NETWORKING & RECONNAISSANCE

🔰 MODULE 2: Networking Basics & Reconnaissance

> "You can't hack what you don't understand. Learn the network, and you unlock the world."

🧠 Lesson 2.1 – What is Networking? (In-Depth)

🔗 What is a Network?

A **network** is a group of devices (computers, smartphones, servers, etc.) that are connected to each other and **share data**.

Imagine a **road system**. Roads = Cables/Wi-Fi

Cars = Data

GPS = Routing

📶 How Data Travels in a Network

When you visit `google.com`:

1. Your browser sends a **request** to Google's IP.
2. This request travels through **your router**, then to your **ISP (like Jio or Airtel)**.
3. The ISP forwards it to the **Google server**.
4. The server sends back a **response (HTML, CSS, JS, images)**.
5. You see the Google homepage.

All of this happens in **milliseconds**.

💡 Important Networking Devices

Device	Role
Router	Connects different networks (e.g., home to internet).
Switch	Connects multiple devices in the same network (LAN).
Modem	Connects your home to the ISP using phone/fiber lines.
Firewall	Controls traffic and blocks unwanted access.
Access Point	Lets Wi-Fi devices join the wired network.
Server	Stores data and handles requests (like a digital waiter).
Client	Your laptop/phone that requests data.

🧠 Lesson 2.2 – Types of Networks (With Use Cases)

Type	Use Case	Range
LAN (Local Area Network)	Home Wi-Fi, School Labs, Offices	10m – 100m
WAN (Wide Area Network)	Internet, MPLS lines between cities	Global
PAN (Personal Area Network)	Bluetooth headphones, smartwatch	1–10m
MAN (Metropolitan Area Network)	City-wide cable networks	Several km

> Ethical Hackers must understand LANs and WANs especially for local attacks and external exploitation.

🧠 Lesson 2.3 – The OSI Model (Simplified Deep Dive)

The **OSI model** breaks networking into 7 layers to understand how data moves.

Layer	Name	Role	Example
7	**Application**	User-facing apps	Chrome, WhatsApp
6	**Presentation**	Encryption/Decryption	SSL/TLS, JPEG
5	**Session**	Starts/stops connection	Login/Logout

4	**Transport**	Ensures delivery	TCP/UDP, Ports
3	**Network**	Finds best path	IP, Routers
2	**Data Link**	Sends frames to next device	MAC address
1	**Physical**	Sends electrical signals	Cables, Wi-Fi

> 🧠 Hackers often focus on Layer 3 (IP) to Layer 7 (Apps) for scanning and exploitation.

🧠 Lesson 2.4 – Reconnaissance in Hacking (Highly Practical)

Recon = Information gathering

Before hacking any system, you must gather **intel**. This step is **80% of hacking**. The better your recon, the easier your attack.

🧍 Types of Recon:

Type	Description	Tools
Passive	No contact with target. Safe and stealthy.	Google, WHOIS, social media
Active	Directly interact with target. Risky but detailed.	Nmap, ping, traceroute
OSINT	Gathering info from public resources.	theHarvester, Shodan, Google Dorking

🧠 Real Goals of Recon:

- Discover target **IP addresses**
- Find **open ports & services**
- Uncover **employee emails**
- Detect **CMS (WordPress, Drupal)**
- Identify **firewalls or WAFs**
- Find **subdomains**, internal apps
- List **technologies** used (e.g., Apache, MySQL, jQuery)

📦 Example of Passive Recon:

You want to target `targetcompany.com`. You can find:

- Emails via Google: `@targetcompany.com`
- Subdomains via Sublist3r: `admin.targetcompany.com`
- Employees via LinkedIn
- Tech Stack via Wappalyzer: **PHP, Apache 2.4, MySQL**

> 🧠 A single misconfigured subdomain might give access to an internal admin panel.

🧠 Lesson 2.5 – Top Recon Tools (Explained)

Tool	Category	What it Does
whois	Passive	Owner info of a domain (contact, registrar, DNS)
nslookup / dig	Passive	DNS records, mail servers, A/NS records
theHarvester	Passive/OSINT	Finds emails, domains via search engines
Shodan	OSINT	Google for exposed devices (cameras, databases)
Sublist3r	Passive	Finds subdomains using OSINT
WhatWeb / Wappalyzer	Passive	Reveals website's tech stack
Nmap	Active	Scans IPs, detects open ports, OS, services
Recon-ng	Active OSINT	Python recon tool with modules for automation
Google Dorking	Passive	Advanced search queries to find secrets/files

🔒 Legal Note (Must-Read!)

⚠️ **NEVER scan, recon, or touch systems you don't own or have permission for.**

- Passive recon might be legal in some countries.

- Active recon (like Nmap) **can get you jailed** without permission.

Always work in labs, CTFs, or bug bounty programs with authorized scope.

✅ Summary – Module 2 Key Takeaways

Topic	Key Insight
Networking	Backbone of hacking. Know how devices talk.
OSI Model	Every hack hits a layer. Focus on 3–7.
Recon	First step of hacking. Info = Power.
Tools	Start with WHOIS, Nmap, theHarvester, Shodan.
Law	No permission = illegal, even for scanning.