🧠 Lecture 15 — Cyber Security & Ethical Hacking (Defensive and Offensive Security)

🛡️ 1. Cyber Security (Defensive Security)

🔹 Definition:

Cyber Security is the practice of **protecting systems, networks, and data** from unauthorized access, attacks, or damage.
It focuses on **defense** — preventing attacks before they happen.

🔹 Understanding Data vs Information:

Term	Meaning	Example
Data	Raw facts or unprocessed input.	100, John, 01/01/2025
Information	Processed, organized, or meaningful data (output).	"John scored 100 marks on 01/01/2025."

👉 In simple words:

When we input **data** and process it through a system, the **output we get is information.**

🔹 What Cyber Security Protects:

1. **People** – Users and employees through awareness & training.
2. **Network Components** – Routers, Switches, Firewalls, VPNs.
3. **Servers** – Web, database, mail, and file servers.
4. **Devices** – Host and end-user devices (computers, mobiles).
5. **IoT Devices** – Internet-connected devices like smart bulbs, fans, and TVs.
6. **CCTV Systems** – Surveillance devices connected via a network.

💻 2. Host Device vs End Device

Type	Definition	Examples
Host Device	A system that provides services or resources to other devices on a network.	Server, Router, Firewall, Web server
End Device	The device that uses or consumes network services.	Laptop, Mobile phone, Printer, IoT Device

💡 *Think of it like this:*
A **host** serves data → an **end device** receives data.

🌐 3. IoT (Internet of Things) Devices

IoT devices are physical objects connected to the internet that send or receive data.
They can be remotely monitored or controlled.

Examples:

- Smart Lights
- Smart Fans
- Smart Cameras
- Smart Door Locks
- Smart Watches

Security Concern:
IoT devices are often **vulnerable** because they use **default passwords** and open ports.

🎥 4. CCTV Security Best Practices

- Never keep CCTV connected to **open ports**.
  → Hackers can access the feed remotely.
- Always **change the default username and password**.
- Use **strong network encryption**.

- Use **firewall/VPN** for accessing CCTV remotely.
- Understand the difference between **NVR** and **DVR**.

System	Full Form	Usage
NVR	Network Video Recorder	Used for **IP (network) cameras** — stores video from cameras connected over LAN/Wi-Fi.
DVR	Digital Video Recorder	Used for **wired analog cameras** — directly connected using cables.

💡 **NVR** is part of network security (uses network connection).
DVR is offline and less vulnerable.

🧍 5. Securing People (Human Aspect of Cybersecurity)

Even if a network is secured, **humans** can still be tricked — that's why organizations need **Security Awareness**.

🔹 **Security Awareness Training:**

- Conducted **every 6 months** in most companies.
- Helps employees identify **phishing**, **social engineering**, and **malware traps**.
- Employees learn about **data handling**, **password policies**, and **incident reporting**.

🔹 **Types of Security Policies:**

Policy Type	Purpose
Employee Policy	Defines acceptable behavior for employees — like password rules, device usage, and access permissions.
Technical Policy	Sets technical controls like firewalls, encryption, VPN rules, and antivirus deployment.

🔹 **ISO Certification and Security:**

- For a company to get **ISO 27001 (Information Security Standard)**, its **physical security** must meet requirements.
- Example: If a company's outer boundary wall is **less than 9 feet high**, it **cannot** receive ISO certification.
- ISO ensures **physical + digital security** standards are maintained.

📜 **Case Example: Domain Hijacking (Disney–Jio Hotstar Case)**

When **Disney Hotstar** rebranded to **Jio Hotstar**, a person had already purchased the domain **jiohotstar.com**.
He demanded **₹21 crore** to transfer ownership.

This is an example of **Cybersquatting** — registering domains similar to famous brands to **demand money** or misuse them.

🧍 **Security Awareness for People**

To protect users and organizations:

- Conduct **regular training**.
- Promote **password hygiene** (no reuse, use strong passwords).
- Teach to **verify URLs** before clicking links.
- Enable **2-factor authentication (2FA)**.
- Report suspicious emails or activities.

⚔️ **6. Ethical Hacking (Offensive Security)**

🔹 **What is Ethical Hacking?**

Ethical hacking is the legal practice of **testing systems, applications, or networks** to find vulnerabilities before malicious hackers do.

Ethical hackers work **with permission** and follow **rules (ethics)**.

🔹 **Purpose:**

- Identify and fix vulnerabilities.
- Test system defenses.
- Strengthen network and data security.
- Help organizations prevent cyberattacks.

🔹 **Process of Ethical Hacking:**

1. **Reconnaissance (Information Gathering)**
   → Collect data about target systems.
2. **Scanning and Enumeration**
   → Identify open ports, IPs, and services.
3. **Gaining Access**
   → Exploit vulnerabilities to enter the system.
4. **Maintaining Access**
   → Create backdoors to test persistence.
5. **Clearing Tracks**
   → Remove traces of testing activity.
6. **Reporting**
   → Document findings and give recommendations.

👩‍💻 **Types of Hackers**

Type	Description	Legality
White Hat Hackers	Work officially for organizations to improve security. Use ethical methods and proper authorization.	✅ Legal
Black Hat Hackers	Hack systems illegally for personal gain or damage.	❌ Illegal

Type	Description	Legality
Grey Hat Hackers	Hack without permission but usually report vulnerabilities publicly or to the company.	⚠️ Semi-legal (depends on intent)

💣 7. Types of Cyber Attacks

🦠 1. Malware Attack

🔹 Definition:

Malware (Malicious Software) is any software designed to **harm, exploit, or steal information** from systems.

Examples:

- Viruses
- Worms
- Trojans
- Ransomware
- Spyware
- Keyloggers

How it spreads:

- Through malicious email attachments
- Infected USB drives
- Pirated or cracked software
- Fake software updates

Purpose:
To damage, steal, or control system data.

🌐 2. DDoS (Distributed Denial of Service) Attack

🔹 Definition:

A **DDoS attack** floods a server or network with massive amounts of fake traffic, making it **unavailable to real users**.

- **DoS (Denial of Service):** Attack from **one** system.
- **DDoS (Distributed Denial of Service):** Attack from **multiple** systems (botnets).

Example:
Thousands of computers (bots) send requests to a single website until it crashes.

Common targets:
E-commerce sites, banks, gaming servers, etc.

Example Website for reference:
tomsguide.com — useful for DDoS prevention research.

Important:

- Malware and DDoS are **different concepts**.
- **Malware infects systems**, while **DDoS overloads networks.**

📧 3. Phishing Attack

🔹 Definition:

A **social engineering attack** that tricks users into revealing personal information (like passwords or credit card details) through **fake emails or websites**.

Example:
An email claims:

“Your Instagram password has been compromised. Click here to reset it.”

When you click and enter your credentials, attackers steal your data.

Prevention:

- Verify sender email addresses.

- Avoid clicking unknown links.
- Use spam filters.
- Enable 2FA on all accounts.

🧩 Summary Table

Concept	Description
Cyber Security	Defensive approach to protect systems, people, and data.
Ethical Hacking	Offensive testing to find and fix vulnerabilities.
Host Device	Provides network services.
End Device	Uses network services.
IoT Devices	Smart internet-connected devices.
NVR/DVR	CCTV recording systems (Network vs Digital).
Awareness Training	Conducted to secure human element in security.
White Hat Hacker	Authorized ethical hacker.
Black Hat Hacker	Unauthorized, malicious hacker.
Grey Hat Hacker	Semi-authorized, awareness-based hacker.
Malware	Harmful software that infects systems.
DDoS	Attack that floods server with traffic.
Phishing	Fake emails to steal user data.

✅ 📘 SUMMARY — Lecture 15 (Cyber Security & Ethical Hacking)

1. Cyber Security (Defensive Security)

Cyber Security focuses on **protecting systems, networks, devices, and data** from unauthorized access or cyberattacks.
It includes protection of:

- Users (humans)
- Network devices (routers, firewalls)
- Servers
- End devices (phones, laptops)
- IoT devices
- CCTV security

Cyber security works by implementing:

- Security policies
- Awareness training
- Network protections (firewalls / encryption)

---

2. Data vs Information

- **Data:** Raw facts (100, John)
- **Information:** Processed data in meaningful form ("John scored 100 marks")

---

3. Host Device vs End Device

- **Host Device:** Provides services (Servers, Routers, Firewalls)
- **End Device:** Uses services (Laptop, Mobile, IoT Devices)

---

4. IoT Security

IoT devices are internet-connected devices like smart bulbs, fans, locks.
They are high-risk because:

- They use **default passwords**
- Have **open ports**
- Lack **strong security**

---

5. CCTV Security (NVR vs DVR)

System	Meaning	Use
NVR	Network Video Recorder	IP Cameras → Connected via LAN/WiFi
DVR	Digital Video Recorder	Analog Cameras → Wired

NVR = Online (needs strong security)
DVR = Offline (less risky)

---

6. Security Awareness

Humans are the weakest link.
Companies give **training every 6 months** to avoid phishing, scams, password mistakes.

Two policies:

- Employee Policy (rules for employees)
- Technical Policy (rules for systems: encryption, firewalls)

---

7. Ethical Hacking (Offensive Security)

Ethical hacking is **legal hacking** done with permission to find weaknesses.

6 Phases of Ethical Hacking:

1. Reconnaissance
2. Scanning

3. Gaining Access
4. Maintaining Access
5. Clearing Logs
6. Reporting

---

8. Types of Hackers

- **White Hat:** Ethical / Legal
- **Black Hat:** Criminal
- **Grey Hat:** Unofficial but not malicious

---

9. Cyber Attacks

1. **Malware:** Virus, worms, trojans, ransomware
2. **DDoS:** Overloading server with traffic
3. **Phishing:** Fake emails or websites to steal data

✅ 📌 CONCLUSION — Lecture 15

Cyber Security protects systems, networks, and people from attacks.
Ethical Hacking complements Cyber Security by identifying vulnerabilities before criminals exploit them.
Organizations must secure:

- People (training)
- Devices (IoT, CCTV)
- Networks (firewalls, encryption)
- Systems (servers, hosts)

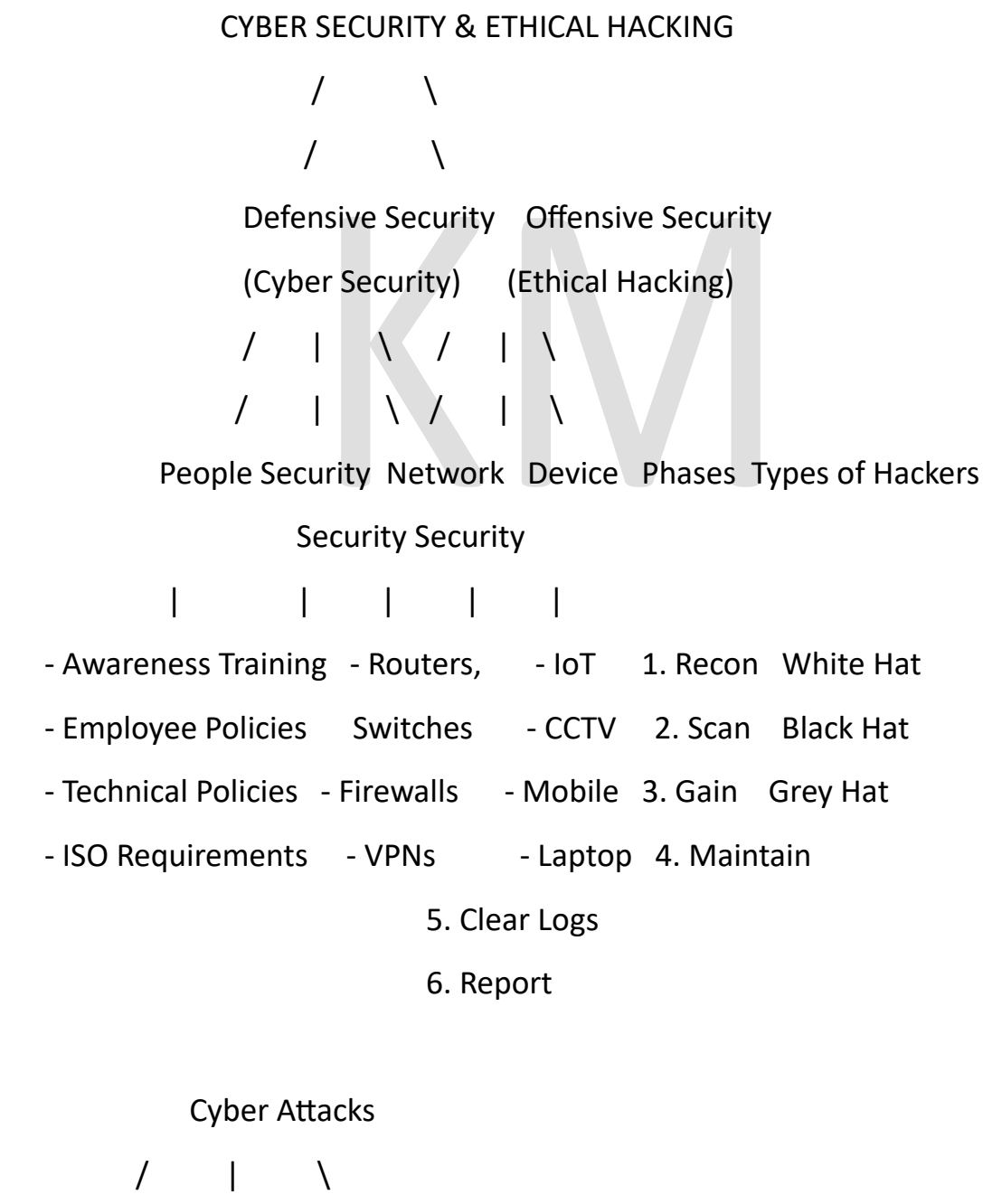
A skilled cybersecurity professional must understand:

- Attack types
- Defensive measures

- Ethical hacking phases
- Security policies
- Human and physical security

This chapter builds the foundation for both **defensive and offensive security**.

🎯 🧠 DETAILED MINDMAP — Cyber Security & Ethical Hacking



/ | \

Malware DDoS Phishing

(Virus, worm, trojan) (Traffic (Fake emails,

flood) fake websites)

🔥 ALL POSSIBLE INTERVIEW QUESTIONS + ANSWERS

⭐ 1. What is Cyber Security?

Answer:
Cyber security is the practice of protecting computers, networks, servers, and data from unauthorized access or attacks.
It focuses on **defense**, meaning its job is to **prevent attacks before they happen**.

⭐ 2. What is the difference between Data and Information?

Answer:

- **Data:** Raw facts (e.g., names, numbers)
- **Information:** Processed, meaningful data
  Example:
  Data → "100, John"
  Information → "John scored 100 marks"

⭐ 3. What is a Host Device and End Device?

Answer:

- **Host Device:** Provides services (Servers, Router, Firewall)
- **End Device:** Receives and uses services (Laptop, Mobile, Printer)

⭐ 4. What are IoT devices? Why are they risky?

Answer:
IoT devices are smart devices connected to internet. (Smart lights, fans, locks, CCTV)
They are risky because:

- They use **default passwords**
- Have **open ports**
- Lack **security updates**

⭐ 5. What is the difference between NVR and DVR?

Answer:

Type	Meaning	Use
NVR	Network Video Recorder	IP cameras (via LAN/WiFi)
DVR	Digital Video Recorder	Analog cameras (wired)

NVR requires **network security**.

⭐ 6. What is Security Awareness Training?

Answer:
Training given to employees every 6 months to prevent:

- Phishing
- Malware
- Social engineering
- Password mistakes

It reduces human error.

⭐ 7. What are Employee Policy and Technical Policy?

Answer:

- **Employee Policy:** Rules for employee behavior (password rules, device usage).
- **Technical Policy:** Rules for systems (firewalls, encryption, VPN configuration).

⭐ 8. What is Ethical Hacking?

Answer:
Ethical hacking is **legal hacking** done with permission to find vulnerabilities before attackers do.
Used for improving security.

⭐ 9. What are the phases of Ethical Hacking?

1. Reconnaissance – Information gathering
2. Scanning – Finding open ports/services
3. Gaining Access – Exploiting vulnerabilities
4. Maintaining Access – Creating persistence
5. Clearing Tracks – Erasing logs
6. Reporting – Documenting issues & solutions

⭐ 10. Types of Hackers?

- **White Hat:** Authorized, ethical
- **Black Hat:** Criminal
- **Grey Hat:** Unauthorized but not harmful

⭐ 11. What is Malware? Give examples.

Malware = Malicious Software designed to harm systems.
Examples:

- Virus
- Worm
- Trojan
- Ransomware
- Spyware
- Keylogger

⭐ 12. What is a DDoS attack?

A DDoS attack floods a server with huge traffic from multiple systems (botnet) to make it unavailable.

⭐ 13. Difference between DoS and DDoS?

- **DoS:** One machine attacks
- **DDoS:** Multiple machines attack simultaneously

⭐ 14. What is Phishing?

Phishing is a social engineering attack using fake emails/websites to steal:

- Passwords
- Bank information
- Personal data

⭐ 15. What is Cybersquatting?

Buying a domain similar to a famous brand to sell it for profit.
Example: jiohotstar.com case.

⭐ 16. What is ISO 27001?

An international standard for Information Security.
It sets rules for:

- Physical security
- Digital security
- Risk management

Example requirement: Boundary wall must be more than 9 feet.