📘 Lecture 6 — Operating System, Drivers, Virtualization & Malware

---

1️⃣ What is an Operating System (OS)

Definition

An **Operating System (OS)** is a **system software** that acts as an intermediary between the **user and the computer hardware**.
It manages **resources** (CPU, memory, storage, devices, and network) and provides a platform for applications to run.

Why it is used

Without an OS, users would have to interact with hardware directly in binary code.
The OS simplifies usage and ensures efficient resource utilization, multitasking, and security.

2️⃣ Types of Operating Systems

OS Type	Description	Interface
Windows	Most common OS by Microsoft. Provides **GUI (Graphical User Interface)**.	GUI
Linux	Open-source, powerful, widely used in servers and hacking tools (Kali, Ubuntu).	Command Line Interface (CLI) & GUI
Mac OS	Apple's Unix-based OS for Mac computers. Known for security & design.	GUI
iOS	Apple's mobile OS for iPhones/iPads. Based on Unix principles.	GUI
Android	Google's mobile OS based on Linux kernel. Open source.	GUI

OS Type	Description	Interface
Ubuntu / CentOS	Linux distributions. Ubuntu for users; CentOS for servers.	CLI & GUI

OS updates & compliance

- OS updates daily/weekly to fix **bugs**, **security vulnerabilities**, and **performance issues**.
- **Compliance** means following organization or government **security policies & rules** (like patching schedules, encryption standards, antivirus enablement).

3️⃣ System Software vs Application Software

Type	Purpose
System Software	Runs hardware and supports other software (OS, drivers, utilities).
Application Software	Programs that perform user tasks (browsers, games, MS Word).

The OS is a **system software** because it controls all other processes.

4️⃣ Resource Management

What it is

Resource management means allocating and controlling **hardware resources** like:

- **CPU** — controls processing tasks.
- **Memory (RAM)** — manages temporary storage of active processes.
- **Storage (Hard disk/SSD)** — for permanent data storage.
- **Network** — manages connections and data transmission.
- **GPU** — handles graphics rendering.

Why it matters

Efficient resource management prevents system overload, ensures fairness, and optimizes performance.

5️⃣ Process & Memory Management

Process Management

- A **process** is a running instance of a program.
- The OS:
  - Starts/stops processes.
  - Allocates CPU time.
  - Manages process communication and scheduling.

Memory Management

- Controls how memory is allocated to processes.
- **Volatile Memory (RAM):** temporary, data lost after shutdown.
- **Non-Volatile Memory (Hard Disk):** permanent data storage.
- Prevents memory leaks, ensures secure isolation of processes.

6️⃣ Security Management

Functions

- **Access control:** defines who can access what (user permissions).
- **Encryption:** protects data at rest or in motion.
- **Authentication:** verifies user identity (passwords, biometrics).
- **System Protection:** uses features like firewall, antivirus, and secure boot.

7️⃣ Job Accounting

Definition

Job accounting tracks how much **CPU time, memory, and storage** each process or user consumes.
Used in enterprise systems to **analyze performance, cost allocation, or detect misuse**.

8️⃣ File Management System

What it does

- Manages how data is **stored, retrieved, organized, and deleted** on storage drives.
- Provides functions like creating, reading, writing, renaming, moving, and deleting files.

Example (Recycle Bin behavior)

- If a file from **D drive** is deleted, it first goes to **Recycle Bin**.
- Recycle Bin is a **system app installed on C drive**, so deleted files from all drives are stored there.
- When you restore, the file returns to its **original location (e.g., D drive)** — this tracking is done via **indexing**.

Hidden system files

- To see deleted or hidden files:
    1. Open any drive.
    2. Go to **View → Options → View tab**.
    3. Enable **"Show hidden files, folders, and drives"**.
    4. Uncheck **"Hide protected operating system files."**
- This helps recover or view system-protected files, including Recycle Bin data from USB or system drives.

9️⃣ Device Manager & Driver Check

What is a Driver?

A **driver** is a small piece of software that allows the OS to communicate with hardware devices (keyboard, GPU, network card, printer, etc.).

How to check/update drivers

1. Press **Windows + R**, type devmgmt.msc, and press Enter.
2. Open **Device Manager**.
3. Expand the category (e.g., “Network Adapters”).
4. Right-click any driver → **Properties → Driver tab** to view details and date.
5. Update regularly via Windows Update or vendor site.

Why update drivers?

- Fixes security vulnerabilities.
- Improves hardware performance and compatibility.

🔟 Networking (Basic Concept)

When two or more devices communicate or exchange data, it is called **networking**.
The OS manages networking through:

- **Protocols (TCP/IP)**
- **Network adapters & drivers**
- **Network services (DHCP, DNS, ARP)**

1️⃣1️⃣ Command Line Interface (CLI) vs Graphical User Interface (GUI)

Interface	Description	Example
CLI	Text-based interface. Faster for admins.	Linux terminal, PowerShell, Command Prompt
GUI	Visual interface with windows, icons, menus.	Windows desktop, macOS Finder

Ethical hackers often prefer CLI for automation, scripting, and deeper control.

1️⃣2️⃣ Backup & Recovery – System Protection

What it is

System Protection creates restore points — snapshots of system files, settings, and registry.

How to enable

1. Press **Windows + R** → type sysdm.cpl → Enter.
2. Go to **System Protection tab**.
3. Click **Configure → Turn on system protection**.
4. Set disk space for restore points.

Why

If the system crashes or malware damages settings, you can **restore** to a previous state easily.

1️⃣3️⃣ Virtualization

What it is

Virtualization means creating virtual versions of hardware (like virtual machines, servers, or networks).

How to check if enabled

1. Open **Task Manager → Performance tab → CPU**.
2. Check if "**Virtualization: Enabled**" is shown.

Why it's used

- Allows running multiple OSes on one physical machine (useful for ethical hacking labs).
- Isolates risky testing environments (malware, penetration testing tools).
- Optimizes server resource utilization.

1️⃣4️⃣ Malware (Malicious Software)

Definition

Malware is any software intentionally designed to damage, steal, or exploit computers, networks, or users.

Common Types of Malware

Type	Description	Function
Virus	Attaches to legitimate files and spreads when opened.	Corrupts data or spreads infection.
Worm	Self-replicates and spreads via network.	Consumes bandwidth, hard to remove.
Trojan Horse	Disguised as legitimate software.	Provides attacker backdoor access.
Ransomware	Encrypts user data and demands ransom.	Extorts money.
Adware	Displays unwanted ads and pop-ups.	Generates revenue, tracks browsing.
Spyware	Secretly monitors user activity.	Steals credentials and data.

Type	Description	Function
Logic Bomb	Malicious code triggered by event/date.	Damages data.
Rootkit	Hides presence of malware or attacker.	Provides admin-level access.
Backdoor	Bypasses authentication to allow remote access.	Exploited by attackers.
Keylogger	Records keystrokes.	Steals passwords and typed data.
Botnet	Network of infected devices controlled remotely.	Used for DDoS, spam, mining.

1️⃣5️⃣ Why Cybercriminals Use Malware

- **Financial gain** (ransomware, banking trojans).
- **Data theft** (spyware, keyloggers).
- **System control** (botnets, backdoors).
- **Espionage or sabotage** (APT attacks).
- **Spreading political or social messages** (hacktivism).

1️⃣6️⃣ How to Protect From Malware

- Keep **OS and software updated** (patch vulnerabilities).
- Use **firewall + antivirus + anti-malware tools**.
- Avoid **cracked software** and unknown email attachments.
- Enable **System Protection & regular backups**.
- Use **VPN and secure browsers**.
- Disable autorun for USBs.
- Monitor processes via Task Manager.

1️⃣7️⃣ Tools Used to Remove Malware

Tool	Function
Windows Defender / Security	Built-in protection, detects and quarantines threats.
Malwarebytes	Advanced malware and ransomware scanner.
Kaspersky, Bitdefender, Norton	Paid antivirus solutions.
HitmanPro, ESET, Avast	On-demand malware scanners.
RogueKiller, AdwCleaner	Removes adware and unwanted programs.
Process Explorer / Autoruns	Finds and removes hidden malicious startup entries.

🔚 Summary — Key Points

- OS = heart of the computer; manages hardware, software, and user interaction.
- Resource management ensures CPU, memory, and storage work efficiently.
- File management organizes and tracks all data and deletions.
- Drivers allow OS ↔ hardware communication; update regularly.
- Virtualization helps build isolated hacking labs safely.
- Malware = enemy; understand its types and removal tools.
- Always keep system protection on and avoid untrusted sources.

✅ SUMMARY

This chapter introduces the fundamental concepts of Operating Systems, how they manage hardware resources, process execution, memory, files, security, and drivers. It also covers virtualization, malware types, infection methods, and system protection techniques.

An Operating System works as the middle layer between the user and the hardware, enabling multitasking, resource allocation, file management, and network communication. Different OS types (Windows, Linux, Mac, Android, iOS) are compared based on interface and common usage.

The chapter explains system software vs application software, process scheduling, RAM vs storage, file management (including Recycle Bin and hidden system files), driver management, networking basics, CLI vs GUI interfaces, and backup/recovery.

Virtualization is introduced as a method to run multiple OSes safely for testing or hacking labs. The chapter ends with an in-depth look at malware types (virus, worm, Trojan, ransomware, spyware, rootkits, botnets, keyloggers, etc.), why attackers use malware, and how to defend systems using tools like antivirus, firewalls, and monitoring.

✅ CONCLUSION

This chapter builds a solid foundation in system operation and cybersecurity. Understanding how an OS manages hardware, processes, memory, files, and security enables you to recognize system vulnerabilities. Knowledge of drivers, updates, virtualization, and malware behavior helps a cybersecurity professional analyze threats, build safe testing environments, and secure systems effectively. Mastery of these topics is essential for ethical hacking, system administration, and defensive security roles.

✅ DETAILED TEXT-BASED MINDMAP

LECTURE 6 – OS, Drivers, Virtualization & Malware

1. Operating System (OS)
   ├── Definition: bridge between user & hardware
   ├── Functions: resource mgmt, security, networking
   └── Types: Windows, Linux, macOS, iOS, Android

2. OS Types & Interfaces
   ├── Windows – GUI
   ├── Linux – CLI + GUI
   ├── macOS – GUI (Unix)
   ├── iOS – GUI
   ├── Android – GUI (Linux kernel)
   ├── Ubuntu/CentOS – Linux distros
   └── Updates for security & compliance

3. System vs Application Software
   ├── System: OS, drivers, utilities
   └── Application: browsers, games, MS Office

4. Resource Management
   ├── CPU scheduling
   ├── RAM allocation
   ├── Storage organization

├— GPU usage

└— Network management

5. Process & Memory Management

├— Process creation/scheduling

├— Inter-process communication

├— RAM (volatile)

└— Storage (non-volatile)

6. Security Management

├— Access control

├— Authentication

├— Encryption

└— System protection (firewall/AV)

7. Job Accounting

├— Track CPU, memory, storage per user/process

8. File Management

├— Create, read, write, delete

├— Recycle Bin behavior

├— Hidden/protected files

└— File indexing

9. Drivers & Device Manager

├— Driver = OS ↔ hardware communication

- ├— Check/update drivers
- └— Fix vulnerabilities & performance

10. Networking Basics
    - ├— TCP/IP
    - ├— DHCP, DNS, ARP
    - └— Network adapter drivers

11. CLI vs GUI
    - ├— CLI = faster, scripting
    - └— GUI = visual ease

12. Backup & Recovery
    - ├— Restore points
    - ├— System protection
    - └— Disaster recovery

13. Virtualization
    - ├— Multiple OS on one machine
    - ├— Isolated environments
    - └— Ethical hacking labs

14. Malware
    - ├— Virus, worm, Trojan, ransomware
    - ├— Adware, spyware, botnets
    - ├— Rootkits, backdoors, keyloggers

└── Logic bombs

15. Cybercriminal Motives

├── Money

├── Data theft

├── Control

├── Espionage

└── Hacktivism

16. Protection From Malware

├── Updates, AV, firewall

├── Avoid cracked software

├── Backups

├── VPN & secure browser

└── Monitoring tools

17. Malware Removal Tools

├── Windows Defender

├── Malwarebytes

├── Kaspersky/Norton/Bitdefender

├── Autoruns, Process Explorer

└── AdwCleaner

✅ INTERVIEW QUESTIONS + SIMPLE CLEAR ANSWERS

🔹 OPERATING SYSTEM – Q&A

1. What is an Operating System?

An OS is system software that manages hardware and provides a platform for applications to run.

2. Why do we need an OS?

Without an OS, users would need to communicate with hardware using binary code. OS makes usage simple and efficient.

3. What are the types of OS you know?

Windows, Linux, macOS, Android, iOS, Ubuntu, CentOS.

4. What is the difference between Windows and Linux?

Windows → GUI-based, commercial.
Linux → Open-source, CLI-heavy, preferred for servers and hacking.

🔹 SYSTEM vs APPLICATION SOFTWARE – Q&A

5. What is system software?

Software that operates hardware and supports other programs (OS, drivers).

6. What is application software?

Software used by end-users to perform tasks (browser, games, MS Word).

🔹 RESOURCE MANAGEMENT – Q&A

7. How does the OS manage resources?

It allocates CPU time, manages memory (RAM), schedules processes, handles network activity, and manages storage I/O.

8. Why is resource management important?

It prevents system overload and ensures fair and efficient performance.

🔹 PROCESS & MEMORY – Q&A

9. What is a process?

A running program instance.

10. Difference between RAM and Storage?

RAM → temporary, volatile.
Storage → permanent.

11. What is memory management in OS?

Deciding which process gets how much RAM, preventing memory leaks, and keeping processes isolated.

🔹 SECURITY MANAGEMENT – Q&A

12. What security features does an OS provide?

Authentication, access control, encryption, firewalls, antivirus integration.

13. What is access control?

Rules defining who can access which files or resources.

🔹 FILE MANAGEMENT – Q&A

14. What is the role of a file management system?

Organizing, storing, retrieving, and deleting files.

15. Why do deleted files go to Recycle Bin?

Because Windows tracks deleted file paths and temporarily stores them for recovery.

16. How do you view hidden system files?

File Explorer → View Options → Enable "Show hidden files" and disable "Hide protected system files."

🔹 DRIVERS & DEVICE MANAGER – Q&A

17. What is a device driver?

Software that allows hardware to communicate with the OS.

18. Why update drivers?

To fix vulnerabilities and improve hardware performance.

19. How do you open Device Manager?

Press Win + R → type *devmgmt.msc* → Enter.

🔹 NETWORKING BASICS – Q&A

20. What is networking?

Communication between two or more devices.

21. Which protocols are handled by OS?

TCP/IP, DNS, DHCP, ARP.

🔹 CLI vs GUI – Q&A

22. What is the difference between CLI and GUI?

CLI → text-based, faster for admins.
GUI → visual interface, easier for beginners.

23. Why do hackers prefer CLI?

For automation, scripting, and deeper system control.

🔹 BACKUP & SYSTEM PROTECTION – Q&A

24. What is System Protection?

A feature that creates restore points to recover system settings.

25. Why are restore points important?

They allow the system to revert after malware or configuration errors.

🔹 **VIRTUALIZATION – Q&A**

26. What is virtualization?

Running multiple virtual OS environments on one physical machine.

27. Why do ethical hackers use virtualization?

To test malware safely and run multiple OSes like Kali Linux.

28. How do you check if virtualization is enabled?

Task Manager → Performance → CPU → Look for "Virtualization: Enabled."

🔹 **MALWARE – Q&A**

29. What is malware?

Malicious software made to damage systems or steal data.

30. Types of malware?

Virus, worm, Trojan, ransomware, spyware, adware, rootkit, botnet, backdoor, keylogger, logic bomb.

31. What is ransomware?

Malware that encrypts files and demands payment.

32. What is a Trojan Horse?

Malware disguised as legitimate software.

33. What is a worm?

Self-replicating malware that spreads through networks.

34. What is a rootkit?

Malware that hides other malware and gives admin-level access.

35. What is a botnet?

A network of infected devices controlled by attackers.

🔹 CYBERCRIMINAL MOTIVES – Q&A

36. Why do attackers use malware?

For money, data theft, system control, espionage, or hacktivism.

🔹 MALWARE PROTECTION – Q&A

37. How to protect a system from malware?

Keep OS updated, use antivirus, enable firewall, avoid cracked software, backup regularly, monitor processes.

🔹 MALWARE REMOVAL TOOLS – Q&A

38. What tools remove malware?

Windows Defender, Malwarebytes, Kaspersky, Bitdefender, Autoruns, AdwCleaner, Process Explorer.

39. Why is Malwarebytes popular?

Strong detection of ransomware and advanced threats.

40. What are Autoruns and Process Explorer used for?

Finding hidden malware running at startup or in memory.