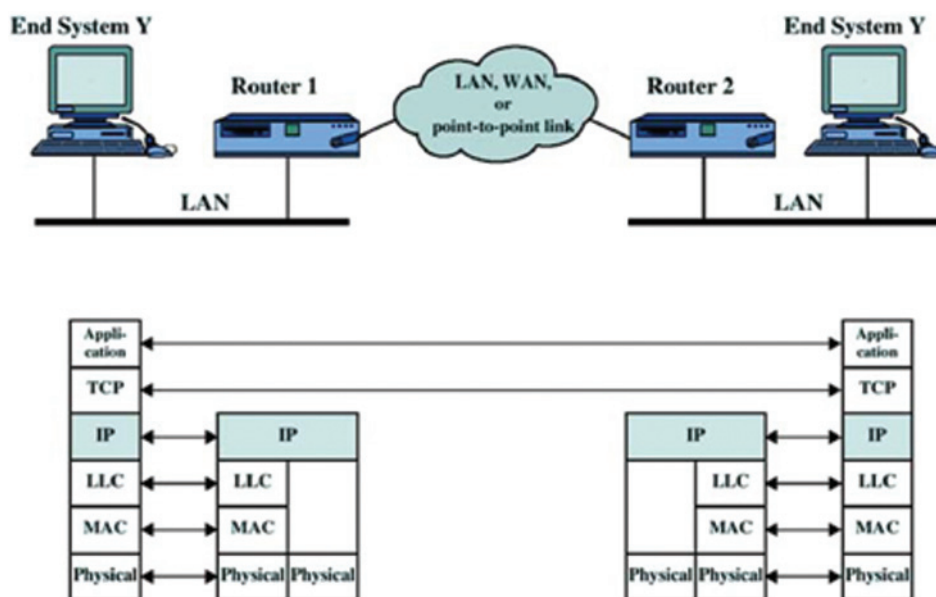


Fig. 7.5: Example of TCP/IP Protocol Working

There is more than one protocol in the IPsec family. A pair of communicating entities can utilize any security technique that is suitable for the communication



Notes

because of IPSec's broad framework and collection of security algorithms. It is an essential part of network security architectures because it offers a framework for guaranteeing the confidentiality, integrity, and authenticity of data transferred between network devices.

7.1.3 User Authentication and Kerberos

In network security authentication plays a very important role because authentication means verifying the identity of a user logging onto a network. Authentication is the process of determining whether someone or something is in fact, who or what it is declared to be.

Kerberos is a centralized private key third party network protocol that provides secure authentication for network users and in a distributed network. It was developed by MIT (Massachusetts Institute of Technology) and is widely used in various environments, particularly in enterprise networks. The main functionality of Kerberos is that it provides a centralized authentication server to verify the identities of users and services, also known as *single sign on* functionality.

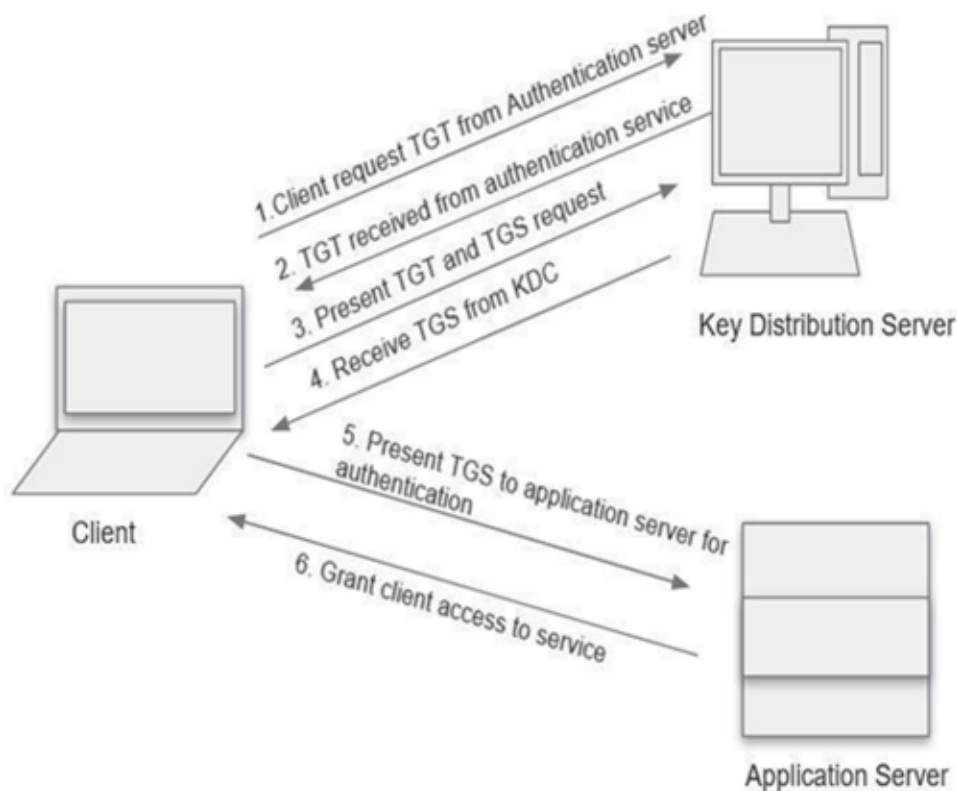


Fig. 7.6: How Kerberos Works



Type of Authentication methods

- **Something user knows:** PINs and passwords fall within this category.
- **Something user have:** A key, token card, smart card, disk, or other device
- **Something user is:** comprises biometric authentication techniques including voice recognition, fingerprints, and iris or retinal scans.

The Kerberos protocol involves the following components:

Client: The user or service requesting authentication.

Key Distribution Center (KDC): The trusted third party that issues tickets. It consists of two components: The Authentication Server (AS) and the Ticket Granting Server (TGS).

Service: The network service to which the client wants to authenticate.

Kerberos environment consists of several components and steps as follows:

User Authentication Request

The user initiates the authentication process by requesting a service from the Kerberos system.

The user provides credentials (usually a username and password) to the Authentication Server (AS).

Ticket Granting Ticket (TGT) Issuance

The AS verifies the user's credentials and, if valid, issues a Ticket Granting Ticket (TGT) to the user.

The TGT is encrypted using the user's password or a key derived from the password.

Ticket Granting Service (TGS) Request

When the user wants to access a specific service, they present the TGT to the Ticket Granting Server (TGS) along with a service request.

The TGS verifies the TGT and, if valid, issues a Service Ticket (TGS) for the requested service.

Service Authentication

The user presents the Service Ticket to the service they want to access.



Notes

The service uses its secret key (known only to the service and the Kerberos system) to decrypt the Service Ticket.

Mutual Authentication

Both the user and the service authenticate each other. The user proves their identity by presenting a valid TGT, and the service proves its identity by decrypting the Service Ticket.

Session Key Establishment

After mutual authentication, a session key is generated. This session key is used to encrypt the communication between the user and the service for the duration of the session.

Access Granted

With successful authentication and the establishment of a session key, the user is granted access to the requested service.

Ticket Expiration

Tickets (TGT and TGS) have a limited validity period. After this period, the user needs to request new tickets for continued access.

Realm: A Kerberos realm is a set of managed network resources and Kerberos servers that share a common authentication database.

The Kerberos protocol helps protect against various security threats, including eavesdropping, replay attacks, and credential theft. It is commonly used in environments that require a high level of security, such as corporate networks, academic institutions, and government organizations.

7.1.5 Virtual Private Network (VPN) Protocols

A VPN is a private network that operates over a public network like the internet to link remote locations or users. Rather than relying on a dedicated physical connection like a leased line, a VPN establishes a “virtual” link that is routed through the internet, connecting the company’s private network to the remote employee’s site.

7.1.5.1 Types of VPN

1. Remote Access VPN

Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the



private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both. An employee of a company, while he/she is out of station, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network. Private users or home users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users aware of Internet security also use VPN services to enhance their Internet security and privacy.

2. Site to Site VPN

A Site-to-Site VPN is also called a Router-to-Router VPN and is commonly used in large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

Intranet based VPN: When several offices of the same company are connected using Site-to-Site VPN type, it is called an Intranet based VPN.

Extranet based VPN: When companies use Site-to-site VPN type to connect to the office of another company, it is called an Extranet based VPN.

3. Cloud VPN

A Cloud VPN is a virtual private network that allows users to securely connect to a cloud-based infrastructure or service. It uses the internet as the primary transport medium to connect the remote users to the cloud-based resources. Cloud VPNs are typically offered as a service by cloud providers such as Amazon Web Services (AWS) and Microsoft Azure. It uses the same encryption and security protocols as traditional VPNs, such as IPsec or SSL, to ensure that the data transmitted over the VPN is secure. Cloud VPNs are often used by organizations to securely connect their on-premises resources to cloud-based resources, such as cloud-based storage or software-as-a-service (SaaS) applications.

7.1.5.2 Key features and Benefits

- Improved security,
- Improved productivity,
- Extended geographic connectivity,
- Reduced operational costs versus traditional WAN,
- Reduced transit time and transportation costs for remote users,
- Simplified network topology.



Notes



INTEXT QUESTIONS 7.1

1. What is the purpose of Network Security Protocols?
2. The Handshake protocol consists of phases.
3. Each message in SSL alert protocol contains bytes
4. The Authentication header ensures the integrity and authenticity of packets.
5. PGP was designed by a software engineer named in the year

7.2 NETWORK SECURITY USING FIREWALL (WINDOWS AND LINUX FIREWALL)

A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined rules. Its primary purpose is to establish a barrier between a trusted internal network and untrusted external networks, such as the internet. Firewalls are a fundamental component of network security and play a crucial role in protecting a local system or network of systems from network based security threats.

A good firewall should be designed to achieve following goals:

- All traffic from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall)
- Only authorized traffic (defined by the local security policy) will be allowed to pass
- The firewall itself is immune to penetration (use of trusted system with a secure operating system)

7.2.1 Characteristics of Firewall

Service control: Determines the types of Internet services that can be accessed, inbound or outbound

Direction control: Determines the direction in which particular service requests are allowed to flow

User control: Controls access to a service according to which user is attempting to access it

Behaviour control: Controls how particular services are used (e.g. filter e-mail)



7.2.2 Types of firewall

Firewalls can be categorized into several types based on their deployment, functionality, and inspection methods. Here are some common types of firewalls:

7.2.2.1 Packet Filtering Firewalls

Functionality: Examines individual packets of data and makes decisions to allow or block them based on predefined rules.

Characteristics: Basic and often the first line of defense. Decisions are typically based on criteria such as source and destination IP addresses, port numbers, and protocols.

7.2.2.2 Stateful Inspection Firewalls

Functionality: Monitors the state of active connections and makes decisions based on the context of the traffic, considering the state of the connection and the history of packets exchanged.

Characteristics: Provides a higher level of security than packet filtering alone. Keeps track of the state of network connections to make more informed decisions.

7.2.2.3 Proxy Firewalls (Application Layer Firewalls)

Functionality: Acts as an intermediary between internal and external systems. It receives requests from internal devices, forwards them to external servers, and returns the responses. This isolates internal systems from direct external communication.

Characteristics: Adds an additional layer of security by hiding internal network details. Can provide content filtering and additional application-specific security.

7.2.2.4 Circuit-Level Gateways

Functionality: Works at the transport layer (Layer 4) and monitors TCP handshakes to ensure that the session is legitimate. It doesn't inspect the content of the data packets.

Characteristics: Useful for creating secure connections for specific applications but may lack the detailed inspection provided by other types of firewalls.

7.2.2.5 Application Layer Firewalls (Proxy Firewalls)

Functionality: Operates at the application layer (Layer 7) and can inspect, filter, and block traffic based on the specific application or service being accessed.

Characteristics: Provides granular control over applications and services. Can enforce security policies at the application layer.



Notes

7.2.2.6 Next-Generation Firewalls (NGFW)

Functionality: Combines traditional firewall features with advanced capabilities such as intrusion prevention, deep packet inspection, and application awareness.

Characteristics: Offers a more comprehensive approach to security, addressing both traditional and modern threats. Can identify and block specific applications or types of content.

7.2.2.7 Hardware Firewalls

Deployment: Implemented as dedicated physical devices (hardware appliances).

Characteristics: Often used to protect entire networks. Provides robust security features and is typically positioned at the network perimeter.

7.2.2.8 Software Firewalls

Deployment: Implemented as software applications and can run on general-purpose operating systems.

Characteristics: Commonly used for protecting individual devices, such as computers and servers. May include personal firewall software for end-users.

7.2.2.9 Cloud Firewalls

Deployment: Hosted in the cloud and designed to protect virtual machines, applications, and services deployed in cloud environments.

Characteristics: Scalable and flexible. Provides security for cloud-based resources and integrates with cloud services.

7.2.2.10 Wireless Firewalls

Deployment: Specifically designed to secure wireless networks.

Characteristics: Includes features for protecting Wi-Fi networks, managing access points, and securing wireless communications.



INTEXT QUESTIONS 7.2

1. What is firewall?
2. How a firewall protects the network from external threats?
3. Write the full form of NGFW?
4. Write the characteristics of Application layer firewall?



7.3 HOW TO CONFIGURE FIREWALL

Configuring a firewall involves setting up rules and policies to control the flow of network traffic and define what is allowed or blocked. The specific steps to configure a firewall can vary based on the type of firewall and the software or hardware being used. Below are general steps that can guide you through the process of firewall configuration

7.3.1 How to Configure Windows Firewall

Configuring the Windows Firewall on a Microsoft Windows system involves creating inbound and outbound rules to control the traffic that is allowed or blocked. Here are the steps to configure the Windows Firewall and create rules:

Configure Windows Firewall

Step 1: To access Windows Firewall Settings:

Open the “Control Panel” on your Windows computer.

Navigate to “System and Security” and then click on “Windows Defender Firewall.”

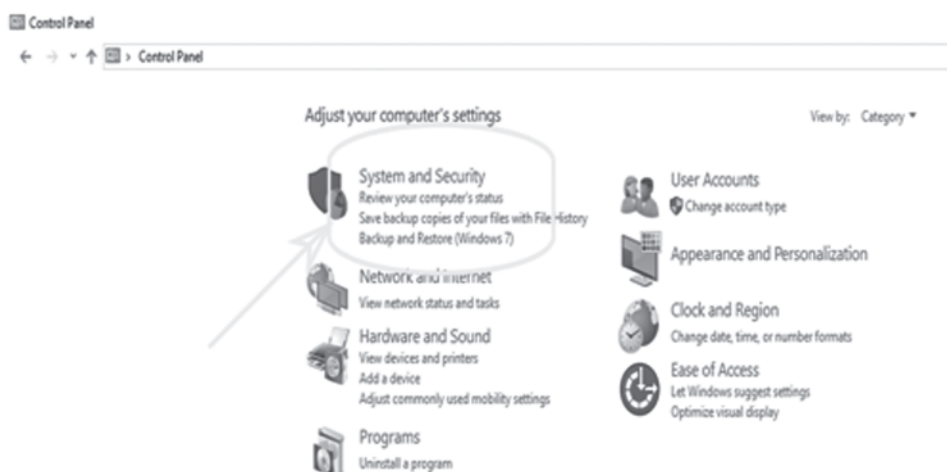


Fig. 7.7

Step 2: Choose Firewall Settings:

In the Windows Defender Firewall window, click on “Advanced settings” in the left pane. This opens the Windows Firewall with an Advanced Security window.



Notes

Introduction to Network Security

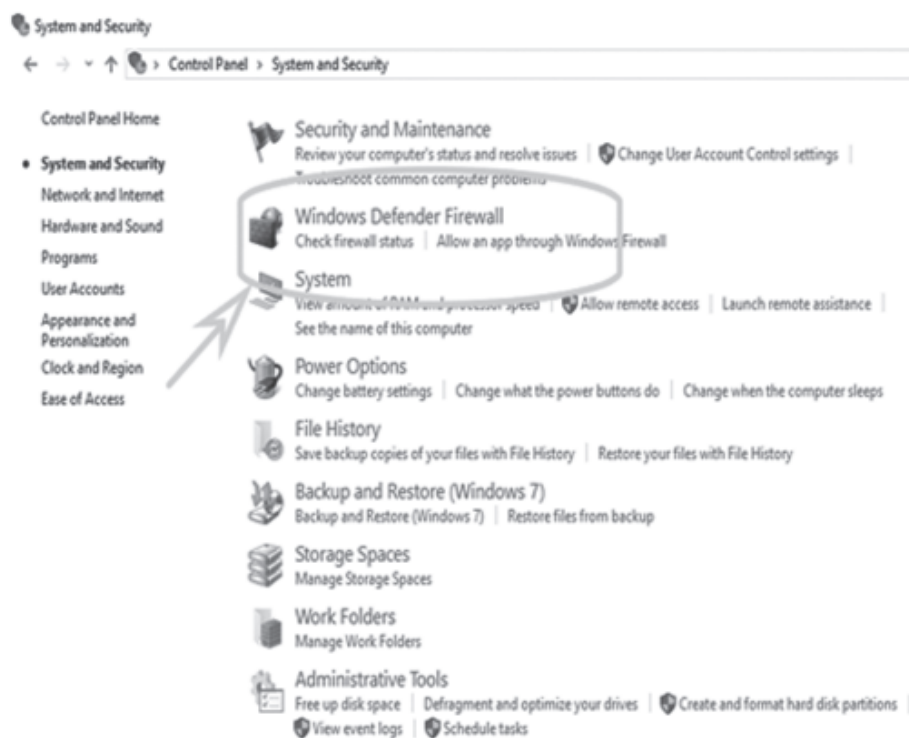


Fig. 7.8

Step 3: Create Inbound Rules: In the Windows Firewall with Advanced Security window, click on “Inbound Rules” in the left pane.

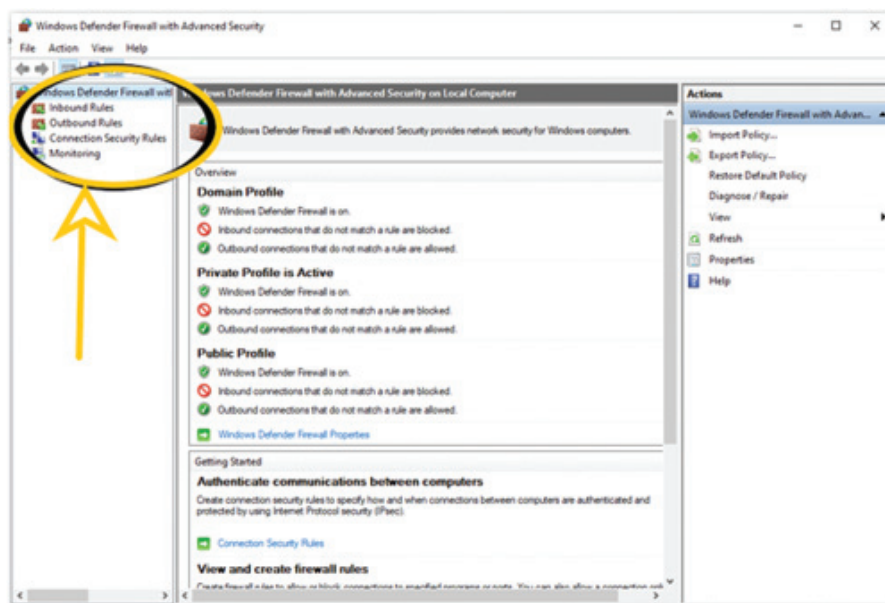


Fig. 7.9



Step 4:- Initiate Rule Creation: In the right pane, click on “New Rule...” This opens the New Inbound Rule Wizard.

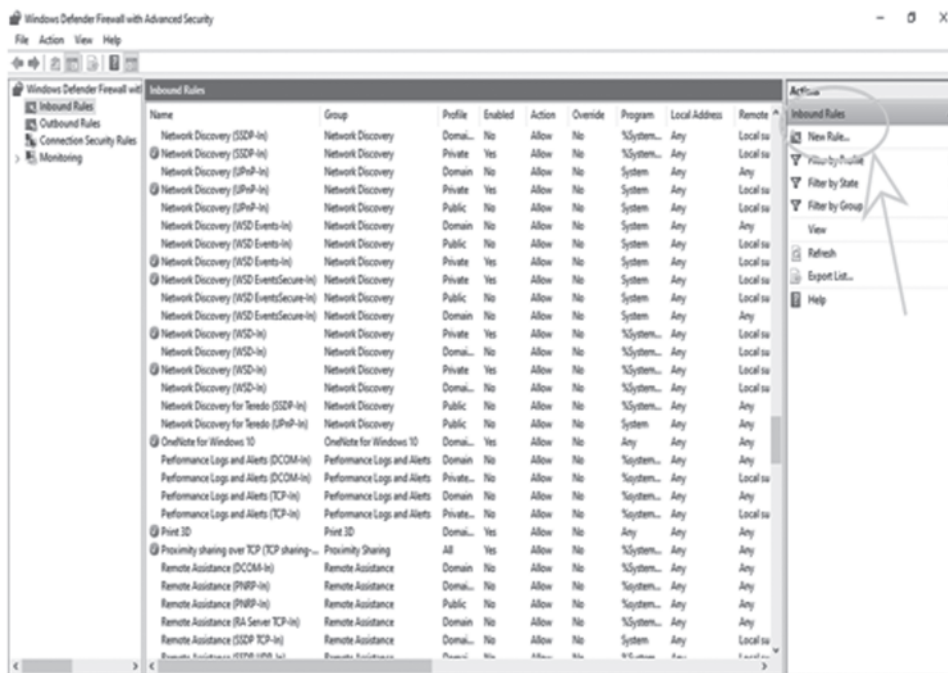


Fig. 7.10

Step 5:- Rule Type: Choose the rule type, select “Port” and click “Next.”

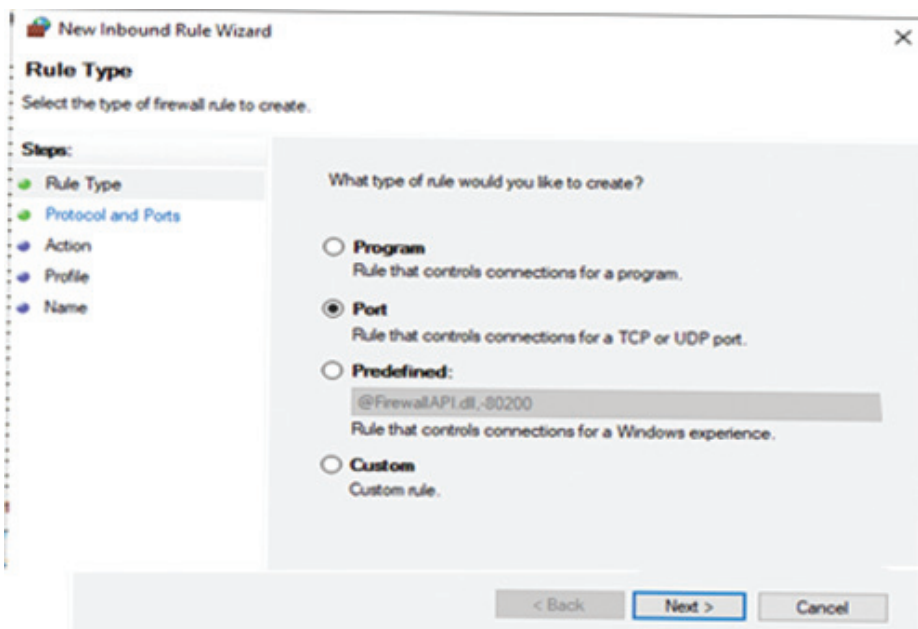


Fig. 7.11



Notes

Step 6: Protocol and Ports: Select the protocol and specify the port number for which you want to create the rule. Click “Next.”

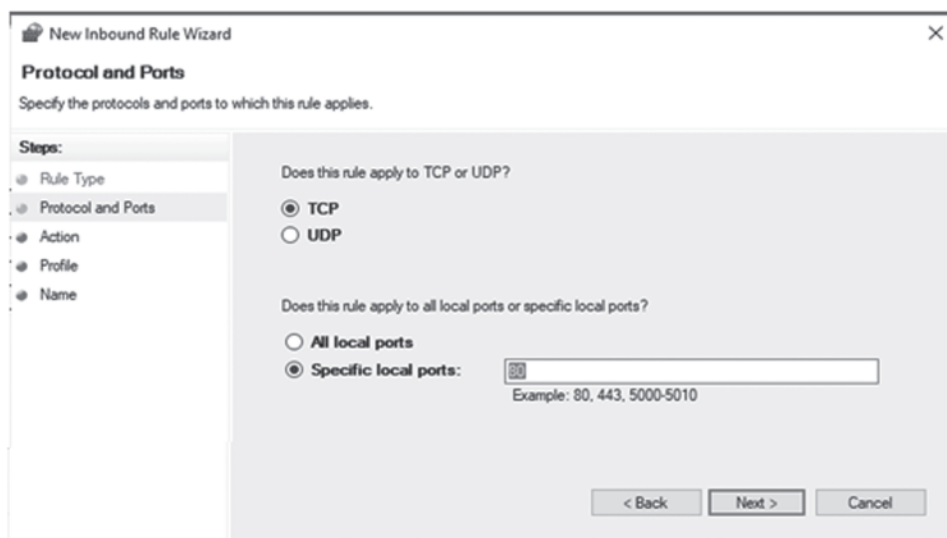


Fig. 7.12

Step 7: Action: Choose whether to “Allow the connection” or “Allow the connection if it is secure.” Click “Next.”

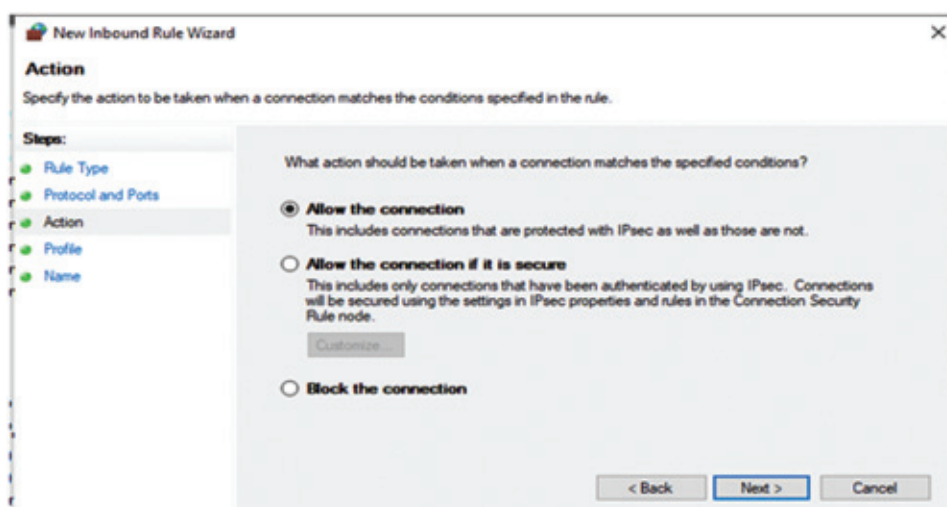


Fig. 7.13

Step 8: Profile: Select the profiles for which the rule should apply (Domain, Private, Public). Click “Next.”

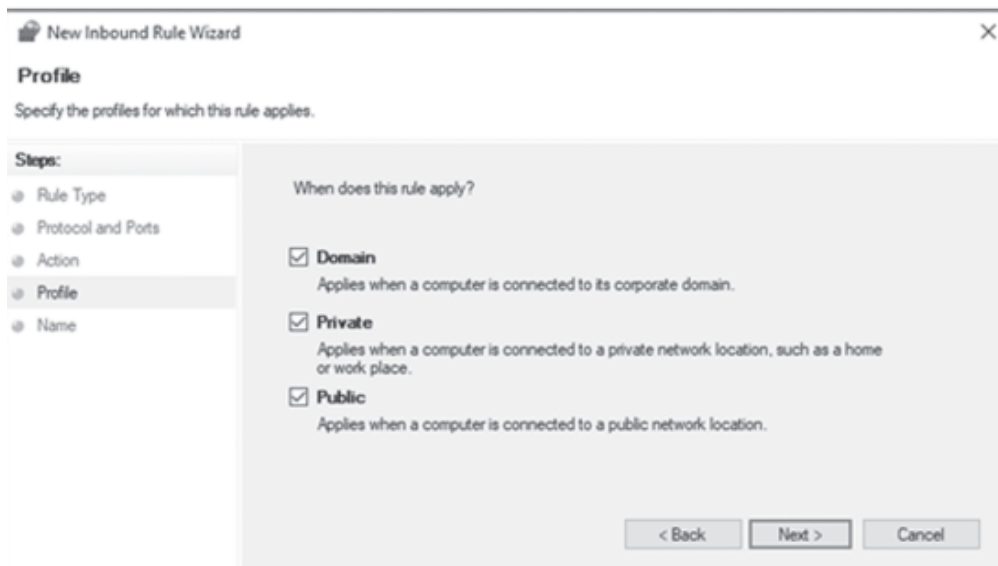


Fig. 7.14

Step 9: Name and Description: Enter a name and description for the rule. Click “Finish” to create the inbound rule.

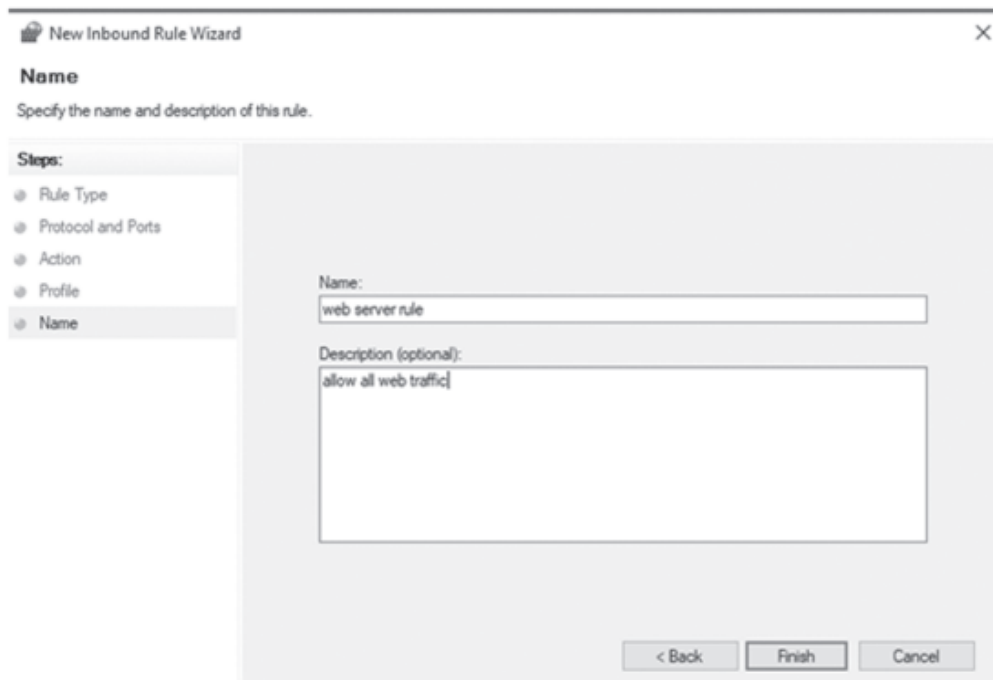


Fig. 7.15



```
bash
sudo systemctl status firewalld
```

2. Start Firewalld (if not running):

If Firewalld is not running, start it with:

```
bash
sudo systemctl start firewalld
```

3. Enable Firewalld (to start at boot):

```
bash
sudo systemctl enable firewalld
```

4. Allow SSH Traffic:

To allow SSH traffic, run

```
bash
sudo firewall-cmd --permanent --add-service=ssh
sudo firewall-cmd --reload
```

5. Allow Additional Services:

You can allow additional services by replacing “ssh” with the service name. For example, to allow HTTP

```
bash
sudo firewall-cmd --permanent --add-service=http
sudo firewall-cmd --reload
```

6. Open Specific Ports:

Alternatively, you can open specific ports. For example, to open port 8080:



Notes

```
bash

sudo firewall-cmd --permanent --add-port=8080/tcp
sudo firewall-cmd --reload
```

7.3.2.2 Using UFW:

1. Check UFW Status:

To check if UFW is installed and active, open a terminal and run:

```
bash

sudo ufw status
```

2. Enable UFW:

If UFW is not enabled, enable it:

```
bash

sudo ufw enable
```

3. Allow SSH Traffic:

To allow SSH traffic, run:

```
bash

sudo ufw allow ssh
```

4. Allow Additional Services:

You can allow additional services by specifying the service name. For example, to allow HTTP:

```
bash

sudo ufw allow http
```



5. Open Specific Ports:

Alternatively, you can open specific ports. For example, to open port 8080:

```
bash
sudo ufw allow 8080
```

6. Check Rules:

To see the configured rules:

```
bash
sudo ufw status verbose
```



IN TEXT QUESTIONS 7.3

1. The command to check the status of the firewall in ubuntu is
2. Common tools to configure firewall in linux are and
3. We can create rules in the firewall to control incoming traffic.
4. We can create rules in the firewall to control outgoing traffic.

7.4 INTRODUCTION TO WIRELESS NETWORK SECURITY

A wireless network is a type of computer network that enables devices to connect and communicate with each other without the need for physical cables or wires. It relies on wireless communication technologies, such as radio waves, infrared, or microwave signals, to transmit data between devices.

Depending on the range and purpose, wireless networks can be categorized as

- WLAN (Wireless Local Area Network)
- WPAN (Wireless Personal Area Network)
- WWAN (Wireless Wide Area Network)
- WLAN (Wireless Mesh Network)



Notes

Each type has its own advantages and limitations in terms of coverage, bandwidth, and security.

Key components of a wireless network include:

Wireless Access Points (WAPs): These are devices that enable wireless communication between devices and connect them to a wired network. WAPs act as a bridge between wireless and wired networks.

SSID: It stands for “Service Set Identifier.” It is a unique identifier that specifies the name of a wireless network. When you search for available Wi-Fi networks on your device, you see a list of SSIDs. Each wireless network has its own SSID, and users use this identifier to connect their devices to a specific Wi-Fi network.

Wireless Network Interface Cards (NICs): These are hardware components installed in devices like computers, laptops, smartphones, and other devices to enable them to connect to a wireless network.

Wireless Standards: Wireless networks follow specific standards to ensure interoperability between devices. Common wireless standards include Wi-Fi (802.11), which has various versions such as 802.11n, 802.11ac, and 802.11ax, each offering different data transfer speeds and features.

7.4.1 Wireless Security Protocols

As you know in wireless networks the communication medium is air and due to broadcast nature of wireless signals, security is a critical concern for wireless networks. To protect data during transmission against unauthorized access, data interception, and other security threats, we use encryption protocols, such as WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access). As the use of wireless technology, such as Wi-Fi, has become widespread, ensuring the security of wireless networks is crucial to protect sensitive information and maintain the privacy of users. The common wireless security protocols are as follows:

7.4.1.1 WEP (Wired Equivalent Privacy)

WEP stands for Wired Equivalent Privacy, and it is a security protocol designed to provide a wireless local area network (WLAN) with a level of security and privacy similar to wired LAN. WEP was part of the original IEEE 802.11 standard ratified in 1997, specifically for the 802.11b wireless networking standard. WEP was one of the earliest wireless security protocols. It uses a shared key for encryption but has significant security weaknesses, making it vulnerable to attacks. WEP is no longer considered secure and is not recommended for use. Therefore, the Wi-Fi Alliance officially deprecated WEP in 2004, recommending stronger alternatives like WPA and WPA2.



7.4.1.2 WPA (Wi-Fi Protected Access)

WPA was introduced as a replacement for WEP, addressing its weaknesses. It introduced TKIP (Temporal Key Integrity Protocol) for encryption and implemented a more robust key management system. However, WPA is also susceptible to some attacks.

7.4.1.3 WPA2 (Wi-Fi Protected Access 2)

WPA2 is an improvement over WPA and is widely adopted as a secure wireless protocol. It uses the more advanced AES (Advanced Encryption Standard) for data encryption and provides a higher level of security compared to WPA.

7.4.1.4 WPA3 (Wi-Fi Protected Access 3)

WPA3 is the latest and most secure wireless security protocol. It addresses vulnerabilities found in WPA2 and introduces stronger encryption methods, including individualized data encryption for each user. WPA3 is designed to enhance security in personal and enterprise Wi-Fi networks.

7.4.2 WEP vs WPA vs WPA2 vs WPA3

With the help of following table lets understand the difference among them

	WEP	WPA	WPA2	WPA3
Description	Ensure wired like privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i features and a new hardware	Announced by Wi-Fi Alliance
Release year	1999	2003	2004	2018
Encryption	RC4	TKIP+RC4	CCMP/AES	GCMP+AES
Session key size	40 bit	128 bit	128 bit	128 bit (WPA3 Personal) 192 bit (WPA3-Enterprise)
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data Integrity	CRC 32	Message Integrity Code	CBC-MAC	Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)



Notes

Introduction to Network Security

Key Management	None	Four way handshake	Four way handshake	Elliptic Curve Digital Signature Algorithm (ECDSA) and the Elliptic Curve Diffie Hellman (ECDH)
----------------	------	--------------------	--------------------	---



INTEXT QUESTIONS 7.4

- What is the primary concern addressed by wireless security?
 - Physical security
 - Network availability
 - Data confidentiality
 - Power consumption
- Which of the following wireless security protocols provides the highest level of security among these options?
 - WEP
 - WPA
 - WPA2
 - WPA3
- What does SSID stand for in the context of wireless networks?
 - Secure System Identifier
 - Service Set Identifier
 - System Security Identifier
 - Signal Strength Identifier
- Which type of attack involves intercepting and altering communication between two parties in a wireless network?
 - Jamming attack
 - Man-in-the-middle attack
 - Spoofing attack
 - Denial-of-service attack
- What is the purpose of MAC filtering in wireless security?
 - Restricting access based on device physical address
 - Filtering unwanted advertisements
 - Managing network bandwidth
 - Enhancing data encryption
- Which encryption algorithm is commonly used in WPA3, the latest Wi-Fi security standard?
 - TKIP
 - AES
 - WEP
 - RC4



7. What security vulnerability does WEP suffer from, making it obsolete for secure wireless communication?
- (a) Weak password hashing (b) Lack of encryption
(c) Vulnerable key exchange (d) Easily cracked encryption keys

7.5 ROUTER CONFIGURATION AND ITS SECURITY

When we are talking about a computer network, we have to take care of a special device known as a router which is responsible for the data transfer between the networks over the internet. Routers serve as the traffic directors of the internet, directing data packets between devices on a network and the wider web. Nowadays if we get an internet connection at home, we need to install a router at home as well. In a home, a router acts as the central hub, connecting various devices – phones, computers, smart home gadgets—to the internet. It enables wireless connectivity via Wi-Fi, allowing seamless access to online resources. Home routers often come equipped with additional features like firewall protection, parental controls, and guest networks for added security and convenience. Configurable through a web interface, they offer users control over network settings, such as Wi-Fi passwords and port forwarding. Essentially, home routers are the gateways to our digital world. Let's understand the installation and setup home router step by step.

7.5.1 Home Router Configuration

Here is the step by step process to configure the home router:-

1. **Connect the Router:**

- Plug in the power adapter and turn on your router.
- Connect your computer to the router using an Ethernet cable or connect to the router's Wi-Fi network.

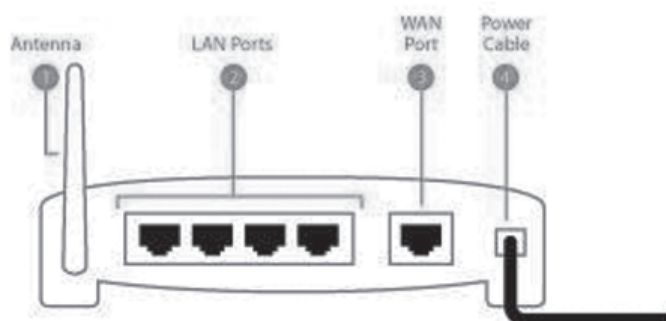


Fig. 7.17



Notes

2. **Access the Router's Interface:**

- Open a web browser on your computer (e.g., Chrome, Firefox, Safari).
- In the address bar, type the default IP address of your router. Common default addresses include 192.168.0.1 or 192.168.1.1. Check your router's manual for the exact address.

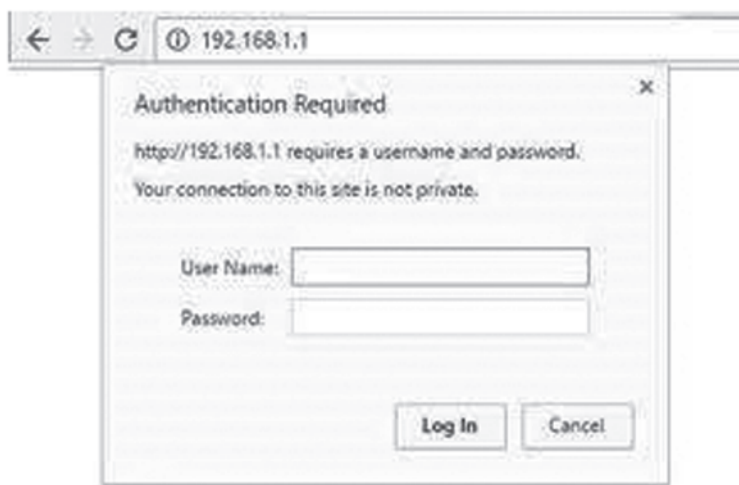


Fig. 7.18

- Press Enter. This should take you to the router's login page.
3. **Login to the Router:**
- Enter the default username and password for your router. You can find this information in the router's manual or on the sticker attached to the router itself. If you've changed the login credentials before, use those instead.
4. **Change the Default Password:**
- Once logged in, navigate to the settings or administration section of the router's interface.
 - Look for the option to change the password. Choose a strong password that is difficult to guess and preferably a mix of letters, numbers, and special characters.
 - Save your changes.
5. **Configure Network Settings:**
- You can assign a static IP address to your router or use DHCP (Dynamic Host Configuration Protocol) to automatically assign IP addresses to devices on your network.



- Set up port forwarding if you need to access specific services from outside your network, such as hosting a website or setting up a gaming server.
- Configure any additional network settings based on your requirements.

The screenshot shows the 'Internet Setup' window. At the top, there are three buttons: 'Apply', 'Cancel', and 'Test'. Below these, a question asks 'Does your Internet connection require a login?' with 'Yes' and 'No' radio buttons; 'No' is selected. The 'Account Name (If Required)' field contains 'R6400'. The 'Domain Name (If Required)' field is empty. Under 'Internet IP Address', 'Get Dynamically from ISP' is selected. Below this are fields for 'IP Address', 'IP Subnet Mask', and 'Gateway IP Address', each with a 4x4 grid of input boxes. Under 'Domain Name Server (DNS) Address', 'Get Automatically from ISP' is selected. Below this are fields for 'Primary DNS' and 'Secondary DNS', each with a 4x4 grid of input boxes. At the bottom, 'Router MAC Address' has 'Use Default Address' selected. The footer contains a 'Help Center' button and a 'Show/Hide Help Center' link.

Fig. 7.19

6. Set Up Wireless Network (Wi-Fi)

- In the router's interface, find the Wireless Settings or Wi-Fi settings section.
- Configure the SSID (network name) and choose whether you want to broadcast it or keep it hidden.
- Set the security mode. WPA2-PSK (AES) is recommended for better security.
- Choose a strong Wi-Fi password. Make sure it's different from the router's login password.
- Save/Apply your settings.



Notes

Fig. 7.20

- **Update Firmware:**
 - Check if there are any firmware updates available for your router. Firmware updates often include security patches and performance improvements.
 - If an update is available, download and install it following the instructions provided by the router manufacturer.
- **Enable Parental Controls:**
 - Some routers offer parental control features that allow you to restrict internet access for certain devices or set up content filtering. Explore these options if needed.
- **Restart the Router:**
 - Once you've made all the necessary changes, restart your router to apply the settings.



7.5.2 Overview of router Security

Home routers face various threats, including malware infiltration, which can compromise network security and steal sensitive information. Unauthorized access poses a significant risk, especially if default passwords are not changed, allowing attackers to gain control over the router and connected devices. Distributed Denial of Service (DDoS) attacks can overwhelm the router with traffic, causing network downtime. Weak passwords are susceptible to brute-force attacks, leading to unauthorized access. Firmware vulnerabilities present another danger, as outdated router software may contain security flaws. Additionally, phishing attacks targeting router settings or Wi-Fi passwords can trick users into revealing sensitive information, further jeopardizing home network security.

Change Default Passwords: Immediately change the default login credentials of your home router. Strong passwords, consisting of a mix of letters, numbers, and special characters, help prevent unauthorized access.

Enable Encryption: Enable WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key) encryption for your Wi-Fi network. This encrypts the data transmitted between devices and the router, safeguarding it from interception by unauthorized users.

Firmware Updates: Regularly update your router's firmware to patch security vulnerabilities and ensure it is equipped with the latest security features. Most routers have an option to automatically check for updates, which should be enabled.

Firewall Configuration: Activate and configure the built-in firewall on your router to filter incoming and outgoing network traffic. This helps block malicious connections and protect your home network from cyber threats.

Guest Network: If your router supports it, set up a guest network for visitors instead of sharing your main Wi-Fi password. Guest networks have restricted access to your local network resources, enhancing security for your primary devices.



WHAT YOU HAVE LEARNT

- To ensure the confidentiality, integrity, and authenticity of data as it travels between devices or systems we use Network security protocols which provides security at various layers in TCP/IP Stack
 - Network layer – IPSec



Notes

Introduction to Network Security

- Transport Layer – SSL or TLS
- Application – Kerberos , PGP
- SSL or TLS – a cryptographic protocols that play a essential role in securing communication channel over computer networks
- IPSec – It provides a framework for ensuring the confidentiality, integrity, and authenticity of data transmitted between network devices, making it a fundamental component of network security architectures.
- PGP is a data encryption and decryption program for authentication and supports message authentication and integrity checking with the help of digital signatures
- Kerberos is a centralized private key third party network protocol that provides secure authentication for network users and in a distributed network.
- VPN is a private network that uses a public network such as internet to connect remote sites or users together.
- A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on rules.
- Wireless network enables devices to connect and communicate with each other without physical cables.
- Wireless Access Points - WAPs act as a bridge between wireless and wired networks.

Suggested Practical Activities

- **Strong Password Creation:**

In today's world hackers have very strong tools and techniques to crack passwords. A strong password should be a mix of letters with uppercase and lowercase, numbers, and symbols. To check the strength of your password and how to make a strong password you may visit <https://passwordmeter.com>.

- **Enable Two-Factor Authentication (2FA):**

Only passwords are not enough to secure our online accounts. We must know how to enable to factor authentication in online portals. Login to your google account and enable 2FA for the same.

- **Configure firewall:**

Try to create some Inbound and Outbound rules in your windows and Linux.



TERMINAL EXERCISE

1. What is the need of Network Security? Explain
2. Explain the working of SSL /TLS protocol ?
3. Describe the key components and processes involved in an IPsec VPN (Virtual Private Network) connection. Highlight the role of Authentication Header (AH) and Encapsulating Security Payload (ESP)?
4. Explain the differences between Transport Mode and Tunnel Mode in IPsec. Provide scenarios in which each mode is most suitable?
5. List some benefits of using IPsec?
6. Explain the steps involved in encrypting and decrypting a message using PGP?
7. Explain the fundamental principles of Kerberos authentication protocol. Describe the key components involved in the Kerberos authentication process?
8. List some differences between remote VPN and Site-to-site VPN?
9. Explain the primary functions of a firewall in network security. Discuss the differences between packet-filtering, stateful inspection, and proxy firewalls?
10. Compare the different wireless security protocols?



ANSWERS TO INTEXT QUESTIONS

7.1

1. The main purpose of these protocols is to secure the communication channel and prevent the data from unauthorized access, interception, or tampering.
2. Four
3. Two
4. IP (Internet Protocol)
5. Philip R. Zimmermann, 1991
6. Following are the disadvantages of PGP Encryption
Compatibility issues Complexity No Recovery



Notes



Notes

7.2

1. A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined rules
2. It allows only authorized traffic to pass through the firewall and protects the network from unauthorized access.
3. Next-Generation Firewall
4. Application layer firewall provides granular control over applications and services. Can enforce security policies at the application layer.

7.3

1. `ufw status verbose`
2. `firewall-cmd , ufw`
3. `inbound`
4. `outbound`

7.4

1. (c) Data confidentiality
2. (d) WPA3
3. (b) Service Set Identifier
4. (b) Man-in-the-middle attack
5. (a) Restricting access based on device physical address
6. (b) AES
7. (d) Easily cracked encryption keys

Key Learning Outcomes

Be able to:

- Explain Network Security threats and Network Security Protocols.
- Illustrate importance of router security and setting a secure router configuration in a router.
- Describe Firewall & Network Protection
- Describe Wireless Networks and their Security



8

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Imagine your digital world as a castle, with doors and windows representing the access points to your personal data – such as passwords, emails, and financial details. Some of these entry points might have hidden weaknesses, like cracks or gaps, that someone with bad intentions could exploit.

This is where Vulnerability Assessment and Penetration Testing (VAPT) play a critical role. VAPT helps identify and fix these weaknesses, ensuring your digital castle stays secure. Regular VAPT is essential to protect against ever-evolving cyber threats.

In this lesson, we will explore the basics of VAPT, learn how to use tools like Nmap, Nessus, and Wireshark, and understand how they help ensure the safety of digital infrastructure against emerging cyber threats.



OBJECTIVES

After reading this lesson, you will be able to:

- describe Vulnerability Assessment and penetration testing;
- identify network vulnerabilities using nmap, nessus, wireshark or equivalent.

8.1 INTRODUCTION TO VA/PT

VA/PT stands for Vulnerability Assessment and Penetration Testing. It's a security testing process used to identify and address vulnerabilities in a computer system, network, or application. The assessment involves finding weaknesses and potential



Notes

Vulnerability Assessment and Penetration Testing

entry points, while penetration testing involves simulating attacks to evaluate the system's resistance to them.

List of some VAPT (Vulnerability Assessment and Penetration Testing) security tools:

- **Nessus:** A widely-used vulnerability scanner that identifies security vulnerabilities across networks, systems, and applications.
- **OpenVAS:** An open-source vulnerability scanner that provides comprehensive scanning capabilities for identifying security weaknesses.
- **Metasploit:** A penetration testing framework offering a wide range of tools for exploiting and validating security vulnerabilities.
- **Burp Suite:** A web vulnerability scanner and penetration testing tool specifically designed for testing web applications.
- **Nmap (Network Mapper):** A powerful network scanning tool used for both vulnerability scanning and network mapping.
- **Wireshark:** A network protocol analyzer used for analyzing network traffic and identifying potential security issues.

This list does not end here. we have an endless list of security tools like Acunetix, QualysGuard, OWASP ZAP (Zed Attack Proxy), SQLMap, Nikto, Aircrack-ng, John the Ripper etc which you can explore later in our cyber security journey.

8.1.1 Importance in Cybersecurity

By systematically evaluating vulnerabilities and simulating real-world cyberattacks, VAPT helps organizations preemptively strengthen their defences against malicious intrusions. It provides invaluable insights into potential entry points for attackers, allowing for targeted mitigation strategies and resource allocation. Through continuous VAPT assessments, businesses can enhance their security posture, minimize the risk of data breaches, and safeguard sensitive information. Ultimately, VAPT serves as a proactive measure to fortify cybersecurity defences and protect against evolving threats in an increasingly interconnected digital landscape.

8.1.2 Ethical Considerations

Ethical considerations are paramount in Vulnerability Assessment and Penetration Testing (VAPT) to ensure responsible and lawful practices. VAPT practitioners must obtain explicit permission from stakeholders before conducting assessments to avoid unauthorized access and legal ramifications. Respecting privacy and confidentiality is essential, with sensitive information handled securely and disclosed only to authorized parties. Additionally, VAPT activities should prioritize minimizing

disruption to systems and networks to avoid unintended consequences. Transparency in reporting findings and collaborating with organizations to implement remediation measures ethically enhances trust and fosters a culture of cybersecurity awareness. Ultimately, ethical conduct in VAPT promotes integrity, accountability, and respect for digital rights while effectively bolstering cybersecurity defenses.



Notes



INTEXT QUESTIONS 8.1

1. What does VAPT stand for?
 - (a) Virtual Application Penetration Testing
 - (b) Vulnerability Assessment and Penetration Testing
 - (c) Virtual Authentication and Protection Techniques
 - (d) Virtual Analysis and Prevention Testing
2. Which of the following best describes the purpose of VAPT?
 - (a) To develop new software applications
 - (b) To identify and remediate security weaknesses in IT systems
 - (c) To enhance network performance
 - (d) To optimize database queries
3. What is the primary difference between vulnerability assessment and penetration testing?
 - (a) Vulnerability assessment identifies security weaknesses, while penetration testing exploits them.
 - (b) Vulnerability assessment involves testing hardware, while penetration testing focuses on software.
 - (c) Vulnerability assessment is automated, while penetration testing is manual.
 - (d) Vulnerability assessment requires permission, while penetration testing does not.
4. Which of the following is an ethical consideration in VAPT?
 - (a) Conducting tests without permission
 - (b) Disregarding privacy and confidentiality
 - (c) Communicating findings transparently
 - (d) Exploiting vulnerabilities for personal gain



Notes

5. What is the importance of VAPT in cybersecurity?
- (a) It enhances network performance
 - (b) It ensures regulatory compliance
 - (c) It identifies and mitigates security weaknesses
 - (d) It optimizes system resources

8.2 PHASES OF VULNERABILITY ASSESSMENT/PENETRATION TESTING

Vulnerability assessment is a systematic process used to identify, quantify, and prioritize vulnerabilities within a system, network, application, or organization. The primary objective of vulnerability assessment is to discover weaknesses in the security posture of the target environment before they are exploited by attackers.

Penetration testing, often abbreviated as “pen testing,” is a proactive cybersecurity practice aimed at exploiting security vulnerabilities within a computer system, network, or application. Unlike vulnerability assessment, which focuses on identifying weaknesses, penetration testing involves simulating real-world cyberattacks to assess the effectiveness of existing security controls and defenses.

Penetration testers, also known as ethical hackers, use a variety of techniques, tools, and methodologies to mimic the tactics and strategies employed by malicious actors, with the goal of gaining unauthorized access to systems or sensitive data. The findings from penetration testing help organizations to prioritize remediation efforts, strengthen their security posture, and mitigate potential risks of cyberattacks.

Here are the key steps involved in VAPT process:

1. Planning

To begin the process of VAPT the very first step is to define the scope, objectives, and methodology of the VAPT engagement. We should create a list of all digital assets including network infrastructure, operating systems, applications, databases, endpoints, cloud services, and even aspects of physical security. to be tested, as well as the goals of the assessment, such as compliance requirements or specific security concerns. Vulnerability assessments may extend to assessing human factors such as user awareness, training, and adherence to security policies, as well as conducting social engineering assessments to gauge susceptibility to manipulation techniques. By defining and regularly reviewing the scope of vulnerability assessments, organizations can proactively identify and prioritize security risks.



2. Reconnaissance

Reconnaissance refers to the preparatory phase of an attack where an individual or group seeks to gather information about a target network, system, or organization. This phase is crucial for security professionals as it allows them to identify potential vulnerabilities, understand the structure of the target environment, and plan their attack strategy accordingly. Reconnaissance can be passive or active and typically involves gathering information from publicly available sources, such as websites, social media profiles, or company directories, as well as conducting technical scans and probes to identify potential weaknesses.

There are several key methods of reconnaissance in cybersecurity:

- **Passive Reconnaissance:** This involves gathering information from publicly available sources without directly interacting with the target.
- **Active Reconnaissance:** This involves more direct interaction with the target environment, often using technical tools and techniques to gather information. This could include port scanning, network enumeration, and vulnerability scanning to identify open ports, active services, and potential security vulnerabilities within the target network.
- **Social Engineering:** Social engineering techniques may also be employed during reconnaissance to manipulate individuals within the target organization into revealing sensitive information.
- **Footprinting:** Footprinting involves systematically gathering information about the target organization's internet presence, such as its domain names, IP addresses, network topology, and infrastructure. This information helps attackers understand the layout and structure of the target network, making it easier to identify potential entry points and weaknesses.

3. Vulnerability Scanning

Conduct automated vulnerability scans using specialized tools to identify known vulnerabilities within the target environment. Scan results provide a list of potential weaknesses, including software vulnerabilities, misconfigurations, and weak authentication mechanisms.

4. Vulnerability Analysis

Analyze the results of vulnerability scans to prioritize and assess the severity of identified vulnerabilities. Determine the potential impact of each vulnerability on the organization's systems, data, and operations.



Notes

5. Exploitation

After the vulnerability analysis attempt to exploit identified vulnerabilities using manual testing techniques, penetration testing tools, and custom scripts. Penetration testers simulate real-world cyberattacks to validate the existence and severity of vulnerabilities and assess the effectiveness of existing security controls.

6. Post-Exploitation

After successful exploitation, explore the compromised systems to gather additional information, escalate privileges, and demonstrate the extent of the potential damage an attacker could inflict. This phase helps organizations understand the full impact of security vulnerabilities and the risks they pose.

7. Reporting

Prepare a detailed report documenting the findings of the VAPT engagement, including identified vulnerabilities, their severity levels, exploitation methods, and recommendations for remediation. Reports should provide actionable insights and prioritize mitigation efforts based on risk severity.

8. Remediation

Work with stakeholders to address identified vulnerabilities and implement recommended security controls and best practices. Remediation activities may include applying patches, updating configurations, enhancing network segmentation, and improving employee training and awareness.

9. Reassessment

Conduct follow-up assessments to verify the effectiveness of remediation efforts and ensure that identified vulnerabilities have been adequately addressed. Regular reassessment helps organizations maintain a strong security posture and adapt to evolving threats over time.

8.2.1 Penetration Testing vs. Vulnerability Assessment

Vulnerability Assessment (VA) and Penetration Testing (PT) are both essential components of a comprehensive cybersecurity strategy, but they serve distinct purposes and have different methodologies.

Aspect	Vulnerability Assessment (VA)	Penetration Testing (PT)
Purpose	Identify and document vulnerabilities within an organization's systems, networks, and applications.	Simulate real-world cyberattacks to evaluate the security posture of an organization's systems and networks.

Vulnerability Assessment and Penetration Testing



Notes

Methodology	Relies on automated scanning tools to scan the organization's infrastructure for known vulnerabilities.	Involves manual testing techniques performed by skilled cybersecurity professionals, often referred to as penetration testers or ethical hackers.
Scope	Broader in scope, aiming to identify as many vulnerabilities as possible across the entire environment.	More focused and targeted, typically involving specific goals such as gaining access to sensitive data or compromising critical systems.
Outcome	Provides a detailed report listing identified vulnerabilities, their severity levels, and recommendations for remediation.	Provides a detailed report highlighting successful attack vectors, compromised systems, and recommendations for improving security defenses.
Key Difference	VA is proactive in identifying vulnerabilities through automated scanning.	PT is proactive in testing the effectiveness of security controls through simulated attacks.



INTEXT QUESTIONS 8.2

1. Fill in the blanks:

- The process of gathering information about a target network or system without directly interacting with it is called reconnaissance.
- The phase where penetration testers attempt to escalate privileges after successful exploitation is known as
- is a technique used during reconnaissance to systematically collect information such as IP addresses, domain names, and network topology.
- The phase of VAPT where the findings are validated by executing attacks to confirm vulnerabilities is called
- testing involves simulating cyberattacks using manual techniques to test the robustness of security defenses.

8.3 WORKING WITH VAPT TOOLS

8.3.1 Nmap

Nmap ("Network Mapper") is a free and open source utility for network investigation and security auditing used by millions of people for network



Notes

Vulnerability Assessment and Penetration Testing

discovery, administration, and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in different ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts.

While Nmap is extremely powerful, it is also complex. More than 100 command-line options add expressiveness for networking gurus, but can confuse beginners. Some of its options have never even been documented. Nmap runs on all major computer operating systems, and both command line console and graphical versions are available. Many experienced users prefer the CLI for its flexibility and efficiency, while others may find the GUI more approachable or convenient for their tasks. It's a good idea to try both and see which one works best for you in different scenarios. Let's start using Nmap.

8.3.1.1 Installation

Before you can use Nmap, you'll need to install it on your system. Nmap is available for various operating systems including Windows, Linux, and macOS.

- **Windows:** You can download the Windows installer from the official Nmap website (<https://nmap.org/download.html>) and follow the installation instructions.
- **Linux:** On most Linux distributions, you can install Nmap using the package manager. For example, on Ubuntu, you can use the following command:

```
sudo apt-get install nmap
```

8.3.1.2 How Nmap works

Once you have installed Nmap successfully on your machine, now you can start using it to perform network scans. There are various types of network scans you can perform on the target machine or target network.

The first step in a vulnerability assessment is network discovery. This reconnaissance stage determines what IP address ranges the target is using, what hosts are available, what services those hosts are offering, general network topology details, and what firewall/filtering policies are in effect.



Network administrators might focus solely on identifying active hosts running specific services, whereas security auditors are likely to be concerned with every device that has an IP address. An administrator may rely on a simple ICMP ping to discover hosts within an internal network, while an external penetration tester may deploy a variety of probes to bypass firewall restrictions.

Lets explore the phases of a Nmap scan.

- **Script pre-scanning:** The Nmap Scripting Engine (NSE) uses a collection of special-purpose scripts to gain more information about remote systems. NSE is not executed unless you request it with options such as `–script` or `–sC`.
- **Target enumeration:** In this phase, Nmap researches the host specifiers provided by the user, which may be a combination of host DNS names, IP addresses, CIDR network notations, and more.
- **Host discovery (ping scanning):** Network scans usually begin by discovering which targets on the network are online and thus worth deeper investigation. This process is called *host discovery* or *ping scanning*. Nmap offers many host discovery techniques, ranging from quick ARP requests to elaborate combinations of TCP, ICMP, and other types of probes.
- **Reverse-DNS resolution:** Once Nmap has determined which hosts to scan, it looks up the reverse-DNS names of all hosts found online by the ping scan.
- **Port scanning.** This is Nmap's core operation. Probes are sent, and the responses (or non-responses) to those probes are used to classify remote ports into states such as open, closed, or filtered.
- **Version detection:** If any ports are found to be open, Nmap may be able to determine what server software is running on the remote system. It does this by sending a variety of probes to the open ports and matching any responses against a database of thousands of more than 6,500 known service signatures.
- **OS detection:** If requested with the `-O` option, Nmap proceeds to OS detection. Nmap matches responses to a standard set of probes against a database of more than a thousand known operating system responses.
- **Traceroute:** Nmap contains an optimized traceroute implementation, enabled by the `–traceroute` option. It can find the network routes to many hosts
- **Script scanning:** Most Nmap Scripting Engine (NSE) scripts run during this main script scanning phase, rather than the prescan and postscan phases. Scripts running during this phase generally run once for each target host and port number that they interact with. They commonly perform tasks such as



Notes

Vulnerability Assessment and Penetration Testing

detecting service vulnerabilities, malware discovery, collecting more information from databases and other network services, and advanced version detection.

- **Output:** Finally, Nmap collects all the information it has gathered and writes it to the screen or to a file. Nmap can write output in several formats. Its default, human-readable format (interactive format) is usually presented but Nmap also offers an XML-based output format, among others.
- As already discussed, Nmap offers many options for controlling which of these phases are run. For scans of large networks, each phase is repeated many times since Nmap deals with the hosts in smaller groups. It scans each group completely and outputs those results, then moves on to the next batch of hosts.
- **Script post-scanning:** After Nmap has completed its scanning and normal output, scripts in this phase can process results and deliver final reports and statistics

Nmap offers various types of network scans. Let's perform some scans and understand the output.

8.3.1.3 Basic Scanning Techniques

1. **Ping Scan (-sP):** ping scan is used to check which hosts are online in a network.

```
root@rhel8:~  
[root@rhel8 ~]# nmap -sP 192.168.80.131  
Starting Nmap 7.70 ( https://nmap.org ) at 2024-02-21 12:51 IST  
Nmap scan report for rhel8.ansible.lab.in (192.168.80.131)  
Host is up.  
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
```

2. **TCP SYN Scan (-sS):** The TCP SYN scan is one of the most commonly used scanning techniques. It sends SYN packets to the target hosts and analyzes the responses to determine which ports are open.

```
[root@rhel8 ~]# nmap -sS 192.168.80.131  
Starting Nmap 7.70 ( https://nmap.org ) at 2024-02-21 12:56 IST  
Nmap scan report for rhel8.ansible.lab.in (192.168.80.131)  
Host is up (0.000039s latency).  
Not shown: 996 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
111/tcp   open  rpcbind  
2049/tcp  open  nfs  
  
Nmap done: 1 IP address (1 host up) scanned in 1.72 seconds
```



3. **Service Version Detection (-sV):** Use service version detection to determine the version of the services running on open ports.

```
[root@rhel8 ~]# nmap -sV 192.168.80.131
Starting Nmap 7.70 ( https://nmap.org ) at 2024-02-21 12:58 IST
Nmap scan report for rhel8.ansible.lab.in (192.168.80.131)
Host is up (0.000074s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.8 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.37 ((Red Hat Enterprise Linux))
111/tcp   open  rpcbind  2-4 (RPC #100000)
2049/tcp  open  nfs_acl  3 (RPC #100227)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 8.32 seconds

4. **Aggressive Scan (-A):** This option enables aggressive scanning techniques including OS detection, version detection, script scanning, and traceroute.

```
[root@rhel8 ~]# nmap -A 192.168.80.131
Starting Nmap 7.70 ( https://nmap.org ) at 2024-02-21 13:02 IST
Nmap scan report for rhel8.ansible.lab.in (192.168.80.131)
Host is up (0.000081s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.8 (protocol 2.0)
|_ ssh-hostkey:
|_ 2048 56:93:0c:17:3c:bf:fd:c5:23:7a:12:ae:a8:71:7c:a4 (RSA)
|_ 256 fe:a3:87:97:b6:53:3f:f5:d6:99:39:c2:a6:f7:48:90 (ECDSA)
|_ 256 9c:10:7d:34:61:e9:75:cb:1e:8f:15:5e:47:d7:e2:cb (ED25519)
80/tcp    open  http     Apache httpd 2.4.37 ((Red Hat Enterprise Linux))
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Apache/2.4.37 (Red Hat Enterprise Linux)
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8) .
111/tcp   open  rpcbind  2-4 (RPC #100000)
|_ rpcinfo:
|_ program version  port/proto  service
|_ 100000 2,3,4      111/tcp    rpcbind
|_ 100000 2,3,4      111/udp    rpcbind
|_ 100003 3,4        2049/tcp   nfs
|_ 100005 1,2,3      20048/tcp  mountd
|_ 100005 1,2,3      20048/udp  mountd
|_ 100021 1,3,4      36377/tcp  nlockmgr
|_ 100021 1,3,4      52919/udp  nlockmgr
|_ 100024 1          48674/udp  status
|_ 100024 1          56531/tcp  status
|_ 100227 3          2049/tcp   nfs_acl
2049/tcp  open  nfs_acl  3 (RPC #100227)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux kernel:3
OS details: Linux 3.7 - 3.10
Network Distance: 0 hops
```

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 17.30 seconds

5. **Output to File (-oN):** You can save the scan results to a file using the -oN option.



Notes

Vulnerability Assessment and Penetration Testing

```
[root@rhel8 ~]# nmap -oN scan_results.txt 192.168.80.131
Starting Nmap 7.70 ( https://nmap.org ) at 2024-02-21 13:05 IST
Nmap scan report for rhel8.ansible.lab.in (192.168.80.131)
Host is up (0.000040s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs

Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds
[root@rhel8 ~]# cat scan_results.txt
# Nmap 7.70 scan initiated Wed Feb 21 13:05:58 2024 as: nmap -oN scan_results.txt 192.168.80.131
Nmap scan report for rhel8.ansible.lab.in (192.168.80.131)
Host is up (0.000040s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs

# Nmap done at Wed Feb 21 13:05:59 2024 -- 1 IP address (1 host up) scanned in 1.73 seconds
```

8.3.1.4 Understanding the Output

Nmap provides detailed output that can be overwhelming for beginners. Here are some key elements of Nmap output:

Open Ports: Nmap lists the open ports on the target host along with the services running on those ports.

Service Versions: If service version detection (-sV) is enabled, Nmap will attempt to determine the version of the services running on open ports.

Host Status: Nmap indicates whether a host is online or not based on the results of the ping scan.

8.3.2 Wireshark

Wireshark is an open-source network protocol analyzer. It's widely used for network troubleshooting, analysis, software and communications protocol development, and education. Being open-source means its source code is freely available to the public, under the GNU General Public License (GPL). This openness fosters collaboration and community-driven development. Wireshark is a versatile network protocol analyzer, allowing users to capture, inspect, and analyze data packets traversing a network. With its intuitive interface, Wireshark provides detailed information about network traffic, including packet contents, protocols, and timing. It supports various platforms and offers powerful features such as live packet capturing, deep protocol dissecting, and customizable filters. Wireshark is indispensable for network troubleshooting, security analysis, and protocol development. Its open-source nature and active community make it a valuable tool for both beginners and experienced users in understanding and optimizing network performance and security.



Wireshark can be used for the following purposes as per the roles like:

- Network administrators use it to *troubleshoot network problems*
- Network security engineers use it to *examine security problems*
- QA engineers use it to *verify network applications*
- Developers use it to *debug protocol implementations*
- People use it to *learn network protocol internals*

8.3.2.1 Installation

Wireshark is available for various operating systems including Windows, macOS, and Linux.

- **Windows:** You can download the Windows installer from the official Wireshark website (<https://www.wireshark.org/download.html>) and follow the installation instructions.
- **MacOS:** You can install Wireshark on macOS using the installer provided on the Wireshark website or through package managers like Homebrew.
- **Linux:** On most Linux distributions, you can install Wireshark using the package manager. For example, on Ubuntu, you can use the following command:

8.3.2.2 Wireshark User Interface

Wireshark's main user interface consists of following parts.

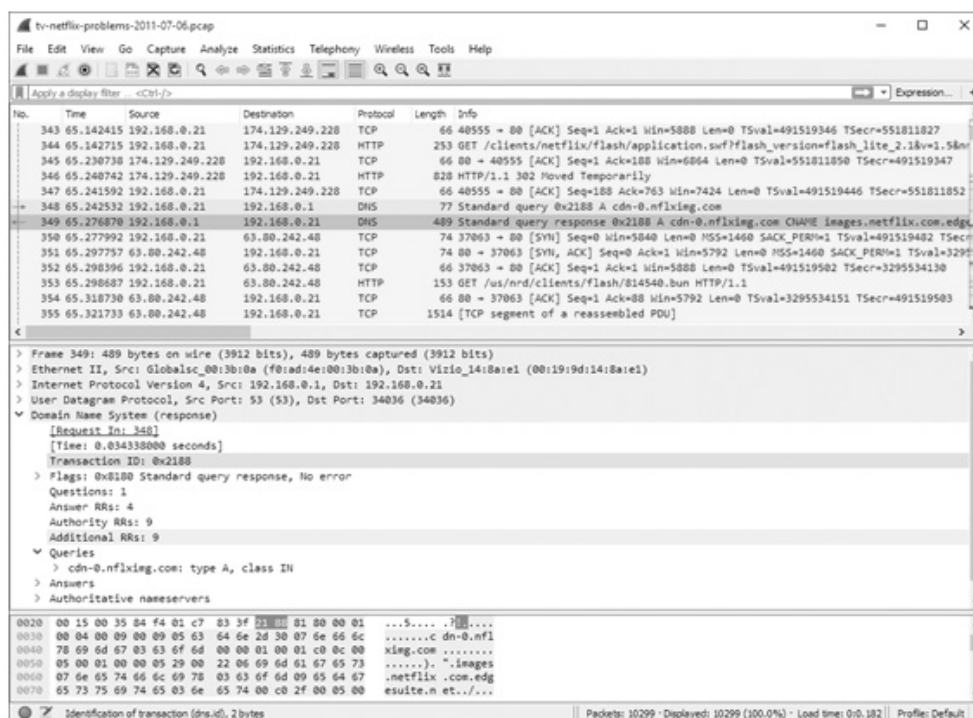
1. The *menu* is used to start actions.
2. The *main toolbar* provides quick access to frequently used items from the menu.
3. The *filter toolbar* allows users to set *display filters* to filter which packets are displayed
4. The *packet list pane* displays a summary of each packet captured. By clicking on packets in this pane you control what is displayed in the other two panes.
5. The *packet details pane* displays the packet selected in the packet list pane in more detail.
6. The *packet bytes pane* the data from the packet selected in the packet list pane, and highlights the field selected in the packet details pane.



Notes

Vulnerability Assessment and Penetration Testing

7. The *packet diagram pane* displays the packet selected in the packet list as a textbook-style diagram.
8. The *statusbar* shows some detailed information about the current program state and the captured data.



8.3.2.3 Capturing Traffic

After installing the Wireshark, you can start capturing network traffic.

Follow these steps to capture traffic

- **Open Wireshark:** Launch the Wireshark application from the Start menu (Windows) or Applications folder (macOS).
- **Select Interface:** Wireshark will prompt you to select the network interface to capture traffic from. Choose the appropriate interface (e.g., Ethernet, Wi-Fi) and click “Start” to begin capturing traffic.
- **Capture Filters (Optional):** You can apply capture filters to capture specific types of traffic. For example, you can filter by IP address, port number, or protocol.
- **Stop Capture:** To stop capturing traffic, click the “Stop” button in the Wireshark toolbar.



8.3.2.4 Analysing Traffic

Once you've captured traffic, you can analyze it using Wireshark's powerful tools and features:

- **Packet List Pane:** The main window in Wireshark displays a list of captured packets. You can view details such as source and destination addresses, protocols, and packet lengths.
- **Packet Details Pane:** Selecting a packet in the packet list pane will display detailed information about that packet in the packet details pane below. This includes protocol headers, packet data, and any other relevant information.
- **Filtering:** Wireshark allows you to apply display filters to focus on specific types of traffic. You can create custom filters based on criteria such as IP addresses, protocols, port numbers, and packet contents.
- **Statistics:** Wireshark provides various statistical tools to analyze captured traffic, including protocol hierarchy, conversations, and endpoints.

8.3.2.5 Exporting and Saving Data

Wireshark allows you to save captured traffic for later analysis or export selected packets to other formats. Here's how:

- **Save Capture File:** To save the entire capture to a file, go to File > Save As and choose a file format (e.g., pcap, pcapng) and location to save the file.
- **Export Packets:** You can export selected packets or filtered packets to formats such as CSV, JSON, or plain text. Go to File > Export Packet Dissections and choose the desired format.

8.3.2.6 Advanced Features

Wireshark offers many advanced features for experienced users, including:

- **Protocol Decoding:** Wireshark can decode and dissect a wide range of network protocols, allowing you to analyze the behavior of network traffic in detail.
- **Colorizing Packets:** Wireshark colorizes packets based on criteria such as protocol, severity, and errors, making it easier to identify important packets.
- **Scripting and Automation:** Wireshark supports scripting and automation using languages like Lua, allowing you to automate repetitive tasks or extend Wireshark's functionality.



INTEXT QUESTIONS 8.3

1. Fill in the blanks:

- (a) **Nmap** stands for “.....” and is a free and open-source utility for network investigation and security auditing.
- (b) For aggressive scanning, the option enables OS detection, version detection, script scanning, and traceroute.
- (c) The option in Nmap allows saving the scan results to a file.
- (d) The toolbar in Wireshark allows users to apply display filters to filter which packets are displayed.
- (e) In Wireshark, the pane displays the data from the packet selected in the packet list pane.
- (f) To save the entire traffic capture to a file, go to File → and choose a format like pcap or pcapng.



WHAT YOU HAVE LEARNT

- Vulnerability Assessment (VA) systematically identifies, quantifies, and prioritizes security weaknesses in systems, networks, and applications. Penetration Testing (PT), also called “pen testing,” proactively exploits vulnerabilities to evaluate and improve an organization’s cybersecurity defenses.
- Penetration testing simulates real-world attacks to test the effectiveness of security controls and identify specific ways a malicious actor could exploit a system.
- Regular reassessments ensure that organizations maintain a robust security posture and are able to adapt their defenses to evolving threats and vulnerabilities over time.
- Wireshark is an open-source network protocol analyzer used for monitoring and analyzing network traffic. It provides detailed insights into packet contents, protocols, and timing, making it a powerful tool for diagnosing network issues and investigating security events.

Vulnerability Assessment and Penetration Testing



Notes

- Nmap (Network Mapper) is a free, open-source utility used for network discovery and security auditing. It is widely utilized to identify devices, open ports, services, and potential vulnerabilities in networks.
- The installation of Nmap is straightforward and can be done on major operating systems like Windows, Linux, and macOS, enabling users to begin network scanning and security auditing.
- Nmap scanning typically includes host discovery, port scanning, service detection, and version detection. These phases provide comprehensive details about the target network's structure and security.
- Nmap offers various scan types, such as TCP connect scans, SYN scans, and UDP scans, each suited for different use cases. Understanding scan outputs is essential for analyzing network vulnerabilities effectively.



TERMINAL EXERCISE

1. What is VAPT? Explain
2. What are the primary objectives of VAPT?
3. How does Vulnerability Assessment differ from Penetration Testing?
4. What are some common tools used in VAPT?
5. What is version detection in Nmap?
6. How does OpenVAS differ from other vulnerability scanners?
7. List different types of scans which we can perform using nmap?
8. Why is it crucial for organizations to invest in VAPT processes regularly?
9. Why VAPT is considered an integral part of regulatory compliance?
10. What justifies the incorporation of VAPT exercises into employee training and awareness programs within organizations?



ANSWERS TO IN TEXT QUESTIONS

8.1

1. (b) Vulnerability Assessment and Penetration Testing



Notes

Vulnerability Assessment and Penetration Testing

2. (b) To identify and remediate security weaknesses in IT systems
3. (a) Vulnerability assessment identifies security weaknesses, while penetration testing exploits them.
4. (c) Communicating findings transparently
5. (c) It identifies and mitigates security weaknesses

8.2

1. (a) passive (b) post-exploitation (c) Footprinting
(d) exploitation (e) Penetration

8.3

1. (a) Network Mapper (b) A (c) -oN
(d) filter (e) packet bytes (f) Save As

Key Learning Outcomes

Be able to:

- Explain Vulnerability Assessment and penetration testing
- Identify network vulnerabilities and the risk involved
- Practical use of nmap, nessus, wireshark tools.



9

DIGITAL FORENSICS: PROCESSES AND DOCUMENTATION

In the previous lessons, we talked about phones, computers, and how to keep them safe from online attacks. Now, let's talk about digital forensics. It's like being a detective but in the digital world. We use special tools to find clues on electronic devices, like computers and phones, to solve cybercrimes. Digital forensics has become really important because there are more cybercrimes happening now. It helps catch the bad guys by looking for evidence on digital devices. Digital forensics is all about collecting, analyzing, and documenting electronic evidence to understand cyber incidents. It is like gathering clues from a crime scene, but the crime scene is on a computer or a phone. This helps in finding out who did what and when. It's crucial for fighting cybercrime and making sure the evidence can be used in court. Specialized knowledge is needed for digital forensics to make sure the data is collected and analyzed properly. It is like having super skills to understand how computers work and find out what happened on them.



OBJECTIVES

After learning this lesson , the learner will be able to:

- describe Digital Forensics and the objectives of Digital Forensics;
- state and describe the process of Digital Forensics;
- explain Digital Evidence and describe Evidence Collection Methods;
- operate Linux Tools for Log Analysis, Web Logs, Windows Events, and Network Events.



9.1 DIGITAL FORENSICS PROCESS

The digital forensics process involves collecting and preserving electronic evidence from devices like computers and phones. This evidence is then analyzed using specialized tools and techniques to uncover insights into cyber incidents.

9.1.1 Steps in the Cyber Forensics Investigation Model

The investigation process typically follows a structured model to ensure the proper collection, preservation, and analysis of digital evidence. One commonly used model is the Cyber Forensics Investigation Model, which outlines the key steps in the investigation process.

- (i) **Identification:** The identification phase involves recognizing and understanding the nature of the incident or cybercrime. This includes determining the type of incident, the affected systems, and the potential impact. Early identification is crucial for a timely response.
- (ii) **Preservation:** Preservation focuses on ensuring the integrity and preservation of digital evidence. It involves taking steps to prevent any alteration, damage, or loss of the electronic evidence. This may include isolating affected systems, creating disk images, and securing physical devices.
- (iii) **Collection:** In the collection phase, investigators gather digital evidence relevant to the incident. This may involve collecting data from various sources, such as computer systems, network logs, mobile devices, and cloud services. The goal is to acquire a comprehensive set of evidence while maintaining a chain of custody.
- (iv) **Examination:** The examination phase involves a detailed analysis of the collected evidence. Digital forensics tools and techniques are used to examine the data for signs of malicious activity, unauthorized access, or other relevant information. Investigators may analyze files, logs, metadata, and system artifacts.
- (v) **Analysis:** Analysis focuses on interpreting the findings from the examination phase. Investigators analyze the relationships between different pieces of evidence, reconstruct events, and determine the timeline of the incident. This phase helps in understanding the methods used by attackers and identifying the motive behind the incident.
- (vi) **Documentation:** Throughout the investigation, detailed documentation is maintained. This includes documenting the steps taken, the tools used, the findings, and any relevant information. Well-documented reports are essential for legal proceedings, incident response, and knowledge transfer.



- (vii) **Presentation:** The presentation phase involves conveying the results of the investigation to various stakeholders. This may include providing reports to law enforcement, legal teams, management, or other relevant parties. Effective communication is crucial to ensure that the findings are clearly understood.
- (viii) **Review:** After presenting the findings, a review of the entire investigation process is conducted. This helps identify any gaps, lessons learned, or areas for improvement. The feedback obtained during the review phase can be valuable for enhancing future investigations.
- (ix) **Closure:** The closure phase marks the formal conclusion of the investigation. This involves closing any legal or administrative processes associated with the incident. Proper closure ensures that all necessary actions have been taken, and the case is considered resolved.

9.1.2 Phases of the Digital Forensics Process

The cyber forensics investigation may vary based on the nature of the incident, legal requirements, and organizational policies.

Thus, the digital forensics process can be divided into several distinct phases:

9.1.2.1 Assessment

The assessment phase involves identifying potential sources of relevant information. It requires evaluating whether the investigation should be conducted internally or by an external agency, determining the need for a search warrant, and gathering preliminary information about the organization's infrastructure.

9.1.2.2 Acquisition

Acquisition is the process of gathering data from various sources, preserving its integrity, and ensuring it is admissible in court. Creating a forensically sound image of the target device is a common approach, often using bit-stream copy options to maintain the originality of the evidence.

9.1.2.3 Preservation

Preservation is as critical as acquisition. It involves safeguarding digital evidence to maintain its integrity for investigation. Proper labeling, forensically clean storage devices, and protection against environmental factors like dust and electromagnetic fields are essential.



Notes

9.1.2.4 Examination and Analysis

In this phase, digital data is examined and analyzed to draw meaningful conclusions for the case. Trained professionals use various tools and techniques to extract, restore, and interpret data. Analysis includes looking for deleted files, examining password protection, and checking for traces of data wiping software.

9.1.2.5 Documentation and Reporting

Documenting the entire process is crucial for presenting findings to a wider audience, including those less familiar with technical details. Detailed reports include information about the operating system, software, versions, actions taken during forensic investigations, keyword searches, logs, and cache details.

9.1.2.6 Creating Case Logs and Reports

1. **Gather and Organize Information:** This step involves collecting all documentation and notes from the assessment, acquisition, and analysis phases. Relevant information is identified, facts supporting conclusions are outlined, and a list of evidence to be submitted is created. This information is then organized and classified to ensure a clear and concise final report.

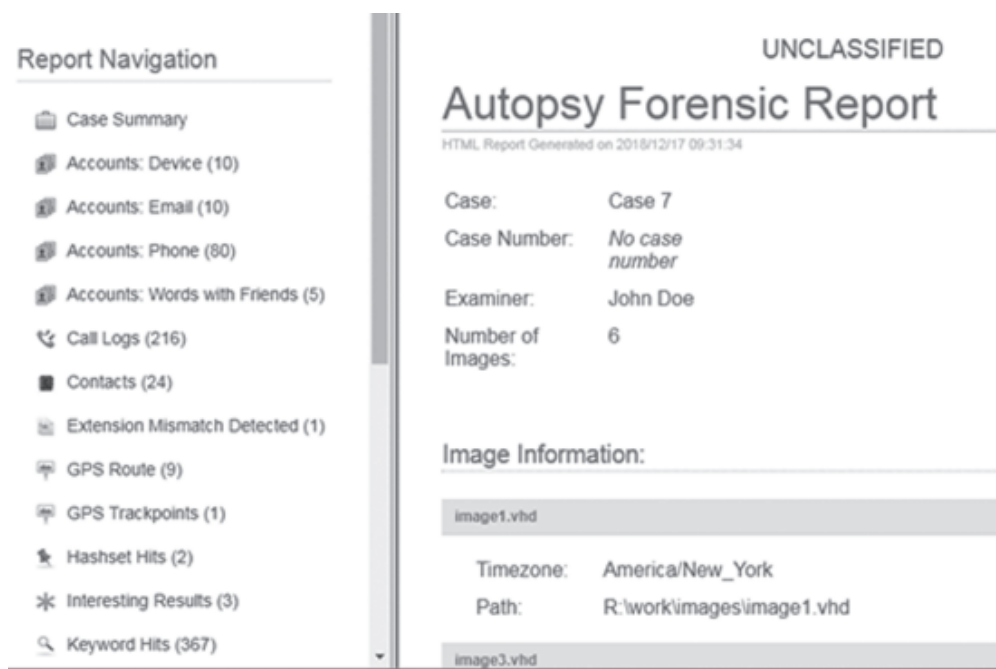


Fig. 9.1: A sample Report generated using Autopsy Software

Source: reports_html_display.png



2. **Write the Report:** Once information is organized, it is used to craft the final report. The report should clearly state the purpose, list all authors and their roles, provide an incident summary understandable to non-technical individuals, describe the evidence acquired, detail the analysis methods used, and present conclusions with supporting evidence. Supporting documents, such as network diagrams and investigation procedures, should be included.



INTEXT QUESTIONS 9.1

1. Fill in the blanks:

- (a) Digital forensics involves the systematic examination of digital devices and electronic data to uncover evidence related to incidents.
- (b) The step-by-step process of digital forensics includes assessment, acquisition, preservation,, analysis, documentation, and reporting.
- (c) Creating comprehensive case logs and reports is significant in digital forensics investigations to provide a transparent and verifiable account of the process and findings.
- (d) The primary objective of digital forensics is to identify
- (e) The process of the digital forensics involves securely collecting digital evidence.

9.2 DIGITAL EVIDENCE AND EVIDENCE COLLECTION METHODS

Digital evidence refers to information stored or transmitted in digital form that is relevant to a legal investigation. Evidence collection methods in digital forensics involve the systematic acquisition of data from electronic devices, ensuring its integrity and admissibility in legal proceedings. Forensic imaging is the process of creating an exact copy or image of a digital storage device, preserving its original state for forensic analysis without altering the original data. A **write blocker** is a hardware or software tool used to prevent any write operations to a storage device during forensic imaging, ensuring the integrity of the original evidence.

9.2.1 Digital Evidence

Digital evidence is any electronic data that can be used to investigate and solve cybercrimes. This can include information from computers, servers, mobile devices, networks, and digital storage media. Digital evidence can take various



Notes

forms, such as documents, emails, images, log files, and more. Understanding the nature of digital evidence is essential for investigators to identify and collect relevant information during an investigation.

9.2.2 Evidence Collection Methods

9.2.2.1 Forensic Imaging

It is the process of creating an exact replica or copy of a digital storage device or a subset of its data for the purpose of investigation and analysis. The primary goal of forensic imaging is to preserve the original evidence in a forensically sound manner, ensuring that the integrity of the data and authenticity of the evidence is maintained throughout the investigative process. Disk Forensics using specialized tools and techniques that create a bit-for-bit copy of the original data. The tool captures not only the file contents but also the unique identification of the device, metadata, File System i.e. structure of the storage device.

To Export a Disk image through *FTK Imager tool* (Open Source tool), you need to add evidence in the tool and then proceed to create a forensic image of the device, There is another aspect to maintain the integrity of the evidence, you need

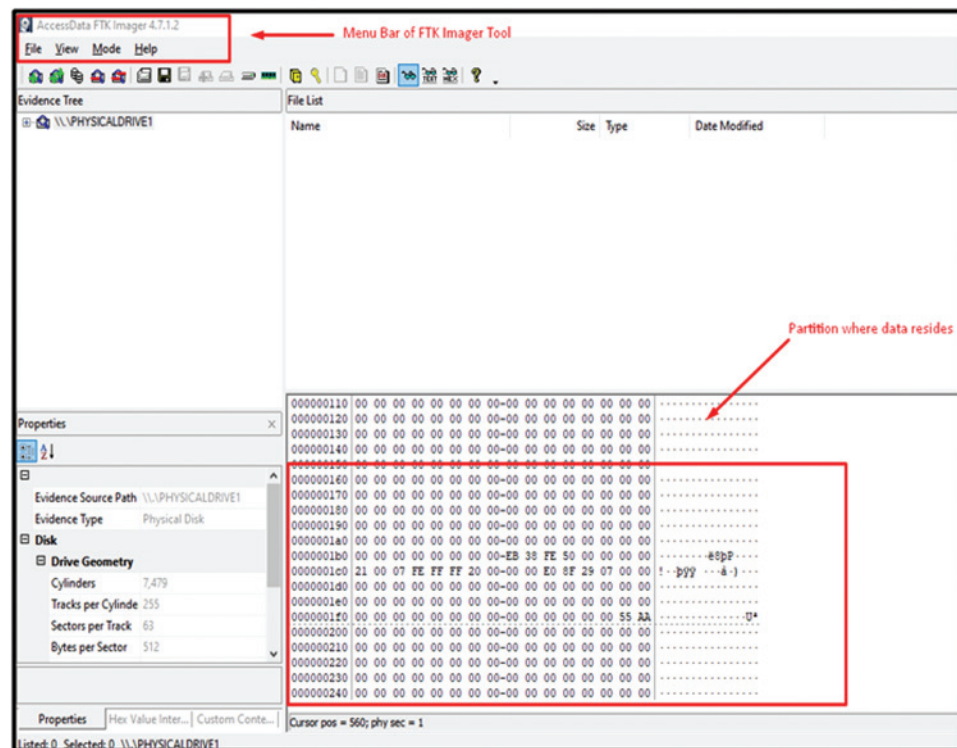


Fig. 9.2: Screenshot of demonstrating adding evidence using FTK Imager tool



to use Write blocker while connecting original evidence to the forensic computer system.

9.2.2.2 Write Blocker

A write blocker is a hardware or software device used in digital forensics to prevent any write operations to the original storage device during the process of creating a forensic image. The primary purpose of a write blocker is to ensure the integrity and preservation of digital evidence by preventing accidental or intentional alterations to the original data.

9.3 EXAMPLES OF DIGITAL FORENSICS METHODS

Collecting digital evidence requires careful planning and adherence to established methods to ensure its admissibility in court. Some key evidence collection methods include:

9.3.1 Chain of Custody

The chain of custody is a documented record of the collection, handling, and storage of digital evidence. It establishes the authenticity and integrity of the evidence by recording every person who had possession of it. This is crucial for demonstrating that the evidence has not been tampered with or altered during the investigation process.

9.3.2 Forensic Imaging

As discussed above, forensic imaging involves creating a bit-for-bit copy or image of a digital storage device. This process ensures that the original evidence remains unchanged while allowing investigators to work with a duplicate for analysis. It is essential to record details such as serial numbers, IP addresses, and hardware information during the imaging process.

9.3.3 Password Recovery

Accessing password-protected files is a common challenge in digital forensics. Password recovery methods involve using specialized tools or techniques to gain access to secured information. This may include dictionary attacks, brute-force attacks, or leveraging known vulnerabilities in encryption algorithms.

9.3.4 Network Forensics

Network forensics focuses on analyzing and monitoring network traffic to uncover evidence related to cyber incidents. This method involves capturing and



examining data packets to identify patterns, anomalies, or malicious activities within a network. Network forensics plays a crucial role in understanding the scope and impact of a cybersecurity incident.

9.4 OPERATING LINUX TOOLS FOR DIGITAL FORENSICS

Let us learn some basic Linux commands to help you get started with using Linux tools for digital forensics. Here are ten simple and essential commands:

1. Navigating the File System

- **cd directory_name:** Change directory.
- **ls:** List files and directories.
- **pwd:** Print the current working directory.
- **mkdir directory_name:** Create a new directory.
- **rmdir directory_name:** Remove an empty directory.

2. File Operations

- **cp source destination:** Copy files or directories.
- **mv source destination:** Move or rename files or directories.
- **rm file_name:** Remove or delete a file.
- **cat file_name:** Display the contents of a file.
- **nano or vi file_name:** Open a text editor to edit a file.

3. File Permissions

- **chmod permissions file_name:** Change file permissions.
- **chown user:group file_name:** Change file ownership.

4. System Information

- **uname -a:** Display system information.
- **df -h:** Show disk space usage.
- **free -m:** Display free and used memory.

5. Process Management:

- **ps:** Display information about running processes.
- **top:** Show real-time system statistics.
- **kill process_id:** Terminate a process.



6. Network Commands

- **ifconfig**: Display network interfaces and their configurations.
- **ping host**: Send ICMP echo requests to test network connectivity.
- **netstat**: Show network statistics and connections.
- **traceroute host**: Display the route that packets take to reach a network host.

7. User Management

- **whoami**: Display the current logged-in user.
- **passwd**: Change user password.
- **useradd username**: Create a new user.
- **userdel username**: Delete a user.

8. Archive and Compression

- **tar options archive_name files**: Create or extract tar archives.
- **gzip file_name**: Compress a file using gzip.
- **gunzip file_name.gz**: Decompress a file compressed with gzip.

9. Search and Find

- **grep pattern file_name**: Search for a pattern in a file.
- **find directory -name file_name**: Search for files in a directory.

10. System Shutdown/Reboot

- **shutdown**: Shut down the system.
- **reboot**: Restart the system.

9.5 IMPORTANCE OF LINUX TOOLS IN DIGITAL FORENSICS

Linux is widely used in digital forensics due to its open-source nature and powerful command-line tools. Investigators leverage various Linux tools to analyze logs, investigate web activities, examine Windows events, and monitor network events. Some commonly used Linux tools include:

9.5.1 Log Analysis

Log analysis tools on Linux help investigators review system logs to identify suspicious activities, unauthorized access, or potential security breaches. Analyzing logs is crucial for reconstructing events and understanding the timeline of a cyber incident.



Notes

9.5.2 Web Log Analysis

Web log analysis involves examining server logs to trace user activities on websites. Linux provides tools that enable investigators to analyze web logs, identify user interactions, and detect patterns indicative of malicious behavior.

9.5.3 Windows Event Analysis

The *Event Viewer* is a tool in Microsoft Windows Operating System that displays detailed information about events on computer system. Event Log is a system-generated log of events and notifications that occur on operating system. You can simply type Event Viewer app at windows start button by giving Admin privileges to access the following:

Application: Applications or programs.

Security: Logon attempts, user privilege changes, and security policy changes.

System: Device driver failures, system startup and shutdown, and critical system errors.

Setup: Software installation and system setup.

Forwarded Events: Remote computers in a centralized location.

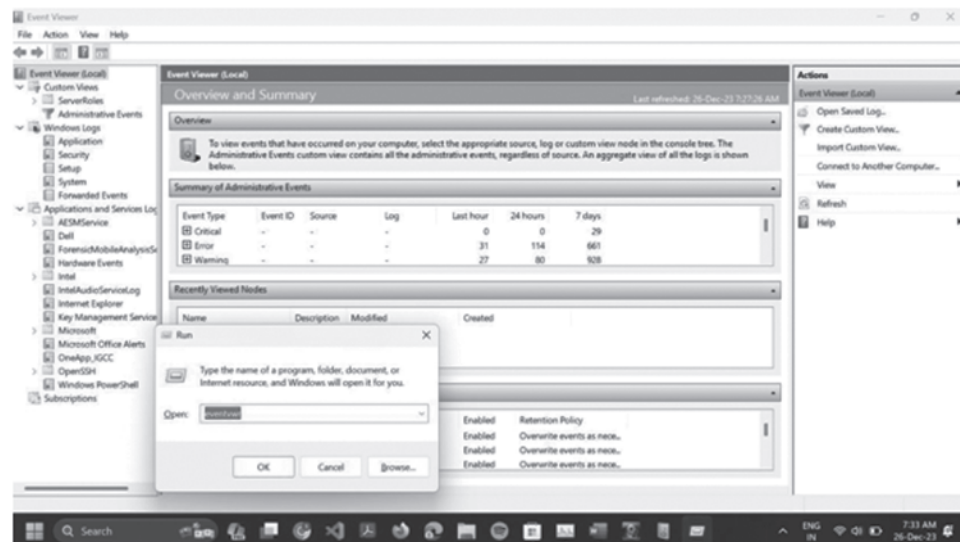


Fig. 9.3

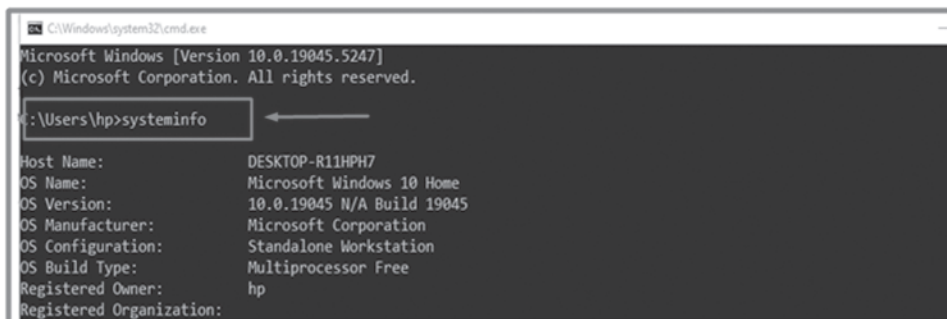
While Linux is prevalent in digital forensics, Windows environments are also common. Linux tools capable of analyzing Windows events are essential for investigators to understand activities on Windows-based systems.



Some common commands used are as follows:

#doskey /history: This will display a list of previously entered commands.

#systeminfo : To get system info of the windows OS



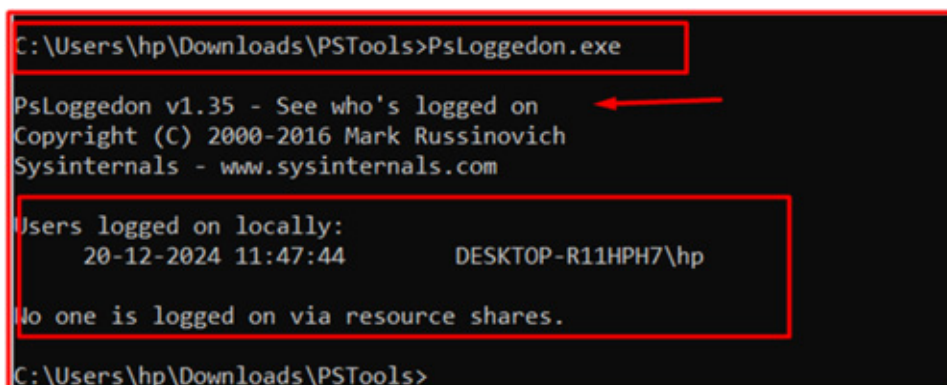
```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.5247]
(c) Microsoft Corporation. All rights reserved.

C:\Users\hp>systeminfo

Host Name:                 DESKTOP-R11HPH7
OS Name:                   Microsoft Windows 10 Home
OS Version:                10.0.19045 N/A Build 19045
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         hp
Registered Organization:
```

Fig. 9.4

During an investigation we will always need to know who all were logged on to the system. Logging to a system can be remotely or locally. Information like these can add logical view to a context or a situation. The logs can be related to an event occurrence. Many tools are available like PsLoggedon, Netsessions, logonsessions etc. to learn the instantaneous information of the users. These tools can be downloaded from the *windows sysinternals* site. *Ps* tools in sysinternals are handy in many ways.



```
C:\Users\hp\Downloads\PSTools>PsLoggedon.exe

PsLoggedon v1.35 - See who's logged on
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
    20-12-2024 11:47:44      DESKTOP-R11HPH7\hp

No one is logged on via resource shares.

C:\Users\hp\Downloads\PSTools>
```

Fig. 9.5: PsLoggedon Output

9.5.4 Network Event Monitoring for Linux

Linux tools for network event monitoring help investigators capture and analyze network traffic. By monitoring network events, investigators can identify suspicious connections, analyze data packets, and trace the source and destination of network activities.



Notes

Digital Forensics: Processes and Documentation

One popular free and open source forensics tool is “Wireshark” that is used for Network troubleshooting and Packets sniffing. You can download this by visiting www.wireshark.org

Note: Tcpdump is a command-line packet analyzer open source tool that runs on various Unix- like operating systems. It allows users to display TCP, UDP, and other packets being transmitted or received over a network to which the computer is attached.

Wireshark’s native network trace file format is the libpcap format supported by libpcap and WinPcap, so it can exchange captured network traces with other applications that use the same format, including tcpdump and CA NetMaster. It can also read captures from other network analyzers, such as snoop, Network General’s Sniffer, and Microsoft Network Monitor.

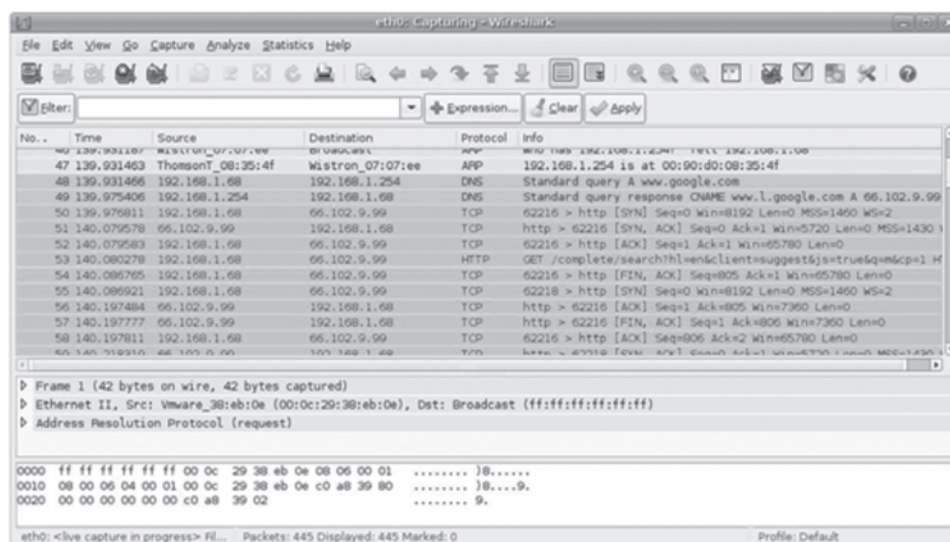


Fig. 9.6



INTEXT QUESTIONS 9.2

1. Fill in the blanks:

- Digital evidence refers to information stored or transmitted in digital form that is relevant to a investigation.
- A is a tool used to prevent write operations on a storage device during forensic imaging.



- (c) The process of creating an exact copy of a storage device for investigation is called
- (d) The ensures that every person who handled the evidence is documented to maintain its authenticity.
- (e) is a popular open-source tool used for network troubleshooting and packet sniffing.

9.6 COMMON MISTAKES AND CHALLENGES IN DIGITAL FORENSICS

9.6.1 Technical Issues

9.6.1.1 Encryption Challenges

Encrypted data poses a significant challenge for digital forensics examiners. Accessing encrypted information requires the correct key or password, which may be stored elsewhere or lost, especially in volatile memory (RAM). Live acquisition techniques are often employed to capture encryption keys.

9.6.1.2 Increasing Storage Space

The growing storage capacity of storage media presents technical challenges. Examiners need sufficient processing power and storage capacity to efficiently search and analyze large datasets.

9.6.1.3 New Technologies

The continuous evolution of technology introduces new challenges for digital forensics. Examiners must stay updated, test and experiment with new technologies, and collaborate with peers to address unfamiliar issues.

9.6.1.4 Anti-Forensics

Anti-forensics practices, such as data overwriting, file obfuscation, and metadata modification, aim to prevent forensic analysis. Detecting and countering anti-forensics techniques require advanced skills and tools.

9.6.2 Legal Issues

Several legal issues and considerations arise during the process of conducting digital forensics investigations.



Notes

9.6.2.1 Chain of Custody

Maintaining the chain of custody is crucial in digital forensics. It involves documenting and ensuring the secure handling, storage, and transfer of digital evidence to preserve its integrity. Any break in the chain of custody may affect the admissibility of evidence in court.

9.6.2.2 Admissibility of Evidence

The methods used in collecting, analyzing, and presenting digital evidence must be reliable and accepted in the laws.

9.6.2.3 Search and Seizure Laws

Investigators must comply with applicable search and seizure laws to ensure that evidence is obtained legally.

9.6.2.4 Privacy Concerns

Privacy is a concern in digital forensics, especially when investigating personal digital gadgets or data. Investigators must balance the need to collect evidence with individual's privacy rights.

9.6.2.5 Expert Testimony

The experts may be required to provide testimony in court regarding the methods used, findings, and conclusions. The experts must demonstrate their qualifications and the reliability of their methods.

9.6.2.6 Spoliation of Digital Evidence

The intentional or negligent destruction, alteration, or concealment of evidence by the Investigator may lead to legal consequences.

9.6.2.7 Trojan Defense

Legal challenges may arise, such as the Trojan Defense, where a suspect claims automated actions by a Trojan. A competent examiner should anticipate and address such arguments during the analysis and reporting stages.

9.6.3 Administrative Issues

9.6.3.1 Lack of Accepted Standards

The absence of universally accepted standards in computer forensics can create confusion. Different standards may apply to law enforcement and commercial forensics, leading to varied practices and interpretations.



9.6.3.2 Fit to Practice

In many jurisdictions, there is no standardized qualification process for computer forensics professionals. This lack of regulation may result in varying levels of competence and integrity among practitioners.

Digital forensics is a dynamic and challenging field that plays a crucial role in investigating cybercrimes. This chapter provided an overview of digital forensics, its objectives, and the comprehensive process involved in conducting investigations. Understanding digital evidence, evidence collection methods, and the importance of creating case logs and reports are fundamental aspects for professionals in this field.

9.7 CREATING CASE LOGS AND REPORTS IN DIGITAL FORENSICS

9.7.1 Importance of Case Logs and Reports

Creating comprehensive case logs and reports is a fundamental aspect of the digital forensics process. These documents serve multiple purposes, including:

9.7.1.1 Documentation of Investigation Steps

Case logs document every step taken during the investigation, ensuring a clear and traceable record of actions. This documentation is crucial for maintaining the integrity of the investigative process and providing transparency.

9.7.1.2 Admissibility in Court

Well-documented case logs and reports contribute to the admissibility of digital evidence in court. Courts require a detailed account of how evidence was collected, preserved, and analyzed to establish its authenticity and reliability.

9.7.1.3 Collaboration and Knowledge Sharing

In collaborative forensic environments, case logs facilitate knowledge sharing among team members. They provide insights into the methodologies, tools, and findings, enabling effective collaboration and continuous improvement.

9.7.2 Components of Case Logs

A comprehensive case log should include the following components:

9.7.2.1 Case Details

Include information such as case number, date and time of the incident, and a brief description of the case. This establishes the context for the investigation.



Notes

9.7.2.2 Investigator Information

Record details about the investigators involved, including their names, credentials, and roles in the investigation. This information helps attribute actions to specific individuals.

9.7.2.3 Case Objectives

Clearly outline the objectives and goals of the investigation. Define what the investigators aim to achieve and the scope of the examination.

9.7.2.4 Evidence Collection

Document the methods and procedures used for evidence collection. Specify the digital devices, storage media, or networks examined and the techniques employed.

9.7.2.5 Chain of Custody

Maintain a detailed chain of custody record, documenting every transfer of evidence between individuals. Include dates, times, and signatures to ensure the integrity of the evidence.

9.7.2.6 Tools and Techniques

List and describe the tools and techniques utilized during the investigation. Include information on software versions, configurations, and any modifications made.

9.7.2.7 Analysis and Findings

Provide a detailed account of the analysis process, including the examination of digital evidence, recovery of deleted files, decryption efforts, and any relevant findings.

9.7.2.8 Challenges and Solutions

Document any challenges encountered during the investigation and the corresponding solutions implemented. This adds context to the investigative process and demonstrates the examiner's problem-solving skills.

9.7.2.9 Recommendations

Offer recommendations based on the findings of the investigation. These may include security improvements, policy changes, or further actions to prevent similar incidents.



9.7.3 Creating Forensic Reports

Forensic reports present the findings of the investigation in a format that is understandable to non-technical stakeholders. Key components of a forensic report include:

9.7.3.1 Executive Summary

Summarize the key findings, objectives, and recommendations in a concise executive summary. This section is often the first point of contact for non-technical audiences.

9.7.3.2 Methodology

Describe the methodologies and procedures followed during the investigation. This provides context for the findings and ensures transparency.

9.7.3.3 Results and Analysis

Present the results of the analysis in a clear and organized manner. Include supporting evidence, visuals, and explanations to aid comprehension.

9.7.3.4 Conclusion

Conclude the report by summarizing the overall findings and their implications. Clearly state whether the objectives of the investigation were met.

9.7.3.5 Appendices

Include any supplementary materials, such as additional data, images, or detailed technical information, in the appendices.

9.7.4 Common Mistakes to Avoid

9.7.4.1 Lack of Detail

Inadequate documentation can compromise the integrity of the investigation. Ensure that case logs and reports provide sufficient detail to reconstruct the entire investigative process.

9.7.4.2 Omission of Challenges

Failing to document challenges faced during the investigation may hinder knowledge sharing and prevent future improvements. Be transparent about encountered difficulties and the strategies employed to address them.

9.7.4.3 Ambiguous Language

Use clear and unambiguous language in case logs and reports. Ambiguities can lead to misinterpretation and may impact the credibility of the forensic findings.



Notes

9.8 SUMMARY

We have explored the crucial aspects of creating case logs and reports in digital forensics. Understanding the significance of documentation, the components of case logs, and the structure of forensic reports is vital for professionals in the field. Users should dive deeper into specific tools, practical applications, and case studies to enhance proficiency in digital forensics.

9.9 PRACTICAL APPLICATION: CREATING CASE LOGS AND REPORTS

9.9.1 Real-world Scenario

To reinforce the importance of creating thorough case logs and reports, let's delve into a hypothetical scenario:

Scenario: Corporate Data Breach Investigation

Suppose a digital forensics team is tasked with investigating a data breach in a corporate environment. The breach involves unauthorized access to sensitive customer data, potentially compromising the company's reputation and legal standing.

9.9.2 Case Log Development

9.9.2.1 Case Details

The investigation begins by documenting essential case details:

- **Case Number:** DF-2024-001
- **Date and Time:** January 15, 2024
- **Description:** Corporate data breach involving unauthorized access to customer data.

9.9.2.2 Investigator Information

Record the investigators involved:

- **Lead Investigator:** Full Name
- **Digital Analyst:** Full Name



9.9.2.3 Case Objectives

Clearly outline the investigation's objectives:

- Identify the source of the data breach.
- Determine the extent of unauthorized access.
- Collect evidence for legal proceedings.

9.9.2.4 Evidence Collection

Document the methods used for evidence collection:

- Targeted examination of compromised servers.
- Acquisition of employee workstations for analysis.
- Capture of network traffic logs.

9.9.2.5 Chain of Custody

Maintain a detailed chain of custody:

- Secure transportation of acquired devices.
- Logging each transfer of evidence.
- Signatures of individuals handling evidence.

9.9.2.6 Tools and Techniques

List the tools and techniques employed:

- FTK Imager/EnCase Forensic for disk imaging.
- Wireshark for network traffic analysis.
- Registry and file system analysis tools.

9.9.2.7 Analysis and Findings

Document the analysis process and key findings:

- Identification of malware responsible for the breach.
- Discovery of unauthorized user accounts.
- Timeline reconstruction of the breach.



Notes

9.9.2.8 Challenges and Solutions

Detail challenges encountered and their solutions:

- Challenge: Encrypted files hindered analysis.
- Solution: Implementation of decryption tools.

9.9.2.9 Recommendations

Offer recommendations based on findings:

- Strengthen cybersecurity protocols.
- Implement regular security audits.
- Update employee training on data security.

9.9.3 Forensic Report Composition

9.9.3.1 Executive Summary

Summarize key findings for non-technical stakeholders:

- Identification of breach source and extent.
- Actions recommended for future prevention.

9.9.3.2 Methodology

Provide an overview of investigative methodologies:

- Tools used for evidence acquisition and analysis.
- Procedures followed during the investigation.

9.9.3.3 Results and Analysis

Present detailed findings in an accessible format:

- Visual representation of the breach timeline.
- Screenshots of malware and unauthorized access.

9.9.3.4 Conclusion

Summarize overall findings and implications:

- Confirmation of a targeted data breach.
- Recommendations for future security measures.



9.9.3.5 Appendices

Include supplementary materials:

- Full data breach timeline.
- Complete network traffic analysis.

9.10 NEXT STEPS

Looking ahead, by indulging interest in Digital Forensics Science will explore specific tools, techniques, and case studies to deepen your practical skills in digital forensics. Stay engaged and continue building your expertise in this dynamic field.



WHAT YOU HAVE LEARNT

- Digital forensics involves the collection, preservation, and analysis of digital evidence to investigate cyber incidents. The digital forensics process follows a structured model, including steps such as identification, preservation, collection, examination, analysis, documentation, presentation, review, and closure.
- The Cyber Forensics Investigation Model helps in organizing the investigation process, ensuring the integrity and chain of custody of evidence. The digital forensics process includes assessment, acquisition, preservation, examination, analysis, documentation, and reporting phases.
- Forensic imaging is the process of creating an exact copy of a storage device to preserve evidence for analysis. A write blocker is used during forensic imaging to prevent alterations to the original evidence.
- Evidence documentation and reporting are critical, ensuring findings are clear for stakeholders, including legal and non-technical audiences.
- **Chain of Custody** ensures the authenticity and integrity of digital evidence by documenting the collection, handling, and storage process, preventing tampering or alteration. **Password Recovery** methods such as dictionary or brute-force attacks are used to access password-protected files during investigations.
- **Network Forensics** involves capturing and analyzing network traffic to detect suspicious activity, helping to understand the scope of cybersecurity incidents.



Notes

Digital Forensics: Processes and Documentation

- **Linux Tools for Digital Forensics** provide powerful command-line utilities to assist in file system navigation, system information retrieval, process management, and network monitoring.
- **Log Analysis** tools in Linux help investigators analyze system logs to identify malicious activity and reconstruct the timeline of cyber incidents.
- **Web Log Analysis** is used to examine server logs for user activity, identifying suspicious behavior through pattern recognition.
- **Windows Event Analysis** involves using the Event Viewer tool to review system logs for significant events, such as user logins and system errors, essential for digital forensic investigations in Windows environment



TERMINAL QUESTIONS

1. Define the term “chain of custody” in the context of Digital Forensics.
2. Why is the preservation of digital evidence important during an investigation?
3. Briefly explain the purpose of the first responder toolkit in Digital Forensics.
4. What challenges do investigators face concerning encryption in computer forensics?
5. What is the significance of creating case logs and reports in the Digital Forensics process?
6. List two technical challenges faced by computer forensics examiners.
7. Explain the concept of “anti-forensics” in Digital Forensics.
8. Describe the role of a first responder in a Digital Forensics investigation.



ANSWERS TO INTEXT QUESTIONS

9.1

1. (a) cybercrime (b) examination (c) investigation
(d) digital evidence (e) collection



9.2

1. (a) legal (b) write blocker (c) forensic imaging
(d) chain of custody (e) Wireshark

Key Learning Outcomes

The learner will be able to:

- explain the objectives and steps involved in the digital forensics process, from identification to closure.
- Describe digital evidence and its collection methods, emphasizing forensic imaging and write blockers.
- Operate Linux tools for analyzing web logs, network events, and Windows events.
- Develop skills in documenting and reporting forensic investigations to ensure clarity and integrity in legal contexts.



10

OPERATING SYSTEM SECURITY

You studied the foundations of digital forensics in the last lesson. Every software and computer system design must take into account all security issues and implement the necessary safeguards to uphold security laws. Striking a balance is crucial, though, as stringent security measures can raise costs while decreasing the system's usefulness, usability, and seamless functioning. System designers must therefore offer the best possible performance without compromising security.

You will learn about the several elements of operating system security in this session, along with a variety of problems and their characteristics.



OBJECTIVES

After reading this lesson, you will be able to:

- describe Operating System Security;
- explain various threats to operating system;
- learn about Tools & Techniques for OS Security;
- describe Windows OS security;
- describe Linux OS security;
- explain about various policies in windows and in Linux OS like access control user account policies.

10.1 OPERATING SYSTEM SECURITY

The process of guaranteeing the accessibility, privacy, and integrity of the operating system is known as **operating system security**. The term “operating system security” describes the procedures and strategies used to protect the



operating system against threats including malware, worms, viruses, and remote hacker incursions. Operating system security is the umbrella term for any preventive-control measures meant to safeguard any system resources that might be lost, stolen, or altered in the case that OS security is compromised.

Ensuring the safety of computer system resources, such as software, CPU, memory, drives, etc., is referred to as security. It is capable of defending against every danger, such as viruses and illegal access. By guaranteeing the availability, confidentiality, and integrity of the operating system, it can be enforced. An unauthorized user may run a computer application and cause major damage to the computer or stored data.

10.1.1 System Security

Two violations that could jeopardize **system security** are as follows:

- (i) **Threat:** A program with the potential to cause significant harm to the system.
- (ii) **Attack:** An unauthorized access to a resource caused by a security lapse.

10.1.2 Security Breach

Malicious and **Accidental** security breaches are the **two** kinds that can damage the system. Destructive computer code or web scripts known as **malicious threats** are intended to create system vulnerabilities that result in back doors and security breaches. Conversely, **accidental threats** are relatively simpler to defend against.

Security flaws could lead to security breaches. Here are a few examples of the breaches:

- **Breach of integrity:** Unauthorized data change is the cause of this infringement.
- **Theft of service:** This refers to the misuse of resources without authorization.
- **Breach of confidentiality:** This occurs when data is read without authorization.
- **Breach of availability:** This refers to data that is destroyed without authorization.
- **Denial of service:** This refers to stopping authorized users from using the system. It's possible that some attacks are unintentional.

10.2 THREATS TO OPERATING SYSTEM

There are various threats to the operating system. Some of them are as follows:



Notes

10.2.1 Malware

It includes trojan horses, worms, viruses, and other malicious software. These are typically little bits of code that have the ability to destroy data, corrupt files, propagate themselves more widely, and even bring down a system. Important data is surreptitiously extracted by crooks while the victim user often remains unaware of the infection.

10.2.2 Network Intrusion

Rogue users, misfeasors, and **masqueraders** are the three categories of network intruders. An unauthorized user who obtains access to a system and makes use of an authorized user's account is known as a **masquerader**. A lawful user who obtains unauthorized access to programs, data, or resources and misuses them is known as a **misfeasor**. A **rogue user** assumes supervisory responsibility and attempts to avoid audit collection and access restrictions.

10.2.3 Buffer Overflow

Another name for it is buffer overrun. It is the most prevalent and hazardous operating system security flaw. It is described as an interface condition wherein more data may be entered into a buffer and data holding area than is permitted and may potentially overwrite existing data. Such an occasion is used by attackers to bring down a system or introduce malware that has been specifically designed to allow them to take over the system.

10.3 TOOLS OPERATING SYSTEM SECURITY SAND TECHNIQUES FOR OS SECURITY

System security can be achieved in a number of ways. These are listed in the following order.

10.3.1 Authentication

Authentication is the process of identifying each system user and linking the programs running with those users. The operating system is in charge of putting in place a security framework that verifies the legitimacy of a user running a particular application.

Operating systems typically employ majorly three methods to authenticate and identify users.

- (i) **Username/Password**: Before gaining access to a system, each user has a distinct username and password that must be entered accurately.



- (ii) **User Attribution:** Typically, these methods involve biometric verification—fingerprints, retinal scans, etc. Based on user uniqueness, this authentication compares the user to pre-existing database samples in the system. If there is a match, users can only grant access.
- (iii) **User card and Key:** The user must insert a key generated by a key generator into an operating system-provided option or punch a card into a card slot in order to log in to the system.

10.3.2 One Time Password

One-time passwords add an additional degree of protection to normal authentication. A different password is required each time a user tries to connect into the One-Time Password system. A one-time password cannot be used again after it has been used.

There are various ways to use one-time passwords.

- (i) **Security Key:** A hardware tool that can create a secret identity tied to the user's ID is provided to the user. Such a secret ID is requested by the system and needs to be created each time you log in.
- (ii) **Random Number:** Cards with printed alphabets and numbers are distributed to users. The algorithm asks for numbers that match a few randomly selected alphabets.
- (iii) **Network Password:** Certain commercial programs require one-time passwords to be entered before logging in, and they are sent to registered email addresses and mobile numbers.

10.3.3 Firewalls

To monitor all incoming and outgoing traffic, **firewalls** are necessary. It limits what kind of traffic is allowed to pass through it and enforces local security. Network systems or local systems can be effectively shielded from network-based security threats by firewalls.

10.3.4 Physical Security

Physical security is the most crucial way to preserve operating system security. Because operating system code and configuration files are kept on the hard drive, an attacker who gains physical access to a machine can alter, delete, or take advantage of crucial files.



Notes



INTEXT QUESTIONS 10.1

I. Fill in the blanks:

1. and accidental are two types of Security Breach
2. Buffer Overflow is also known as Buffer .
3. Unauthorized reading of data comes under Breach of .

II. State whether the following statements are true or false:

1. A masquerader is an unauthorized person who gains access to a system and uses an authorized person's account
2. Firefox is essential tool for OS Security.

10.4 WINDOWS OPERATING SYSTEM SECURITY

10.4.1 Virus and Threat Protection in Windows Security

- (i) **Access Virus & Threat Protection in Windows Security:** Windows Security includes a virus and threat protection feature and you can access this feature by following the operation below:
- Press **Windows + S**, type **Windows security** in the search box, and click Windows Security App
 - Click the **Virus & threat protection** option in the left panel or the right window to access the Virus & threat protection feature in Windows Security.
- (ii) **Virus and Threat Protection Feature:** It mainly offers protection for your device against various threats. It helps scan your computer for threats, prevents malicious programs from being installed on your computer, etc. You can run different types of scans, see the results of the previous scans, get the latest protection of Microsoft Defender, etc.
- (iii) **Different Scan for Your Device:** Although Windows Defender is turned on and automatically scans your Windows computer, you can manually perform a scan if you want.
- **Quick Scan:** If you don't want to spend much time performing a full scan for your device, you can select Quick Scan. This scan option scans various folders on your Windows computer including the Downloads



folder, Windows folder, Startup folder, and more. It may help find out suspicious files or viruses on your device.

- **Full Scan:** If a quick scan is not enough and Windows Security recommends that you should run other types of scans, you may continue to run a full scan for your computer. The Full Scan option will scan all files and running programs on your hard disk. However, it may take a long time, maybe a few hours.
- **Custom Scan:** If you like, you can also run a custom scan with Windows Security. This scan option only scans your selected files and folders. It lets you choose a file, folder, or location and perform a quick scan.
- **Offline Scan:** Some malicious files or viruses may be hard to remove from your computer. You may try the offline scan option to see if it can help you remove the tough malware or virus. Microsoft Defender Offline Scan uses the latest definitions to scan your device for the latest threats. It runs after a computer restart, without loading Windows. Save your open files before you run this type of scan.

10.4.2 Windows Defender

Windows Defender Offline, earlier called Microsoft Standalone System Sweeper Tool, is a reliable software solution to keep your computer protected from rootkits, find potentially unwanted programs and have them removed from your PC. The primary benefit of using this tool is that it runs before **malware**, such as rootkits, can hide. Apart from above, Windows Defender Offline comes equipped with the Microsoft Active Protection Service (shortly known as MAPS) that automatically reports malware to Microsoft, thus providing you with better protection.

10.5 LINUX OPERATING SYSTEM SECURITY

When it comes to security, Linux Security users are at a decided advantage over their Windows- or Mac-using counterparts. Unlike proprietary OSes, Linux is the most secure OS by design, as Linux Security features are built into the system. The increasingly popular open-source secure OS is highly flexible, configurable, and diverse. Linux Security OS also implements a strict user privilege model and offers a selection of built-in kernel security defenses to safeguard against cyber security vulnerabilities and attacks. Linux source code is transparent to make sure any network security issues are short-lived despite being inevitable on even the most secure OS.



Notes

Linux Features that make it secure are as follows:

10.5.1 User Privileges

To keep Linux secure, all users require individual IDs and passwords. In addition, the operating system offers multiple levels of access privilege, such as root-level access (which essentially receives administrative privileges). However, users are automatically assigned lower access rights, which limits their access to computer files. This is to ensure Linux is safe by making it harder for malware to spread. If a computer running Linux is compromised, the malware cannot get root access and therefore, cannot cause system-wide damage. In addition, Linux keeps each user separate, limiting the possibility of malware cross-contaminating across the system.

10.5.2 Open Source Code

The Linux Kernel operates as open-source software. Although this may lead most people to question how secure Linux is – because technically, hackers could easily insert malicious code – in reality, it boosts the operating system’s security. The source code is split into several subsystems that are carefully reviewed and maintained, which ensures that all changes are carefully vetted. In addition, because its code is open source, more people can see it and test it for vulnerabilities. Upon finding these, they can deploy code enhancements that insert security patches that help keep Linux secure.

10.5.3 System Event Logs

The Linux operating system maintains a log file that tracks all file and system accesses. These include failed login attempts, changes, and security issues. This gives administrators a useful resource for monitoring their networks and allows them to take necessary preventative measures to boost the security of their Linux systems.

10.5.4 SELinux

This is an enhancement for Linux system security that gives administrators control over file access by providing a native flexible Mandatory Access Control (MAC) system for the Linux Kernel. Essentially, SELinux allows administrators to manage security by defining access permissions for all applications, processes, and files.



10.6 VARIOUS POLICIES IN WINDOWS AND LINUX

10.6.1 Access Control

Windows supports two types of access control rules. One determines who can access the files on the disk, and the other determines who can access the data blocks on the disk. Windows allows you to have one permission list for each rule type, so users who have filesystem-level access may not have block-level access and vice versa.

Linux only supports one type of access control rule, and that rule determines who can have access to the both the files and the data blocks on the disk.

10.6.2 User Account Policy Windows

Account Lockout Policy: Indicates how many unsuccessful attempts at login are allowed before an account is locked, as well as how long the lockout lasts.

Password Policy: Sets rules for password complexity, expiration, and length.

User Rights Assignment: Defines what actions or tasks users or groups can perform on a system (e.g., shutdown, install software).

Audit Policy: Determines the level of auditing and logging for security events.

User Rights Policies: Assigns specific permissions and privileges to users or groups (e.g., granting administrative privileges).

Linux:

User Account Policies (Managed via configuration files and commands):

User and Group Management: Creation, modification, and deletion of users and groups.

Access Control Lists (ACLs): Defines access permissions for users and groups to files and directories.

Pluggable Authentication Modules (PAM): Configures authentication rules, including password policies, account lockout, and session management.

sudo Configuration: Controls privileges for specific users or groups to execute commands with elevated permissions.

File Permissions: Assigns read, write, and execute permissions to users, groups, and others for files and directories.



Notes



INTEXT QUESTIONS 10.2

I. Write the full form of following terms:

- (a) MAPS (b) MAC

II. Fill in the Blanks:

1. The Scan option will scan all files and running programs on your hard disk.
2. The Scan option only scans your selected files and folders
3. Microsoft Tool is earlier name of Windows Defender Offline.



WHAT YOU HAVE LEARNT

- The overview of Operating Security.
- The process of ensuring OS availability, confidentiality, integrity is known as operating system security
- Various Threats to Operating System.
- Security Tools for Windows and Linux OS
- A masquerader is an unauthorized person who gains access to a system and uses an authorized person's account.
- A misfeasor is a legitimate user who gains unauthorized access to and misuses programs, data, or resources.
- A rogue user takes supervisory authority and tries to evade access constraints and audit collection.
- Windows Defender is a reliable software solution to keep your computer protected from rootkits, find potentially unwanted programs and have them removed from your PC



TERMINAL EXERCISE

1. Explain various threats to Operating System
2. What are different types of Security Breach

3. What is Buffer Overflow
4. What is the use of Firewall
5. Explain Linux Features that make it secure.



ANSWERS TO INTEXT QUESTIONS

10.1

- I.** 1. malicious 2. Overrun 3. Confidentiality
- II.** 1. True 2. False

10.2

- I.** (a) **MAPS:** Microsoft Active Protection Service
(b) **MAC:** Mandatory Access Control
- II.** 1. Full 2. Custom 3. Standalone System Sweeper



Notes



11

CYBER AWARENESS

The Cyber Awareness chapter is all about helping you stay safe when using computers and the internet. After learning about keeping our operating system secure in the previous chapter, we'll now explore a bigger picture – the world of cyber threats. This includes things like viruses and tricks that people use to steal information. Understanding these threats is crucial, and we'll talk about how we can protect our personal and organizational data.

The goal is not just to give you information but to make you feel responsible for your own cyber security. We'll discuss simple things you can do, like managing your passwords well, browsing the internet safely, and recognizing when someone is trying to trick you (like in phishing emails). This chapter helps you see the connection between keeping your operating system secure and doing things to protect yourself in the broader online world. The idea is to create a mindset that understands how everything is connected when it comes to staying safe online.



OBJECTIVES

After reading this lesson, you will be able to:

- Secure usage guidelines of Social Media platform
- Digital payment system and security.
- Digital literacy and Digital Hygiene

11.1 CYBER AWARENESS

Cyber awareness means knowing and understanding the potential dangers and safety measures in the digital world. It involves being aware of different cyber threats like viruses, scams, and tricks people use to get information. Being cyber



aware also means doing things to protect you; like managing passwords well, keeping software updated, and being careful when browsing the internet.

It's not just about technical stuff, it's also about understanding what's going on in the world of online safety and how our actions affect it. Cyber awareness is like being proactive and smart about staying safe online. It's about using technology responsibly, protecting personal and organizational information, and staying informed about the always-changing world of online threats. This awareness is super important for both people and organizations to reduce risks, handle threats effectively, and help keep the digital world safe.

11.1.1 Importance of Cyber Awareness

In today's world, knowing about cyber threats is super important because it helps protect against various evolving dangers online. Since digital technology is everywhere in our lives, understanding and giving importance to cyber security is crucial. Here's why cyber awareness matters:

1. **Stopping Cyber Attacks:** It helps prevent cyber-attacks. If people and organizations know about dangers like phishing and malware, they can avoid falling into these traps. This proactive approach makes it much less likely for hackers to break into systems or steal data.
2. **Keeping Information Safe:** In a time where personal and business data are valuable to cybercriminals, being cyber aware is key to keeping this information safe. People who know about cyber security are more likely to protect their personal data, and businesses can put measures in place to safeguard important information.
3. **Avoiding Financial Losses:** Cyber incidents can cause big financial losses for individuals and businesses. Cyber awareness helps everyone put measures in place to lower the chances of falling for scams, ransomware attacks, or other harmful activities that could lead to financial consequences.
4. **Protecting Online Reputation:** Since we rely a lot on digital platforms, being cyber aware is crucial for safeguarding one's online reputation. This means understanding the risks of online activities, acting responsibly online, and protecting personal or business reputation from potential harm caused by cyber incidents.
5. **Making a Safe Digital Community:** Cyber awareness is not just about individual or business security; it's also about making the whole online world safer. When people are careful about cyber security, they help create a safer online community. This shared responsibility builds a strong and secure digital space that can handle and fight against cyber threats together.



11.1.2 Evolution of Cyber Crimes

The story of cybercrime has changed a lot as technology has gotten better and our digital world has become more connected. Let's look at how it has evolved:

1. **Early Exploitation (1970s-1980s):** At the beginning, when computers were just starting out, some people exploited weaknesses just to show off or for personal gain. This is when computer viruses and unauthorized access first appeared.
2. **Commercialization (1990s):** As the internet became more common, cybercrime turned into activities that were mostly about making money. Criminals started using things like malware and phishing to steal important info like credit cards and login details. Online shopping and banking became big targets.
3. **Globalization and Organized Crime (2000s):** The internet became a big thing worldwide, and cybercrime went from being just individuals to organized groups. Crimes like online fraud and stealing identities got more complicated, and criminals could now operate across borders.
4. **State-Sponsored Cyber Attacks (2010s):** Countries got into cybercrime, using it for political, economic, or military reasons. Big incidents like Stuxnet showed that governments could use cyber stuff for strategic goals, changing how we see cyber threats.
5. **Ransomware and Cryptocurrency (2010s-2020s):** Ransomware attacks became more common. Cybercriminals would lock up data and ask for payment in cryptocurrency to unlock it. Cryptocurrencies made it harder to catch these criminals because they could hide their transactions.
6. **IoT Exploitation and AI Threats (2020s):** More and more devices are connected to the internet, like smart fridges or thermostats. Cybercriminals started to find ways to attack these devices. Also, they started using artificial intelligence in their attacks, making it even trickier to defend against.
7. **Supply Chain Attacks (2020s):** Recently, there's been an increase in attacks on the sources of software or hardware, affecting lots of users. Cybercriminals target trusted companies or software makers, causing big problems for many people.

Cybercrime is always changing as technology grows, and cybercriminals find new ways to take advantage of weaknesses. To stay safe, it's important to have a smart and flexible approach to cyber security that deals with what's happening now and what might come in the future.



11.2 SOCIAL MEDIA PLATFORM AND ASSOCIATED CYBER CRIMES

Social media platforms have become integral parts of our daily lives, providing avenues for communication, information sharing, and social interaction. However, they also present opportunities for cybercriminals to exploit vulnerabilities and engage in various illicit activities. Here are some prominent social media platforms and associated cybercrimes:

1. Facebook

Phishing Attacks: Cybercriminals may create fake login pages or profiles to trick users into sharing their login credentials.

Fake Profiles and Impersonation: Criminals create fake profiles to impersonate individuals for fraudulent activities, such as scamming friends or spreading misinformation.

2. Twitter

Account Hijacking: Cybercriminals gain unauthorized access to Twitter accounts, often for spreading spam, fake news, or malicious links.

Phishing via Direct Messages: Criminals send phishing messages through direct messages, attempting to trick users into revealing sensitive information.

3. Instagram

Identity Theft: Cybercriminals create fake profiles to impersonate users, often to carry out identity theft or scamming activities.

Privacy Exploitation: Malicious actors exploit weak privacy settings to harvest personal information for various purposes.

4. LinkedIn

Job Scams: Cybercriminals post fake job listings or approach users with fraudulent job offers, aiming to extract personal or financial information.

Profile Scraping: Malicious actors may scrape LinkedIn profiles to gather information for phishing attacks or targeted cybercrimes.

5. Snapchat

Privacy Breaches: Despite Snapchat's ephemeral nature, users can still be targeted for privacy breaches through screenshot captures or unauthorized access to accounts.



Notes

Cyberbullying: The platform is not immune to cyberbullying, where users may be harassed, threatened, or intimidated.

6. WhatsApp

Phishing via Messages: Cybercriminals send phishing messages, often posing as someone the user knows, to trick individuals into disclosing sensitive information.

Fake WhatsApp Web Scams: Criminals trick users into scanning QR codes, giving unauthorized access to their WhatsApp accounts.

7. YouTube

Video Scams: Cybercriminals create fake videos or channels to promote scams, phishing links, or fraudulent schemes.

Comment Section Exploitation: Malicious actors may use the comment section to share malicious links or engage in social engineering tactics.

It's really important for people to stay watchful, be smart about online safety, and be careful about what they share on social media. The websites and apps you use also work hard to make sure they have good security to stop cyber threats and keep users safe.



INTEXT QUESTIONS 11.1

1. State whether the following are True or False:

- (a) Cyber awareness involves understanding potential cyber threats, risks, and security measures in the digital environment.
- (b) Cyber awareness only focuses on technical aspects of cyber security.
- (c) Being cyber aware means recognizing various types of cyber threats, such as malware, phishing, ransomware, and social engineering.
- (d) Cyber awareness only applies to organizations, not individuals.
- (e) Social media platforms are completely secure, and users don't need to worry about cybercrimes.
- (f) Cybercriminals cannot use social media to gather personal information about individuals.
- (g) Sharing personal information on social media has no impact on the risk of identity theft.



11.3 DIGITAL PAYMENT SYSTEM

A digital payment system is like a tech-based way for people and businesses to pay for things without using cash or checks. These systems are becoming more popular because they are easy, quick, and efficient. Here are some types:

1. Online Banking and Mobile Banking

What it is: Banks let you do money stuff online, like pay bills or transfer money. Mobile banking lets you do this on your phone.

How it's safe: You use a secure login, and they might ask you for two things to make sure it's really you.

2. Credit and Debit Cards

What it is: Cards you use to buy things. They're connected to your bank or credit.

How it's safe: They use chips and special tech to make sure your card is used safely. Some cards let you pay without touching anything.

3. Mobile Wallets

What it is: Apps like Apple Pay or Google Pay where you keep your card info on your phone. You can pay by tapping your phone.

How it's safe: They use special tech and might ask for your fingerprint or face to make sure it's you.

4. Digital Currencies and Cryptocurrencies

What it is: Online money like Bitcoin. No banks needed.

How it's safe: They use special codes and keys to keep it safe.

5. Peer-to-Peer (P2P) Payment Platforms

What it is: Apps like PayPal or Venmo to send money to friends.

How it's safe: They use codes and checks to make sure your money goes to the right person.

6. QR Code Payments

What it is: Scanning a code to pay. People or shops make the code for you to scan.

How it's safe: The codes use special tech and might change to stay safe.



7. Near Field Communication (NFC) Payments:

What it is: Paying by putting your phone close to a thing.

How it's safe: They use special tech and might ask for more security stuff.

These systems are always getting better with new tech, and they make sure your money is safe from bad things.

11.3.1 Security of Digital Payment System

Security Aspect	Description
Encryption and SSL	Utilizes strong encryption protocols such as SSL to secure data transmission, ensuring the confidentiality and integrity of information during digital trans-actions.
Multi-Factor Authentication	Implements multi-factor authentication methods, including passwords, biometrics, or one-time passcodes, to add an additional layer of security and verify the identity of users initiating transactions.
Tokenization	Applies tokenization to replace sensitive information (e.g., credit card numbers) with unique tokens, reducing the risk of unauthorized access to sensitive data and enhancing overall transaction security.
Fraud Detection and Prevention	Incorporates robust fraud detection systems that employ machine learning algorithms and anomaly detection to identify and prevent suspicious activities, minimizing the risk of fraudulent transactions.
Regulatory Compliance	Adheres to relevant regulatory standards and compliance requirements, ensuring that the digital payment system meets industry-specific security standards and legal obligations to protect user data and privacy.

This table highlights key security aspects of a digital payment system, emphasizing the importance of encryption, multi-factor authentication, tokenization, fraud detection, and regulatory compliance in safeguarding transactions and user information.



11.4 CYBER CRIME

Cyber crime is a tricky and always-changing type of crime that uses computer systems and the internet to do bad stuff. As our world gets more digital, people who do cybercrime (we call them hackers or cybercriminals) use smart ways to target normal people, businesses, and even governments. They do it for money, politics, or just because they can. Cyber crime includes lots of illegal activities done online, and it can happen across borders, making it hard for traditional law enforcement to catch them.

Cybercriminals use different tricks like hacking, phishing, putting harmful stuff (malware) on your computer, and stealing identities. This can lead to losing money, getting unauthorized access to important information, messing with important systems, and even putting a whole country in danger.

Cyber crime comes in many forms, from one person doing online scams to big, organized attacks by countries trying to spy on each other. Targets can be banks, online shops, important systems, and regular people who might fall for scams.

Because technology is always changing, stopping cybercrime is tough. Cybercriminals keep finding new ways to do bad stuff, and the internet is everywhere, making it hard for cops to catch them. So, we need a bunch of things to stop cybercrime – good online security, laws to punish cybercriminals, countries working together, and people knowing how to stay safe online.

As we use more and more digital stuff, it's super important for everyone – regular people, companies, and governments – to understand the risks of cybercrime and work together to stay safe. This way, we can keep our digital world secure and protect against all kinds of cybercrimes.

11.4.1 Types of Cyber Crime

Cyber crime encompasses a wide range of illicit activities conducted in the digital realm, exploiting vulnerabilities in computer systems, networks, and online platforms. Here are some common types of cyber crimes:

1. **Hacking:** Unauthorized access to computer systems or networks to gain information, disrupts services, or deploys malicious activities.
Example: Intrusion into a corporate network to steal sensitive data.
2. **Phishing:** Deceptive attempts to obtain sensitive information, such as usernames, passwords, and financial details, by posing as a trustworthy entity in electronic communication.
Example: Fake emails pretending to be from a bank, requesting users to provide login credentials.



Notes

Cyber Awareness

3. **Malware:** Malicious software designed to damage, disrupt, or gain unauthorized access to computer systems. Includes viruses, worms, trojan horses, ransomware, and spyware.

Example: Ransomware encrypting files and demanding payment for their release.
4. **Identity Theft:** Unauthorized use of someone's personal information, such as Social Security numbers or credit card details, to commit fraud or other criminal activities.

Example: Opening bank accounts or applying for credit using stolen personal information.
5. **Online Fraud:** Various fraudulent activities conducted on the internet, including online scams, fake auctions, credit card fraud, and deceptive practices to deceive individuals or organizations.

Example: Non-existent online sales with the intention to collect payment without delivering goods.
6. **Denial-of-Service (DoS) Attacks:** Deliberate attempts to overwhelm a computer system, network, or website with excessive traffic to disrupt its normal functioning, rendering it temporarily or permanently unavailable.

Example: Flooding a website with traffic to make it inaccessible to legitimate users.
7. **Cyber Espionage:** Covert activities aimed at obtaining sensitive information from individuals, organizations, or governments for political, economic, or military purposes.

Example: State-sponsored hacking to steal classified information from another country's government.
8. **Financial Cybercrimes:** Crimes targeting financial institutions or individuals, including online banking fraud, credit card fraud, and cryptocurrency-related crimes.

Example: Unauthorized access to online banking accounts to transfer funds illegally.
9. **Cyberbullying:** Harassment, intimidation, or humiliation of individuals using digital platforms, often through social media, messaging apps, or email.

Example: Posting offensive or threatening messages on social media to harm an individual's reputation.



10. **Data Breaches:** Unauthorized access and theft of sensitive data stored by organizations, resulting in the exposure of personal or confidential information.

Example: Hackers gaining access to a company's database and stealing customer information.

These examples represent a fraction of the diverse and constantly evolving landscape of cybercrime. The complexity of cyber threats requires a comprehensive approach to cyber security to mitigate risks and protect individuals and organizations from various cybercriminal activities.

11.4.2 Cyber Law

Cyber law is like the rules and regulations that help manage things in the digital world. It covers a lot of legal stuff related to using the internet and technology. The main goal is to make sure that people, businesses, and governments are protected when they're online. Cyber law deals with important things like online shopping, keeping your data safe, and fighting against cybercrimes.

It gives us guidelines for doing things online, tells us what rights and duties we have in the digital world, and sets rules to stop cyber threats. Cyber law also deals with tricky issues like who owns things online, keeping our personal info private and handling new tech challenges.

As technology keeps getting better, cyber law has to keep up with new problems. There are more and more cybercrimes like hacking, stealing identities, and online fraud. Cyber law also has to figure out how to deal with problems that happen across different parts of the world. Balancing the need for new tech ideas with keeping everyone's rights safe is a big challenge for the people who make and follow cyber law rules. In the end, cyber law helps make sure our digital world is safe, fair, and follows the rules as technology keeps evolving.

11.4.3 Key Components of Cyber Law

The key components of cyber law encompass a wide array of legal principles and regulations that collectively address the challenges and opportunities arising from the use of information technology and the internet. Here are some fundamental components:

1. **Electronic Commerce (e-Commerce):** It Governs online commercial transactions, electronic contracts, and consumer protection in the digital marketplace. It establishes legal frameworks for online businesses, digital signatures, and electronic payment systems.



Notes

2. **Data Protection and Privacy:** Regulates the collection, processing, and storage of personal and sensitive data online. It establishes individuals' rights to privacy and outlines obligations for organizations to safeguard user information.
3. **Cybercrime Legislation:** Encompasses laws addressing various cybercrimes such as hacking, identity theft, online fraud, and computer-related offenses. It outlines legal measures for the investigation, prosecution, and punishment of cybercriminal activities.
4. **Intellectual Property Protection:** Addresses issues related to the protection of intellectual property in the digital realm. This includes laws governing copyright, trademarks, patents, and digital piracy, ensuring the fair use and protection of creative works.
5. **Cyber security and Computer Security:** Establishes legal frameworks for ensuring the security and integrity of computer systems, networks, and data. It often includes regulations for preventing unauthorized access, data breaches, and cyber-attacks.
6. **Online Defamation and Cyberbullying:** It governs legal aspects related to online defamation, libel, and cyber bullying. It provides legal remedies for individuals or entities harmed by false or harmful statements made on the internet.
7. **Electronic Evidence and Digital Forensics:** Addresses the admissibility and handling of electronic evidence in legal proceedings. It also outlines the use of digital forensics in investigating cybercrimes and ensuring the integrity of digital evidence.
8. **Regulation of Internet Service Providers (ISPs) and Platforms:** Governs the responsibilities and liabilities of internet service providers and online platforms. It includes regulations related to content moderation, user agreements, and the liability of hosting illegal or harmful content.
9. **Cyber Ethics and Internet Governance:** Encompasses legal principles and guidelines for ethical conduct in cyberspace. It may include regulations related to internet governance, standards for responsible online behavior, and international cooperation in addressing global cyber challenges.
10. **Jurisdiction and Cross-Border Issues:** Addresses legal challenges related to jurisdiction in cyberspace, particularly when online activities transcend traditional geographical boundaries. It involves determining which legal jurisdiction should govern a particular online incident.



These key components collectively form the foundation of cyber law, creating a legal framework that aims to protect the rights of individuals, ensure the fair and secure use of technology, and address the challenges posed by the dynamic and interconnected nature of the digital world.

11.5 DIGITAL LITERACY

Digital literacy means knowing how to use and understand digital technology well. It includes having the skills to work with things like computers, apps, and online tools for different reasons, like talking to people, finding information, solving problems, and working together with others. In the world we live in today, being digitally literate is really important. It helps people take part in the digital world and make the most of all the good things that come with technology. The main parts of digital literacy include:

1. **Basic Digital Skills:** Understanding fundamental digital tools and concepts, such as using computers, operating systems, word processing, and file management.
2. **Information Literacy:** Evaluating, critically analyzing, and effectively using digital information from various sources. This includes the ability to assess the reliability and credibility of online content.
3. **Media Literacy:** Understanding and critically engaging with various forms of digital media, including images, videos, and news articles. This involves the ability to interpret media messages and distinguish between different types of media.
4. **Communication Skills:** Effectively communicating through digital channels, including email, social media, instant messaging, and video conferencing. This also includes understanding online etiquette and responsible digital communication.
5. **Cybersecurity Awareness:** Recognizing and practicing good cybersecurity habits to protect personal information and devices from online threats. This involves understanding the risks associated with online activities and implementing security measures.
6. **Critical Thinking and Problem-Solving:** Applying critical thinking skills to solve problems, make informed decisions, and adapt to new technologies. This includes the ability to troubleshoot digital issues and find solutions independently.



Notes

7. **Digital Citizenship:** Understanding the rights, responsibilities, and ethical considerations associated with digital participation. This includes respecting online communities, practicing responsible digital behavior, and contributing positively to the digital environment.
8. **Adaptability to Technological Changes:** Embracing a growth mindset and being open to learning and adapting to new technologies. Digital literacy involves staying updated on technological advancements and being able to navigate changes in digital tools and platforms.
9. **Collaboration Skills:** Effectively collaborating with others using digital platforms and tools. This includes participating in online teamwork, using collaborative software, and understanding the dynamics of virtual collaboration.
10. **Digital Accessibility:** Ensuring that digital resources and technologies are accessible to individuals of all abilities. This involves considering inclusivity in the design and use of digital tools and content.



INTEXT QUESTIONS 11.2

1. Fill in the blanks:

- (a) Cybercrime is a form of activity that exploits vulnerabilities in digital technologies and the internet.
- (b) Cybercriminals use tactics like hacking, phishing, malware attacks, and identity theft to compromise the security of systems and networks.
- (c) Cybercrime can result in financial losses, unauthorized access to sensitive information, and even threats to security.
- (d) The increasing prevalence of cybercrimes underscores the importance of a robust legal framework to combat
- (e) Cyber law encompasses legal principles and regulations designed to govern issues arising from the use of technology and the internet.
- (f) Cyber law plays a pivotal role in establishing the legal framework for activities conducted in
- (g) As technology advances, cyber law faces ongoing challenges in addressing new and sophisticated issues.
- (h) Cyber law serves as a critical tool in shaping a secure, ethical, and accountable digital environment where legal norms evolve alongside advancements.



11.6 DIGITAL HYGIENE

Digital hygiene refers to the set of practices and habits individuals adopt to maintain a healthy and secure digital presence while using technology and engaging with online platforms. Similar to personal hygiene, which involves practices to maintain physical health, digital hygiene aims to safeguard individuals from online threats, protect personal information, and ensure a positive and secure digital experience. Key aspects of digital hygiene include:

1. **Password Management:** Use strong, unique passwords for different online accounts. Regularly update and change passwords to enhance security. Consider using password management tools for secure storage.
2. **Software Updates:** Keep operating systems, antivirus software, and applications up to date. Enable automatic updates to ensure timely installation of security patches.
3. **Secure Wi-Fi Practices:** Use strong, unique passwords for Wi-Fi networks. Enable encryption protocols, such as WPA3, for secure wireless communication. Regularly update router firmware to address vulnerabilities.
4. **Phishing Awareness:** Be cautious of unsolicited emails, messages, or links. Verify the authenticity of requests for personal information. Avoid clicking on suspicious links or downloading attachments from unknown sources.
5. **Device Security:** Set up screen locks, PINs, or biometric authentication on devices. Enable device tracking and remote wipe features for smartphones and tablets. Install reputable antivirus and anti-malware software.
6. **Privacy Settings:** Review and adjust privacy settings on social media platforms and online accounts. Limit the amount of personal information shared publicly. Regularly audit and update privacy preferences.
7. **Backup Your Data:** Regularly back up important files and data. Use cloud storage or external drives for secure data backup.

Ensure backup systems are functioning correctly.
8. **Two-Factor Authentication (2FA):** Enable 2FA for additional account security. Use authentication apps or hardware tokens when available.
9. **Social Media Awareness:** Be mindful of the information shared on social media. Review and adjust post visibility settings.



Notes

Be cautious about accepting friend or connection requests from unknown individuals.

10. **Educate Yourself:** Stay informed about common cybersecurity threats and best practices. Participate in cybersecurity awareness programs and training. Report any suspicious activities to appropriate authorities.

If you follow these digital cleanliness tips, you can make it less likely that bad online stuff will happen to you. It helps keep your personal info safe and makes the digital world a better and safer place. Remember to check and update your digital cleanliness habits because technology and online safety always change.

11.7 DIFFERENCE BETWEEN DIGITAL LITERACY AND DIGITAL HYGIENE

Aspect	Digital Literacy	Digital Hygiene
Definition	Refers to the ability to use digital tools, technologies, and platforms effectively for various purposes.	Encompasses practices and habits to maintain a healthy and secure digital presence, focusing on online safety and security.
Scope	Encompasses a broad range of skills, including information retrieval, communication, critical thinking, and collaboration in the digital realm.	Focuses specifically on practices that promote online security, protect personal information, and prevent cyber threats.
Skills and Competencies	Involves skills such as information literacy, media literacy, communication skills, critical thinking, and adaptability to technological changes.	Involves practices such as password management, software updates, secure Wi-Fi usage, phishing awareness, and device security.
Purpose	Empowers individuals to engage meaningfully with digital technologies and leverage them for personal, academic, and professional purposes.	Aims to safeguard individuals from online threats, protect privacy, and ensure a secure and positive digital experience.
Application	Applicable to a wide range of digital activities, from using social media to conducting online research and participating in e-commerce.	Applicable to specific practices aimed at maintaining a secure digital environment, such as securing passwords, updating software, and avoiding phishing attempts.



Examples	Understanding how to use digital tools for research, creating digital content, and participating in online discussions.	Creating strong, unique passwords, regularly updating software, being cautious of phishing emails, and securing Wi-Fi networks.
Long-Term Goals	Fosters a holistic understanding of digital technologies and their applications, supporting lifelong learning in the digital age.	Establishes habits and practices that contribute to ongoing online safety and security, reducing the risk of falling victim to cyber threats.



INTEXT QUESTIONS 11.3

1. Fill in the Blanks:

- Digital hygiene involves adopting and regular software updates to maintain a healthy and secure digital presence.
- To enhance account security, enable for an additional layer of protection.
- Digital literacy focuses on the ability to use digital tools effectively, while digital hygiene emphasizes password management and awareness.
- Regularly updating, antivirus software, and applications is a key aspect of digital hygiene.
- Reviewing and adjusting settings on social media platforms helps protect personal information.



WHAT HAVE YOU LEARNT

- Cyber Awareness** is the understanding of potential risks in the digital world and the steps required to stay safe online. This includes knowing about threats like phishing, scams, and malware, and using practices such as strong passwords and updated software to mitigate risks.
- Cybercrimes** have advanced from simple virus creation in the 1970s to sophisticated attacks using AI and targeting supply chains in the 2020s. Cybercriminals continually exploit new technologies and vulnerabilities.
- Platforms like Facebook, Twitter, Instagram, and LinkedIn are often misused for phishing, impersonation, account hijacking, privacy exploitation, and scams.



Notes

Cyber Awareness

- **Digital Payment Systems** facilitate cashless transactions through methods like online banking, mobile wallets, and cryptocurrencies, ensuring convenience and security through encryption, tokenization, and fraud prevention mechanisms.
- **Cyber crimes** like hacking, phishing, malware, and identity theft exploit vulnerabilities in digital systems, posing threats to individuals, businesses, and governments globally.
- **Cyber law** governs the digital world, addressing issues like online fraud, intellectual property protection, data privacy, and international jurisdiction to ensure a safe and fair cyberspace.
- **Digital Literacy** involves mastering digital tools, critical thinking, cybersecurity awareness, and ethical digital behavior to effectively participate in the evolving digital landscape.
- **Digital Hygiene** involves adopting habits to ensure a secure and healthy digital presence, protecting personal information, and minimizing online threats.
- **Core cyber security Practices** aspects include password management, software updates, secure Wi-Fi practices, phishing awareness, and device security, among others.



TERMINAL QUESTIONS

1. What does cyber law aim to regulate in the digital era?
2. How does cyber law address the challenges posed by cybercrimes?
3. Why is cyber awareness important in today's digital society?
4. What are some common cyber threats that individuals should be aware of?
5. How does practicing digital hygiene contribute to online safety?
6. What are the key security measures used in digital payment systems to ensure safe transactions?
7. How does cyber law help in addressing challenges like online fraud and data privacy?
8. Why is digital literacy important in today's technology-driven world, and how does it contribute to safe online behavior?
9. Why is it important to regularly update digital hygiene habits, and how can this reduce cyber threats?



ANSWERS TO INTEXT QUESTIONS



Notes

11.1

1. (a) True (b) False (c) True (d) False
(e) False (f) False (g) False

11.2

1. (a) criminal (b) computer (c) national (d) cyber threats
(e) information (f) cyberspace (g) legal (h) technological

11.3

1. (a) secure password management
(b) Two-Factor Authentication (2FA)
(c) phishing
(d) operating systems
(e) privacy

Key Learning Outcomes

- explain the significance of cyber awareness in protecting individuals and organizations against evolving threats.
- describe the various types of digital payment systems and the security measures that protect online transactions.
- Differentiate between digital literacy and digital hygiene.



12

UNDERSTANDING CYBER LAW AND IT ACT, 2000

Crime refers to any unlawful act that is punishable by a state or authority. It covers a wide range of behaviors that violate societal norms or laws and can result in various consequences, such as fines, imprisonment, or other forms of punishment. Crimes can include offenses against persons (like murder or assault), property (such as theft or vandalism), morality (like drug offenses), or the state (such as treason or espionage).

Cybercrime specifically refers to criminal activities carried out using computers or the internet. This can include hacking, phishing scams, identity theft, spreading malware, cyberbullying, online harassment, and various forms of fraud committed electronically. With the increasing reliance on digital technology in our daily lives, cybercrime has become a significant concern for individuals, businesses, and governments worldwide.

In the vast landscape of the internet, where we shop, connect, and share, there exists a set of rules similar to a playbook for the digital game. Here, this playbook can be understood as Cyber Law, and one of its crucial chapters is the Information Technology Act, 2000 (IT Act) which is further

divided into 13 chapters and over 90 sections. Let's board on a journey into this digital rulebook to understand the vital aspects.



OBJECTIVES

After reading this lesson, the learner will be able to:

- list and explain various cyber security initiatives of India;
- explain important sections of IT Act, 2000 relevant to cybercrimes;
- describe Intermediary guidelines and DPDP Act.



12.1 CYBER LAW

Imagine you have a favorite game, and to play it well, you need rules. Cyber Law is precisely that – rules for the online world. It's the law that keeps things fair and secure when we're surfing the internet, chatting with friends, or buying cool stuff online.

12.1.1 Why Does the IT Act, 2000 Matter?

Think of it as the superhero in our digital world, fighting against the villains of cybercrimes. This law was created to make sure our online adventures are safe and sound. It's like a shield that protects us from the bad stuff that can happen on the internet. India enacted its Information and Technology Act in the year 2000.

12.1.2 Why Do We Need These Rules?

Picture the internet as a big city. In cities, we have rules to keep things in order – traffic lights, no littering, and so on. Similarly, Cyber Law and the IT Act are our digital city rules. They keep our online streets safe, ensure fair play, and make sure everyone can enjoy the digital city without worrying about bad things happening.

12.1.3 Inside the IT Act and UN's Model Law on E-commerce

Before we dive into the IT Act, let's go back a bit. In 1996, the United Nations Commission of International Trade Law (UNCITRAL) introduced the Model Law on e-commerce. This was like a guideline for countries to deal with the challenges of the growing tech-driven business sector. The United Nations recommended all its member states to adopt this model, giving recognition to electronic records and transactions. Then came India's answer – the Information Technology Act, 2000. **It became effective on 17th October 2000**, and it's the one and only law in India that deals with cyber regulations and e-commerce. The main goal was to create a legal framework for e-commerce activities, e-governance, electronic records, and signatures, and everything related to the digital world.

12.2 SALIENT FEATURES OF THE ACT

The Act is like a big book, divided into 13 chapters, 4 schedules, and 94 sections. Each chapter deals with a different concept. Here they are being mentioned for easy understanding, but for in depth knowledge it is advised to refer the IT Act 2000 from the official site of Ministry of Electronics and IT (MEITY) (<https://www.meity.gov.in/content/information-technology-act>)

- **IT Act, 2000 : Chapter 1: Preliminary - Definitions and Applicability:**
The first chapter defines various terms used in the Act. It applies to all of India,



Notes

Understanding Cyber Law and IT Act, 2000

except a few things like negotiable instruments, power of attorney, trusts, wills, and contracts for immovable property. It even applies to offenses committed by someone outside India.

The Act made changes to other laws like the Indian Penal Code, Indian Evidence Act, Bankers Book Evidence Act, and Reserve Bank of India Act.

- **IT Act, 2000 : Chapters 2 and 3: Authentication and Electronic Governance**

IT Act, 2000 : Chapter 2: Digital Signatures - Authentication of Electronic Records: It gives the green light to electronic records and digital signatures. It says that a person with a digital signature certificate can authenticate an electronic record. Fancy words like “asymmetric crypto system” and “hash function” are just ways of keeping things safe and secure.

IT Act, 2000 : Chapter 3: Electronic Governance - Legal Recognition of Electronic Records and Signatures in Government: It is all about electronic governance by giving legal recognition to electronic records and signatures in government activities. The government can make rules about how digital signatures should work.

- **IT Act, 2000 : Chapter 4: Attribution, Acknowledgment, and Dispatch of Electronic Records:** Specifies rules for attributing electronic records, acknowledging their receipt, and the dispatch of electronic records.
- **IT Act, 2000 : Chapter 5: Secure Electronic Records and Digital Signatures:** Focuses on ensuring the security of electronic records and digital signatures through prescribed methods and standards.
- **IT Act, 2000 : Chapter 6: Regulation of Certifying Authority:** This chapter introduces a “certifying authority.” The government appoints controllers to supervise these authorities. Certifying authorities issue digital signature certificates – like digital passports – with powers to issue, suspend, and revoke.
- **IT Act, 2000 : Chapter 7: Electronic Signature Certificates:** It outlines the requirements and procedures related to electronic signature certificates, ensuring their authenticity and reliability.
- **IT Act, 2000 : Chapter 8: Duties of Subscribers:** This talks about the responsibilities of subscribers. If you have a digital signature, you must take care of it like you take care of your secret codes. Don’t let it fall into the wrong hands.



- **IT Act, 2000 : Chapter 9: Penalties and Adjudication:** This is a crucial chapter as it mentions that Penalties are imposed if there's damage to computers or networks. An adjudicating officer, like a judge, looks into these matters. They can impose fines or compensate victims.
- **IT Act, 2000 : Chapter 10: Cyber Regulations Appellate Tribunal:** It introduces a Cyber Appellate Tribunal, a place where you can appeal if you're not happy with decisions from certifying authorities or adjudicating officers. It's like a higher court for cyber matters.
- **IT Act, 2000 : Chapter 11: Cyber Offenses:** It lists various cybercrimes like tampering with computer documents, sending offensive messages, identity theft, and more. The punishment depends on the severity of the crime.
- **IT Act, 2000 : Chapter 12: Liability of Network Service Providers:** Not to be Liable in Certain Cases.

It talks about the responsibilities of network service providers. They are exempt from liability if they follow the rules and act as intermediaries without conspiring or aiding in illegal activities.

- **IT Act, 2000 : Chapter 13: Miscellaneous, Power to Make Rules:** It Provides the government with the authority to make rules for carrying out the provisions of the Information Technology Act, 2000, ensuring adaptability to technological advancements.



INTEXT QUESTIONS 12.1

1. State True or False:

- (a) Cyber Law serves as a protective framework to ensure fairness and security in the online world.
- (b) The IT Act, 2000 was enacted by India in 1996 following the UN's Model Law on E-commerce.
- (c) Digital signatures and electronic records do not have legal recognition under the IT Act, 2000.
- (d) The IT Act, 2000 has provisions for penalties and adjudication for cybercrimes and related offenses.
- (e) The Cyber Appellate Tribunal under the IT Act hears appeals related to decisions by certifying authorities and adjudicating officers.
- (f) The IT Act, 2000 applies only within India and does not cover offenses committed by someone outside India.



Notes

12.3 SOME PROMINENT SECTIONS MENTIONED IN THE ACT

The IT Act has several sections, each dealing with a different aspect of the online world. Let's dive into the key parts:

- **Section 43 - No Sneaking Allowed:** This section is all about not sneaking into someone else's computer, data, or network without permission. It's like saying, "Hey, knocking before entering is the right thing to do!"

Why it Matters: Sneaking into someone's digital space can cause a lot of trouble, just like entering someone's house without permission.

- **Section 66 - Computer Troubles:** It deals with various computer-related problems. If someone steals information, messes with computers, or does other naughty things, this section steps in.

Why it Matters:

Imagine someone taking your online piggy bank or messing with your game scores – that's what this section protects us from.

- **Section 67 : Punishing for any Obscene transmission:** Section 67 of the Information Technology Act, 2000 deals with publishing or transmitting obscene material in electronic form. It prohibits the publishing, transmitting, or causing to be published or transmitted any material that is lascivious or appeals to the prurient interest or is likely to deprave or corrupt people.

One notable case involving Section 67 of the Information Technology Act, 2000 is the "Sharukh Khan Cyber Sex Scandal" that occurred in 2001. In this case, fake MMS clips allegedly showing Bollywood actor Shah Rukh Khan engaged in explicit acts were circulated online. The dissemination of these clips was considered a violation of Section 67, which prohibits the publishing or transmitting of obscene material in electronic form. Although the authenticity of the clips was disputed, the incident highlighted the legal implications of sharing explicit content online and the role of the IT Act in regulating such activities.

- **Section 69 - Keeping an Eye for a Good Reason:** This part gives the government the power to check on information, but only for good reasons like national security. It's like having superheroes watching over the city to keep everyone safe.

Why it Matters:

Balancing safety and privacy is tricky, but this section tries to make sure the good guys can protect us without invading our personal space too much.



- **Section 72 - Keeping Secrets Safe:**

It is all about keeping secrets safe. If someone spills the beans on your private stuff without permission, there are consequences.

Why it Matters:

Just like we trust our friends to keep our secrets, this section makes sure people online do the same.

- **Section 79 - Middle Folks and Their Jobs:**

It is like the boss telling the middle folks (internet service providers) what they can and can't do online. It's about making sure they play fair in the online playground.

Why it Matters:

Imagine a referee in a game making sure everyone follows the rules – that's what this section does for the internet.

In conclusion, the Information Technology Act, 2000, is like a guidebook for navigating the digital realm. However, with technology evolving rapidly, it's time to update this guidebook to meet the demands of our contemporary world. The last amendment was in 2008, and with the surge in cybercrimes, a redraft is essential. The IT Act, 2000 is a stepping stone, and it's high time for reimagining to ensure it keeps pace with the ever-changing technology landscape.

12.4 VARIOUS CYBER SECURITIES INITIATIVES OF INDIA:

India has taken several initiatives to enhance cybersecurity and address the evolving challenges in the digital landscape.

Some key cybersecurity initiatives in India include:

1. **National Cyber Security Policy (NCSP):** The NCSP was introduced in 2013 to provide a framework for securing cyberspace and creating a resilient information infrastructure. It focuses on enhancing the capabilities of law enforcement agencies, promoting research and development in cybersecurity, and fostering international cooperation.
2. **Indian Computer Emergency Response Team (CERT-In):** CERT-In is the national nodal agency responsible for responding to and mitigating cybersecurity incidents. It provides early warning, vulnerability management, and incident response to protect the country's digital assets.



Notes

3. **National Critical Information Infrastructure Protection Centre (NCIIPC):** NCIIPC is tasked with safeguarding critical information infrastructure from cyber threats. It identifies critical sectors, assesses vulnerabilities, and develops strategies to protect essential services like energy, transportation, and finance.
4. **Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre):** Launched by CERT-In, this initiative aims to detect and clean malware-infected systems in India. It provides tools and resources to help users secure their systems and promotes a cleaner and safer cyberspace.
5. **National Cyber Coordination Centre (NCCC):** The NCCC is designed to act as a central hub for monitoring and responding to cyber threats in real-time. It enables situational awareness and facilitates coordination among various stakeholders to enhance the overall cybersecurity posture.
6. **Cyber Crime Reporting Portal (Cybercrime.gov.in):** The Ministry of Home Affairs launched this portal to provide a platform for citizens to report cybercrimes. It helps law enforcement agencies in investigating and addressing cyber threats more effectively.
7. **Information Security Education and Awareness (ISEA) Project:** The ISEA project focuses on creating awareness about information security and promoting education and research in cybersecurity. It includes initiatives to train professionals, students, and law enforcement personnel.
8. **Cyber Surakshit Bharat Initiative:** Launched by the Ministry of Electronics and Information Technology, this initiative aims to spread awareness about cybersecurity among common users and enterprises. It provides information and tools to secure systems and data.
9. **National Cyber Security Awareness Campaign (NCSAC):** NCSAC is a collaborative effort involving government agencies, industry partners, and academia to promote cybersecurity awareness across various sectors. It conducts workshops, training programs, and awareness campaigns.
10. **Indian Cyber Crime Coordination Centre (I4C):** I4C is a comprehensive initiative to combat cybercrime effectively. It includes components like the National Cyber Crime Threat Analytics Unit and the National Cyber Crime Reporting Portal, working together to strengthen the response to cyber threats.

These initiatives collectively aim to build a secure and resilient cyberspace in India, emphasizing collaboration among government agencies, industry stakeholders,

and the public. The ongoing efforts reflect the recognition of cybersecurity as a critical component of national security and economic well-being.



INTEXT QUESTIONS 12.2

1. Fill in the Blanks with Answers:

- (a) of the IT Act deals with unauthorized access to a computer, data, or network without permission.
- (b) prohibits the publishing or transmitting of obscene material in electronic form.
- (c) **The National Cyber Security Policy (NCSP)** was introduced in the year to enhance cybersecurity infrastructure in India.
- (d) **CERT-In** stands for the Computer Emergency Response Team, which is responsible for managing cybersecurity incidents in India.
- (e) of the IT Act defines the responsibilities and limitations of internet service providers in ensuring fair play online.
- (f) is an initiative aimed at cleaning and protecting systems from malware infections.

12.5 IT RULES 2021 (SOCIAL MEDIA)

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were introduced in the month of February 2021 in India. These rules impact social media platforms, digital media, and online streaming services etc. This is divided into various Parts covered under VI main chapters and key points are as follows:

- Social media platforms with more than 5 million users in India are required to appoint a Chief Compliance Officer, a Nodal Contact Person, and a Resident Grievance Officer. These officers are responsible for addressing user complaints and ensuring compliance with the rules.
- Social media intermediaries are required to remove or disable access to unlawful content within 36 hours of receiving a court order or a government notification. They are also required to remove content that is flagged by appropriate government agencies.



Notes



Notes

Understanding Cyber Law and IT Act, 2000

- Social media platforms are required to enable the identification of the first originator of information if needed for investigating or preventing offenses related to the sovereignty and integrity of India, security of the state, and public order.
- Social media platforms with more than 5 million users are required to provide the capability to trace the origin of a message upon government request.
- Social media platforms are required to implement mechanisms to categorize content and ensure that users have the option to voluntarily verify their accounts.
- Social media platforms are required to obtain user consent before collecting sensitive personal data or information
- Social media platforms are required to submit periodic compliance reports to the government detailing the steps taken to comply with the rules

The Revised IT Rules Guidelines 2021 is like a rulebook for online content in India, with several chapters covering different areas. It talks about everything from how online games should be to keeping an eye on news and current affairs. There's a set of ethical guidelines for digital media, stressing the need to be clear and open about things. It makes sure that those who share content follow the rules and even lays out what happens if they don't. The guidelines also say that content should be classified based on its theme, violence, nudity, and other things. They want publishers to be careful about what they show, especially if it's about India's safety or could cause problems. The rules also highlight the importance of making content accessible to everyone, including people with disabilities. The main idea is to make sure online content is responsible, thinking about its impact on society, and making sure everyone follows the rules.

12.6 UNDERSTANDING INDIA'S DIGITAL PERSONAL DATA PROTECTION (DPDP) ACT, 2023: A GAME-

12.6.1 Changer in Data Privacy

The Digital Personal Data Protection Act, 2023, is a groundbreaking legal framework designed to be the guardian of personal data in the digital realm. This comprehensive legislation aims to fortify the protection of individuals' digital privacy while introducing regulations for entities handling personal data. Let's delve into the intricacies of this significant development:

The Act responds to the evolving challenges posed by the increasing digitization of personal information. Its primary objective is to establish a robust regulatory



mechanism preventing unauthorized access, use, and exploitation of personal data. At its core, the Act introduces the Digital Protection Authority, commonly known as the Board, entrusted with supervision and enforcing the stipulations outlined in the legislation.

Key Definitions: Decoding Data Dynamics (Who's Who in the Data World)

- **Data Principal:** That's you – the person whose data is being used. This refers to individuals whose personal data is subject to processing.
- **Data Fiduciary:** These are the companies or organizations using your data, such as govt. or private entities, engaged in the processing of personal data.
- **Consent Manager:** Think of them as facilitators managing user consent regarding the processing of personal data.

Rights of Individuals: Empowering Digital Citizens

The Act places considerable emphasis on empowering individuals with control over their personal data. It grants individuals the right to be informed about how their data is being used and mandates obtaining informed consent before processing. An innovative addition is the concept of a Consent Manager, introduced to streamline the process of managing user consent, enhancing transparency, and ensuring individuals are fully aware of how their data is being utilized.

Appointment and Powers of the Board: The Sentinel of Data Protection

The legislation entrusts the Digital Protection Authority (Board) with the responsibility of effective implementation. The Board, with prior approval from the Central Government, has the authority to appoint officers and employees necessary for the efficient discharge of its functions. Furthermore, the Chairperson, Members, officers, and employees of the Board are designated as public servants under the Indian Penal Code.

The Chairperson is vested with critical powers, including general superintendence over administrative matters, authorization of officers for scrutinizing complaints, and delegation of functions to individual Members or groups.

Powers, Functions, and Procedures of the Board: Upholding Digital Justice

The Board is empowered to address personal data breaches, conduct inquiries, and impose penalties. Urgent remedial measures can be directed in case of a breach, and inquiries can be initiated based on complaints, references, or court directions. The Board also possesses the authority to issue directions deemed necessary and may modify, suspend, or withdraw them based on representations. In implementing



Notes

Understanding Cyber Law and IT Act, 2000

a digital approach, the Board functions as a digital office, utilizing technological measures to expedite complaint processing. It can determine the sufficiency of grounds for an inquiry, and upon concluding an inquiry, issue orders based on the principles of natural justice. The Board's powers are similar to those vested in a civil court under the Code of Civil Procedure, 1908.

Appeal and Dispute Resolution: Ensuring Fair Play

The Act establishes an Appellate Tribunal to address appeals against Board decisions. The Tribunal's orders are executable as civil court decrees. It is expected to function digitally, promoting efficiency and expeditious resolution of appeals. The legislation also provides for alternate dispute resolution mechanisms, including mediation, to resolve disputes amicably.

Voluntary Undertaking: A Pledge for Responsible Data Handling

A noteworthy provision of the Act is the acceptance of voluntary undertakings from entities regarding compliance. This mechanism allows entities to commit to specific actions or refraining from certain activities under the supervision of the Board.

Penalties and Adjudication: Enforcing Compliance

Monetary penalties are a key enforcement tool under the Act. The Board, after an inquiry, may impose penalties based on the significance of the breach. Factors such as the nature, duration, and impact of the breach, as well as the actions taken to mitigate, are considered in determining the penalty amount. All penalties collected are credited to the Consolidated Fund of India.

Miscellaneous Provisions: Legal Safeguards and Public Interest

The Act provides legal protection for actions taken in good faith under its provisions, shielding the Central Government, the Board, and its members, officers, and employees from legal proceedings for actions performed in line with the legislation.

To ensure effective implementation, the Central Government can request information from the Board, Data Fiduciaries, or intermediaries. The Act also grants the government the authority to issue directions for blocking information in specific instances, emphasizing public interest.

Rules, Amendments, and Conclusion: Adapting to the Digital Future

The Central Government is empowered to make rules for the Act's effective implementation. These rules cover various aspects, including data breach notification, consent management, and the functioning of the Appellate Tribunal.



The rules must be laid before Parliament for scrutiny. The Act introduces amendments to existing legislation. Notably, the Telecom Regulatory Authority of India Act, 1997, sees changes to include the Appellate Tribunal under the Digital Personal Data Protection Act, 2023. Amendments are also made to the Information Technology Act, 2000, removing section 43A and adjusting other relevant sections. The Right to Information Act, 2005, undergoes a change, replacing clause (j) of sub-section (1) of section 8 with a clause relating to personal information.

Therefore, the Digital Personal Data Protection Act, 2023, represents a significant step towards enhancing digital privacy, empowering individuals with control over their data, and establishing a robust regulatory framework for the responsible handling of personal information. The Act introduces innovative concepts, such as the Consent Manager, and leverages technology to streamline processes, ensuring the legislation remains relevant in the rapidly evolving digital landscape. It serves as a digital safeguard, paving the way for a more secure and accountable digital future in India.



INTEXT QUESTIONS 12.3

1. Fill in the Blanks with Answers:

- (a) The were introduced in the month of February, 2021 to regulate social media platforms, digital media, and online streaming services.
- (b) The establishes the Digital Protection Authority as the regulatory authority for data protection.
- (c) The under the DPDP Act is empowered to address appeals against Board decisions.
- (d) Penalties imposed under the DPDP Act are credited to the Fund of India.
- (e) The DPDP Act amends the replacing clause (j) of sub-section (1) of section 8 with a clause related to personal information.

12.6.2 Some of the case studies are given below

1. Sim swap fraud of 80 Lakh by a 24yr old

Investigators said Mukherjee, a BCA Degree holder and his associates were in cahoots with a gang of cybercriminals based in Nigeria. The gang from Nigeria had bugged the victim's system and got banking details. Mukherjee and his aides, who



Notes

were dealing with employees of telecom service providers, then got his number and swapped the sim. A police officer said, “Cybercriminals get the personal details of a target through phishing, vishing or smishing. They use this information to trick telecom companies into issuing duplicate sim cards. Once the duplicate sim begins to function, the original gets blocked. The cybercriminals then used the duplicate sim to gain access to the victim’s bank accounts and get one-time passwords (OTP) to carry out transactions.

Source: <https://timesofindia.indiatimes.com/>

2. Cyber fraud via AI-enabled voice change

India’s internet-using population, which surpassed 720 million in December 2022, according to Nielsen’s India Internet Report 2023, may be vulnerable to a new type of voice-based cyber scam, wherein scammers are employing artificial intelligence to replicate user voices and exploit them in cyberattacks on unsuspecting individuals, according to a report. Cybersecurity firm McAfee revealed in a 1 May report that 47% of Indian users have either encountered or know someone who fell victim to AI voice cloning scams in January-March.

The surge in the AI voice-cloning scams corresponds with growing interest in generative AI, where algorithms process user inputs in text, image, or voice formats, and produce results based on user queries and the specific platform. On 9 January, for instance, Microsoft introduced Vall-E, a generative AI-based voice simulator capable of replicating a user’s voice and generating responses with the user’s unique tonality by using just a three-second audio sample.

Fraudsters duped people by making them believe that they are one of their close friends or relatives while speaking to them over phone in their AI-modulated voice. The fraudsters while speaking to them cited an emergency situation while asking them to transfer money.

Uttarakhand state cyber police are working on a strategy to tackle such cases which it says are going to increase in the coming days. To protect against these scams it is important to verify the identity of callers using a safe word, avoid publicly sharing personal videos, images, be cautious of suspicious AI bots and report any cybercrime to the authorities.

Source: <https://timesofindia.indiatimes.com/city/dehradun>

3. The city cyber-crime sleuths arrested six accused involved in fingerprint cloning

A city cyber-crime sleuths arrested six accused involved in fingerprint cloning using rubber fingerprints and Seemandhar machine to illegally withdraw Rs 10



lakh from bank account holders. One K. Srinu got enrolled as a business correspondent for providing banking services using POS (Point of Sale) and Bank's Merchant portal and was allotted a Terminal ID. He misused

Terminal ID, Aadhaar Enabled Payment System (AEPS). As per their plan, they ordered an Image Pack Stamp Machine through the flipkart app and also managed to procure a "Seemandhar" heat machine, polymer liquid gel, transparent A4 papers and AB powder.

In July, the arrested accused Ch. Narendra, who is a childhood friend of another accused Uday, supplied up to 2,500 land registration document files in soft copies including fingerprints through pen drive to Asadharan and Illyas. They managed to convert a total of 1,000 fingerprints into cloned fingerprints. Later, the accused opened various bank accounts and merchant IDs and carried 2,500 AEPS (Aadhaar Enabled Payment System) transactions through different merchant ID's and shared the withdrawn amount among themselves.

Source: <https://www.pressreader.com/india/deccan-chronicle>



Fig. 12.1

Source: https://legalserviceindia.com/legal/uploads/cyberfraudsintheindianbankingindustry_2063793_616.jpg

4. New Digital Arrest cyber fraud is causing widespread terror in India

A new form of cybercrime known as "digital arrest" scams is emerging, where fraudsters deceive individuals into believing they are facing imminent digital arrest for fabricated legal violations. The perpetrators, through digital communication methods like video messages or calls, create a sense of urgency and fear, manipulating victims with false evidence, threatening language, and demands for significant payments to avoid supposed legal consequences. In the mentioned



Notes

case, the victim was coerced into believing she was involved in a passport trafficking case and may have to pay Rs 15 lakh to avoid a “digital arrest.” She finally settled the issue for Rs 2.5 Lakhs.

Source: <https://www.firstpost.com/tech>



WHAT YOU HAVE LEARNT

- The IT Act, 2000 ensures a secure and regulated digital environment by addressing cybercrimes and providing a legal framework for electronic governance, e-commerce, and digital transactions. The Act is organized into 13 chapters, 4 schedules, and 94 sections, covering areas like authentication, electronic governance, penalties, and cybersecurity offenses.
- Digital signatures, validated by certifying authorities, are legally recognized for ensuring secure authentication of electronic records.
- The IT Act applies to offenses both within India and those committed by individuals outside India if they impact systems or individuals in India.
- **The Key Sections of the IT Act, 2000 are :**
 - Section 43: Protects against unauthorized access to computers or networks.
 - Section 66: Deals with computer-related offenses such as theft of information.
 - Section 67: Penalizes publishing/transmitting obscene material.
 - Section 69: Grants government authority for surveillance under specific conditions.
 - Section 79: Regulates the liability of internet service providers.
- **The major Cybersecurity Initiatives in India include:**
 - **NCSP (2013):** Strengthens national cybersecurity infrastructure.
 - **CERT-In:** National agency for handling cybersecurity incidents.
 - **Cyber Swachhta Kendra:** Focuses on detecting and cleaning malware.
 - **NCIIPC:** Protects critical information infrastructure.
 - **I4C:** Centralized framework for combating cybercrimes effectively.



- **Government Efforts** like Awareness programs such as **Cyber Surakshit Bharat** and **ISEA Project** aim to educate users. Collaborative platforms like **NCSAC** and **Cyber Crime Reporting Portal** encourage public participation in reporting and tackling cyber threats.
- The IT Rules 2021 regulate social media and digital platforms, requiring compliance officers, quick removal of unlawful content, and message origin tracing for platforms with over 5 million users.
- The DPDP Act 2023 empowers individuals with data privacy rights, mandates informed consent, and establishes the Digital Protection Authority for overseeing compliance and addressing breaches.



TERMINAL QUESTIONS

1. Briefly explain the key provisions of the IT Act 2000.
2. What are some of the major guidelines for social media platforms outlined in the Social Media Guidelines 2021?
3. Discuss the significance of the Data Privacy and Protection (DPDP) act in safeguarding individuals' digital privacy in India.
4. How has the IT Act 2000 evolved over the years to address emerging challenges in the digital space?
5. A popular social media platform with over 10 million users in India receives a government order to remove a post spreading misinformation about national security. What steps should the platform take to comply with the IT Rules 2021? What could be the consequences if it fails to act within the stipulated time frame?
6. An individual discovers that a digital app has shared their personal data with third-party advertisers without consent. What steps can the individual take under the DPDP Act, 2023, to address this breach? Which authority would oversee this complaint, and what penalties could the app face?



ANSWERS TO INTEXT QUESTIONS

12.1

1. (a) True (b) False (c) False (d) True (e) True (f) False



Notes

12.2

1. (a) Section 43 (b) Section 67 (c) 2013
(d) Indian (e) Section 79 (f) Cyber Swachhta Kendra

12.3

1. (a) IT Rules 2021
(b) Digital Personal Data Protection (DPDP) Act, 2023
(c) Appellate Tribunal
(d) Consolidated
(e) Right to Information Act, 2005

Key Learning Outcomes

- explain the significance of the IT Act, 2000 in safeguarding digital transactions and combating cybercrimes.
- describe the various provisions, such as digital signatures, electronic governance, penalties, and the regulation of certifying authorities.
- explain the primary sections of the IT Act, 2000, and their role in governing digital behavior and safeguarding online users.
- Identify reporting mechanisms like the **Cyber Crime Reporting Portal** for addressing cyber threats effectively.