📘 Networking Notes – Ethical Hacking (Lecture 1)

1. Networks

- A **network** is a collection of computers, devices, or servers connected together to share data and resources.
- Networks allow communication (emails, messages, file transfer, internet browsing).
- Two main types:
    - **LAN (Local Area Network):** Small area like home, office.
    - **WAN (Wide Area Network):** Covers large areas like cities, countries, the internet.

---

2. IP Address

- An **IP (Internet Protocol) address** is a unique number given to every device in a network.
- It identifies a device's location on a network (like a digital home address).
- Example: 192.168.1.1

---

3. Types of IP Address

- **Static IP:**
    - Manually assigned and doesn't change.
    - Useful for servers, hosting websites, and CCTV.
- **Dynamic IP:**
    - Automatically assigned by ISP using **DHCP (Dynamic Host Configuration Protocol)**.
    - Changes whenever you reconnect to the network.
    - Common for normal users (cheaper & safer).

4. ipconfig /all

- A **Windows command** used to check network details.
- It shows:
    - IP address
    - Default gateway
    - DNS server
    - MAC address (Physical address)

---

5. ISP (Internet Service Provider)

- The company that provides internet access.
- Examples: Jio, Airtel, BSNL.
- ISPs assign you an IP address and control how you connect to the internet.

---

6. PING

- A **network command** to test connectivity between two devices.
- Example: ping google.com → checks if Google's server is reachable.
- Works by sending small data packets and measuring **response time (latency).**
- Useful in troubleshooting.

---

7. IPv4 (Internet Protocol version 4)

- Uses **32-bit addressing system**.
- Total available addresses: ~4.2 billion.
- Format: 192.168.1.1 (4 octets separated by dots).
- Problem: Almost all addresses are used (shortage).

---

8. IPv6 (Internet Protocol version 6)

- Uses **128-bit addressing system**.
- Total available addresses: ~520 billion *billion* (practically unlimited).
- Format: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- Needed because IPv4 is running out.
- Supports better security and faster routing.

---

9. DNS Server (Domain Name System)

- Converts **domain names** into **IP addresses**.
- Example:
  - You type: www.google.com
  - DNS translates it to: 142.250.190.14
- Without DNS, we would have to remember numbers instead of names.

---

10. Physical Address (MAC Address)

- **MAC (Media Access Control) address** = Unique ID assigned to your network card (NIC).
- Written in hexadecimal (e.g., 00:1A:2B:3C:4D:5E).
- Works at the hardware level.
- Cannot be changed (though can be spoofed in hacking).

---

11. Logical Address (IP Address)

- Unlike MAC (physical), an **IP address is logical** and can be changed.
- Used for identifying devices in a network.
- Works at software/network level.

---

12. Classes of IP Address

IP addresses are divided into **classes** based on range:

- **Class A:** 1–126 → Large networks (millions of devices).
- **Class B:** 128–191 → Medium networks.
- **Class C:** 192–223 → Small networks (most common for homes).
- **127.x.x.x:** Reserved for **loopback (testing only).**

---

13. 127.0.0.1 (Loopback Address)

- Special IP used for testing your own computer.
- If you ping 127.0.0.1, you're checking whether your network card is working.
- Nickname: **localhost**.

---

14. NIC Card (Network Interface Card)

- A hardware component that connects your computer to a network.
- Every NIC has a **MAC address**.
- Without NIC, you can't connect to LAN/Wi-Fi.

✅ SUMMARY of the Chapter

This chapter introduces the fundamentals of computer networking. It explains how devices communicate in a network, how IP addresses work, and the difference between IPv4 and IPv6. You learn about LAN/WAN, MAC addresses, DNS, ISP, and basic commands like ipconfig and ping. The chapter builds understanding of how devices identify each other using logical (IP) and physical (MAC) addresses and how data travels on the internet. It also covers IP address classes and the loopback address.

✅ CONCLUSION

This chapter builds the foundation for ethical hacking by explaining how networks operate. It teaches the importance of IP addressing, MAC addresses, DNS, NIC cards, and key commands used in troubleshooting. Understanding these concepts is essential before learning scanning, enumeration, or exploitation in ethical hacking. Mastering these basics helps you think like both a defender and an attacker — since all attacks and defenses begin with understanding networks.

✅ DETAILED MINDMAP

Networking

|

├── 1. Networks

| ├── Definition: Connected devices sharing data/resources

| ├── LAN – Small area (home/office)

| └── WAN – Large area (cities/countries)

|

├── 2. IP Address

│ ├── Unique number for device identification

│ ├── Example: 192.168.1.1

│ └── Acts like digital home address

│

├── 3. Types of IP

│ ├── Static IP – Permanent, manual, used for servers

│ └── Dynamic IP – Temporary, via DHCP, common for users

│

├── 4. ipconfig /all

│ ├── Shows IP address

│ ├── Default Gateway

│ ├── DNS Server

│ └── MAC Address

│

├── 5. ISP

│ ├── Provides internet access

│ ├── Assigns IP address

│ └── Examples: Jio, Airtel

│

├── 6. PING

│ ├── Tests connectivity

│ ├── ping google.com

│ ├── Measures latency

│ └── Troubleshooting tool

├── 7. IPv4
│ ├── 32-bit address
│ ├── 4 octets
│ └── ~4.2 billion addresses
│
├── 8. IPv6
│ ├── 128-bit address
│ ├── Practically unlimited
│ └── Better security & routing
│
├── 9. DNS
│ ├── Converts domain to IP
│ └── Example: google.com → 142.250.190.14
│
├── 10. MAC Address
│ ├── Hardware address
│ ├── Hex format
│ └── Unique for every NIC
│
├── 11. Logical vs Physical Address
│ ├── Logical = IP (changeable)
│ └── Physical = MAC (permanent)

├── 12. IP Classes

│ ├── Class A: 1–126

│ ├── Class B: 128–191

│ ├── Class C: 192–223

│ └── 127.x.x.x = Loopback

│

├── 13. 127.0.0.1 (Loopback)

│ └── Tests your own network card

│

└── 14. NIC Card

├── Connects device to network

└── Has a MAC address

✅ INTERVIEW QUESTIONS + SIMPLE DETAILED ANSWERS

---

1. What is a network?

Answer:
A network is a group of connected devices (computers, servers, phones) that share data and resources. It allows communication like emails, browsing, and file transfer.

---

2. What is the difference between LAN and WAN?

Answer:

- **LAN:** Covers a small area like home or office.
- **WAN:** Covers a large area like cities, countries, or the internet.

---

3. What is an IP address?

Answer:
An IP address is a unique identification number assigned to a device on a network. It works like a digital address that tells where the device is located on the network.

---

4. What is the difference between Static IP and Dynamic IP?

Answer:

- **Static IP:** Manually assigned, doesn't change, used for servers and CCTV.
- **Dynamic IP:** Given automatically by DHCP, changes frequently, used for normal users.

---

5. What is DHCP?

Answer:
DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses to devices, so users don't have to set it manually.

---

6. What does the command ipconfig /all do?

Answer:
It shows complete network information including IP address, MAC address, DNS server, and default gateway.

---

7. What is an ISP?

Answer:
ISP (Internet Service Provider) is a company that gives internet access and assigns IP addresses (e.g., Jio, Airtel).

---

8. What is PING and why is it used?

Answer:
PING checks if one device can reach another device over the network. It sends small packets and measures the response time. Used for troubleshooting connectivity issues.

---

9. Difference between IPv4 and IPv6?

Answer:

- **IPv4:** 32-bit address, 4.2 billion addresses.
- **IPv6:** 128-bit address, almost unlimited, better security.

---

10. Why was IPv6 created?

Answer:
Because IPv4 addresses were running out due to increasing number of devices.

---

11. What is a DNS server?

Answer:
DNS converts domain names (google.com) into IP addresses. Without DNS, users would have to remember numeric addresses.

---

12. What is a MAC address?

Answer:
A MAC address is a permanent hardware identifier given to a network interface card (NIC). It is written in hexadecimal and is unique for every device.

---

13. Difference between Logical and Physical addresses?

Answer:

- **Logical Address:** IP address, software-based, can change.

- **Physical Address:** MAC address, hardware-based, cannot change (but can be spoofed).

---

14. What are IP Address Classes?

Answer:

- **Class A:** 1–126, large networks.
- **Class B:** 128–191, medium networks.
- **Class C:** 192–223, small networks.
- **127.x.x.x:** Reserved for loopback testing.

---

15. What is 127.0.0.1 used for?

Answer:
It is the **loopback address** used to test if your own computer's networking hardware and software are working.

---

16. What is a NIC card?

Answer:
NIC (Network Interface Card) connects a computer to a network and contains the MAC address.

---

17. What is a Default Gateway?

Answer:
It is the router or device that connects your local network to the outside internet.

---

18. What is an octet in IPv4?

Answer:
IPv4 has 4 octets (each 8 bits). Example: 192.168.1.1

---

19. What is latency?

Answer:
Latency is the time a packet takes to travel from one device to another. Measured in milliseconds.

---

20. Can a MAC address be changed?

Answer:
Not permanently. But it can be **spoofed** temporarily for testing or security purposes.