🧠 Lecture 18 – Ethical Hacking & Information Gathering

💻 1. What is Ethical Hacking?

🔹 Definition:

Ethical Hacking is the **authorized process** of finding and fixing vulnerabilities in systems, applications, or networks using hacking techniques — but **legally and with permission**.

The main goal is to **identify security weaknesses before malicious hackers do.**

🔹 Why It's Important:

- To **protect organizations** from cyberattacks.
- To **test security systems** and identify loopholes.
- To **ensure compliance** with data security standards (like ISO, GDPR, etc.).

🔹 The Ethical Hacking Process (Phases)

Ethical hacking usually follows **five main stages** known as the **Hacking Lifecycle** or **Penetration Testing Phases**.

🧩 Phase 1: Reconnaissance (Information Gathering)

🔹 Meaning:

In this first step, the hacker (or ethical hacker) **gathers as much information as possible** about the target.

This phase is also known as **Footprinting**.

🔹 **Types of Reconnaissance:**

1. **Active Reconnaissance** – Directly interacting with the target (e.g., ping, port scan).
2. **Passive Reconnaissance** – Gathering data **without direct contact** (e.g., from public websites or social media).

🔹 **Information Collected:**

- IP addresses
- Domain details
- Employee names
- Emails and phone numbers
- Technology used (CMS, web server, etc.)

🔹 **Example Tools:**

- Google Dorking
- Whois lookup
- nslookup, dig, ping commands
- Maltego
- theHarvester

🧩 **Phase 2: Scanning**

🔹 **Meaning:**

Once basic information is gathered, the hacker **scans the network** to find **open ports, services, and vulnerabilities**.

🔹 **Objectives:**

- Identify **live hosts** in the network.
- Map **open ports** and **running services**.
- Detect **vulnerable systems**.

🔹 **Common Scanning Techniques:**

- **Port Scanning** – Find open ports using tools like **Nmap**.
- **Network Mapping** – Identify connected devices and routers.
- **Vulnerability Scanning** – Detect known weaknesses using scanners like **Nessus** or **OpenVAS**.

🧩 **Phase 3: Gaining Access**

🔹 **Meaning:**

After finding vulnerabilities, the hacker tries to **exploit them** to gain unauthorized access to the system.

🔹 **Methods Used:**

- Exploiting **weak passwords** or **unpatched software**.
- Using **SQL Injection**, **XSS**, or **Buffer Overflow** attacks.
- Sending **malware payloads** or **remote shells**.

🔹 **Objective:**

To get **administrator-level privileges** or **control over the target system**.

🧩 Phase 4: Maintaining Access

🔹 Meaning:

Once access is gained, hackers try to **maintain that access** for future use — so they can return anytime.

🔹 How They Do It:

- Installing **backdoors** or **Trojans**.
- Creating **hidden user accounts**.
- Using **rootkits** to remain undetected.

🔹 Purpose:

To ensure persistent access even if the vulnerability is later patched or the system is rebooted.

🧩 Phase 5: Clearing Tracks

🔹 Meaning:

After completing the attack, hackers **erase all evidence** to avoid detection.

🔹 How They Hide:

- **Deleting event logs** (so system admin can't trace them).
- **Clearing IP and MAC addresses** from logs.
- **Using VPNs or proxies** to hide their identity.

🔹 Objective:

To leave **no trace of intrusion** and **avoid forensic tracking.**

🔍 2. Information Gathering Tools and Techniques

This is part of the **Reconnaissance phase**, but it's such an important step that it deserves detailed notes.

⚙️ A. Google Dorking (Advanced Google Search)

🔹 Meaning:

Google Dorking (or Google Hacking) is a technique used to **find hidden information** on websites using **advanced search operators**.

It helps discover:

- Exposed files (PDFs, Excel, etc.)
- Login pages
- Database errors
- Sensitive directories

🔹 Example Google Dorks:

Command	Use
intext:ethical hacking	Finds pages containing "ethical hacking" in the text.
filetype:pdf ethical hacking	Finds PDFs related to ethical hacking.
site:codingseekho.in	Searches only inside that website.
intext:username filetype:xls	Finds Excel files that contain the word "username".
inurl:codingseekho	Finds URLs containing the word "codingseekho".
indexof:ethicalhacking	Finds open directories related to "ethical hacking".

🔹 **Useful Website:**

- Exploit-DB Google Hacking Database
  → Contains hundreds of **ready-made Google Dork queries** to find vulnerabilities and exposed data.

⚙️ **B. Whois Lookup**

🔹 **Website:**

👉 https://www.whois.com/whois/

🔹 **Purpose:**

Used to find **domain registration information**, such as:

- Owner's name and contact details
- Registrar name
- Creation and expiry date
- Server name and DNS details

🔹 **Example:**

Searching for codingseekho.in on Whois will show:

- Domain owner information
- IP address
- Hosting provider
- DNS servers

⚙️ **C. Linux Commands for Info Gathering**

These commands are available in **Kali Linux** and other pentesting OS.

1. dig <domain>

- Stands for **Domain Information Groper**.

- Used to gather DNS records and the IP address of the domain.
- Example: dig codingseekho.in

2. ping <domain>

- Tests if the target host is active and measures latency.

3. nslookup <domain>

- Used to query DNS to get IP addresses and hostnames.

⚙️ D. theHarvester Tool

🔹 Definition:

theHarvester is a powerful **open-source reconnaissance tool** used to **gather emails, subdomains, IPs, and hosts** related to a target domain.

It searches across:

- Search engines (Google, Bing, Yahoo)
- Social networks
- Public databases

🔹 How to Use:

1. Open **Kali Linux Terminal**.
2. Type command:
3. theHarvester -h

→ Shows all available options and help menu.

4. Example:
5. theHarvester -d codingseekho.in -l 300 -b all
    - -d = domain name
    - -l = number of results (limit)
    - -b = data source (like Google, Bing, etc. or use all)

It will list all related emails, subdomains, IPs, and servers.

⚙️ E. HTTrack Website Copier

🔹 **Meaning:**

HTTrack is a **website cloning tool** that downloads an entire website (including pages, images, scripts) for **offline analysis**.

🔹 **Use Case:**

Ethical hackers use it to:

- Study website structure.
- Find **hidden directories or sensitive files**.
- Analyze **source code** for vulnerabilities.

🔹 **Example:**

If a website has **downloadable videos or files**, HTTrack can fetch those files along with the HTML structure.

⚙️ F. Maltego

🔹 **What is Maltego:**

Maltego is an **advanced data mining and link analysis tool** used for **open-source intelligence (OSINT)** and **digital forensics**.

It visually shows **relationships between people, companies, emails, social media accounts, and domains**.

🔹 **Main Features:**

- Collects public information about any target.
- Displays data in **graph format** (nodes and connections).

- Can link **email addresses → social accounts → phone numbers → domains.**
- Used widely by **law enforcement agencies**, cybersecurity analysts, and **digital investigators**.

🔹 **Example Usage:**

If you input an **email address**, Maltego can show:

- All social media profiles linked to that email.
- Whether it appeared in **data leaks**.
- Which websites or databases it's associated with.

This helps **trace people or organizations** during investigations.

🔹 **How to Download Maltego:**

1. Go to official site: https://www.maltego.com/downloads/
2. Choose your OS (Windows, Linux, macOS).
3. Create a free account on the site.
4. Download **Maltego CE (Community Edition)** – it's free.
5. Install and open the application.
6. Log in with your Maltego account and start using.

🔹 **How to Use Maltego:**

1. Open Maltego → select **"New Graph"**.
2. Enter a target (like email, phone, domain, IP).
3. Choose **Transform** → Maltego will start gathering info.
4. It will show **connected entities** in real-time.

🔹 **Why Maltego Is Used:**

- Digital Forensics & Cybercrime investigation.
- Social engineering and OSINT research.
- Tracing criminal networks, phishing campaigns, or leaked data.

🧩 **3. Summary Table**

Phase / Tool	Purpose	Example / Command
Reconnaissance	Gather target info	Whois, Google Dorks, dig
Scanning	Identify open ports & vulnerabilities	Nmap, Nessus
Gaining Access	Exploit weaknesses	SQL Injection, Metasploit
Maintaining Access	Keep connection alive	Backdoors, Rootkits
Clearing Tracks	Erase evidence	Delete logs, hide IP
Google Dorking	Find hidden data using Google	intext:username filetype:xls
Whois Lookup	Domain details	whois.com
theHarvester	Gather emails, subdomains	theHarvester -d example.com -l 300 -b all
HTTrack	Clone website for offline analysis	Website Copier
Maltego	OSINT & Relationship Mapping	Trace emails, phones, social accounts

---

✅ **Final Takeaway:**

- Ethical Hacking is done **legally** to strengthen security.
- The **5 Phases** form the foundation of every penetration test.

- Tools like **Google Dorking, theHarvester, HTTrack, and Maltego** make **information gathering efficient and professional.**
- Every step should be done **with authorization** to remain ethical and legal.