Edversity.

CYBERSECURITY SPECIALIZATION PROGRAM WEEK 2 - DAY 1

Instructor: Muddassir Shafique

TA: Suleiman Taj

Agenda

Week 1: Introduction to Cyber Security and Kali Linux (Completed)

Week 2: Networking and Security Fundamentals

Week 3: Cryptography

Week 4: OS Security

Week 5: Web Security

Week 6: Incident Response and Management

Week 7: Security Policies and Risk Management

Week 8: Emerging Technologies and Future trends

Week 9: CAPSTONE Project and Review

Week 10: CAPSTONE Project Presentations

What We'll Learn Today

- Introduction to Networking
- Understand networks, devices, IPs, etc
- Practice with basic tools

Why Learn Networking?

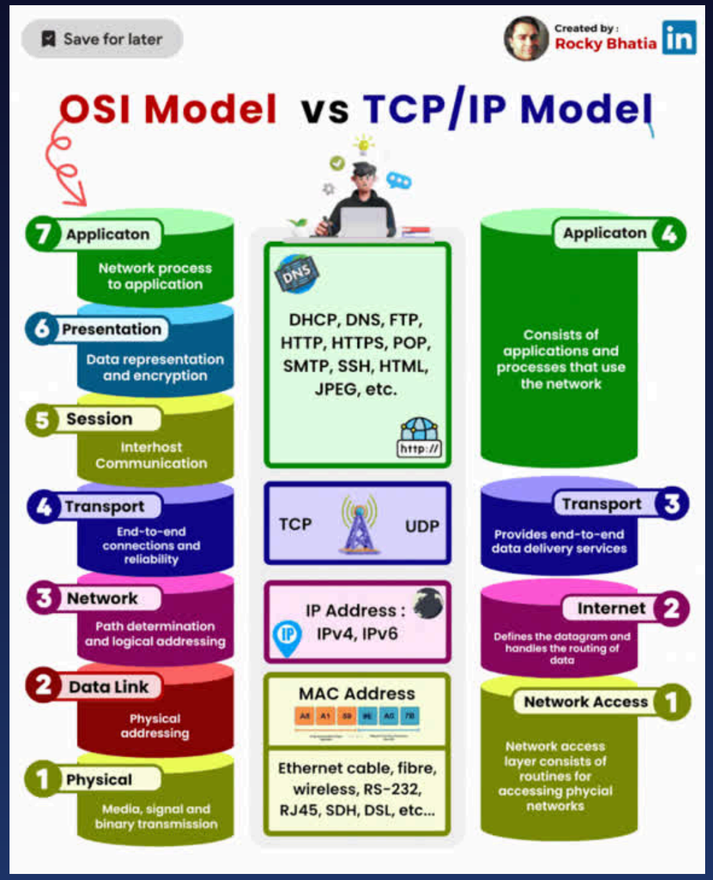
- All modern systems are networked
- Helps troubleshoot issues
- Builds foundation for cybersecurity

What is Network?

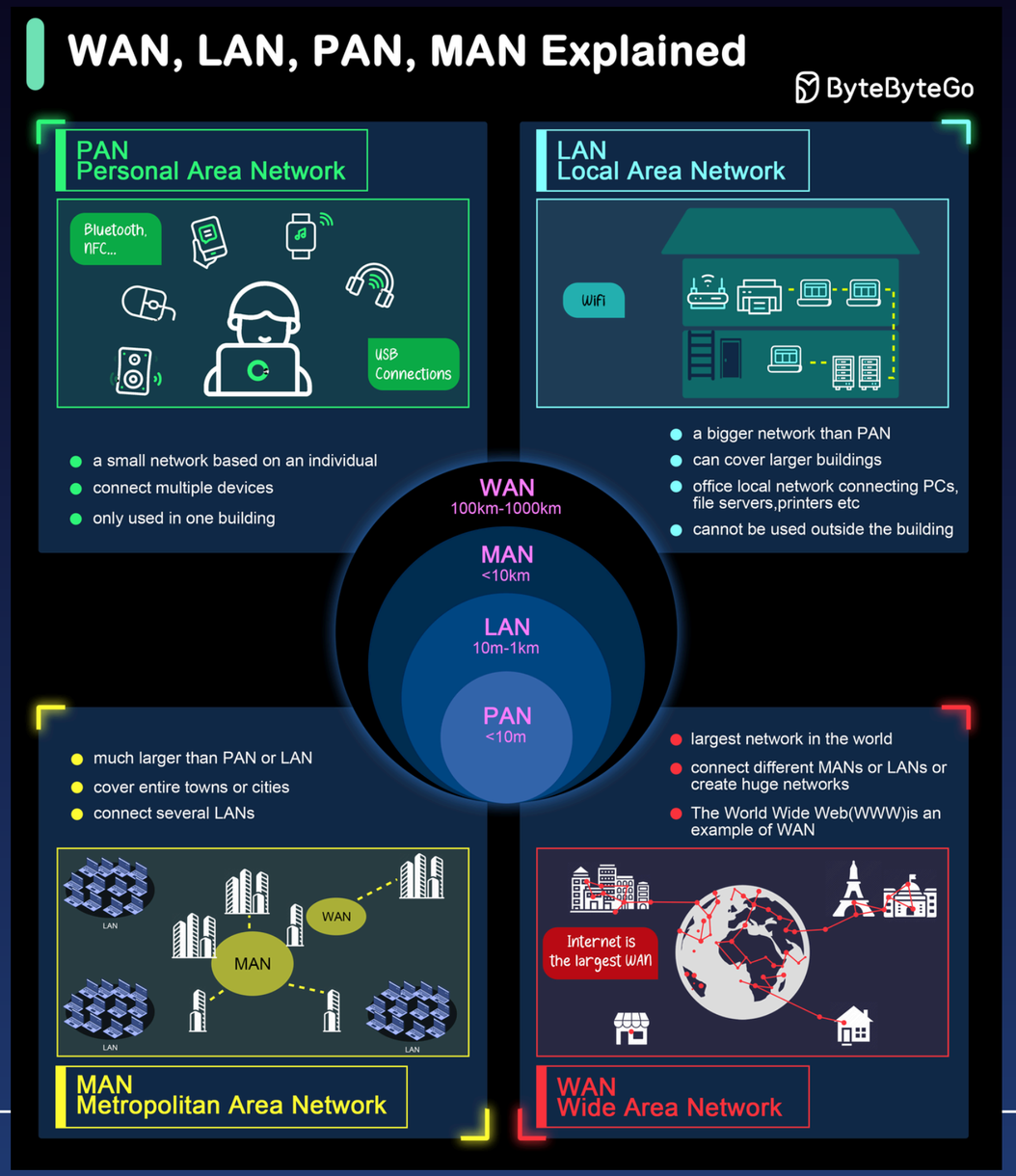
A network is a collection of computers, servers, mainframes, network devices, and other devices connected to each other to share data and resources.

OSI and TCP/IP Models

The OSI Model is a 7-layer framework that standardizes network functions to help with troubleshooting, design, and understanding. Each layer represents a different function involved in the process of communication between devices on a network.



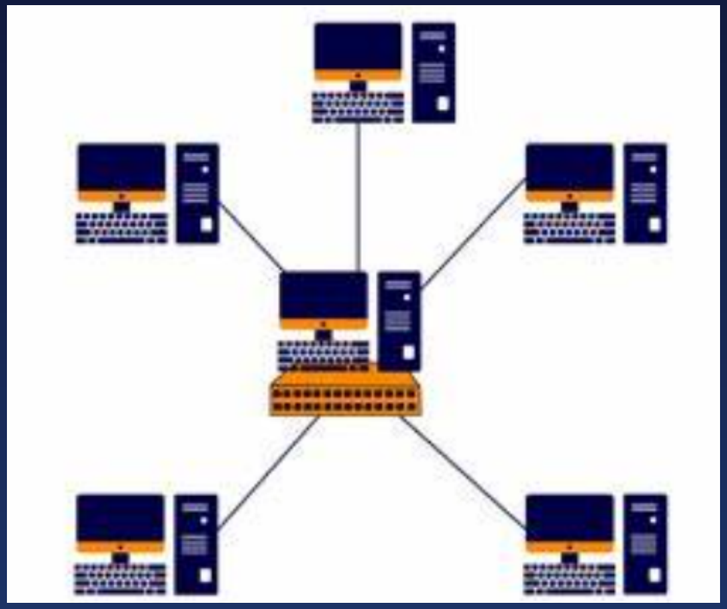
Types of Networks



Network Topologies

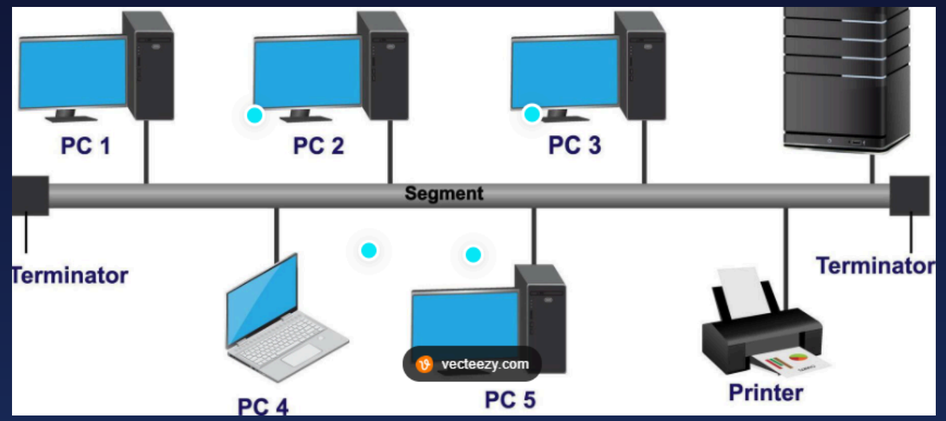
Network topology is the blueprint of how devices are connected and communicate in a network. It plays a key role in the efficiency, cost, and resilience of a network system.

- **Star Topology**
- **Structure:** All nodes are connected to a central hub or switch.
- **Pros:**
- Easy to install and manage.
- Failure of one node doesn't affect the rest of the network.
- **Cons:**
- Central hub failure affects whole network



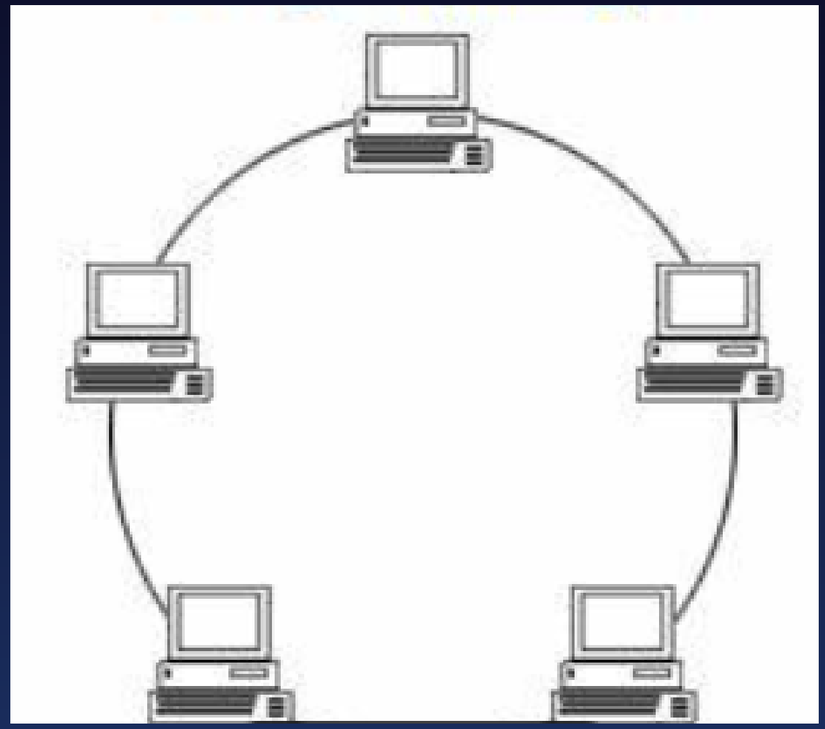
Network Topologies

- **2. Bus Topology**
- **Structure:** All nodes are connected to a single backbone cable.
- **Pros:**
- Easy to implement for small networks.
- Uses less cable than star topology.
- **Cons:**
- A break in the main cable can bring down the entire network.
- Performance degrades with more nodes or high traffic.



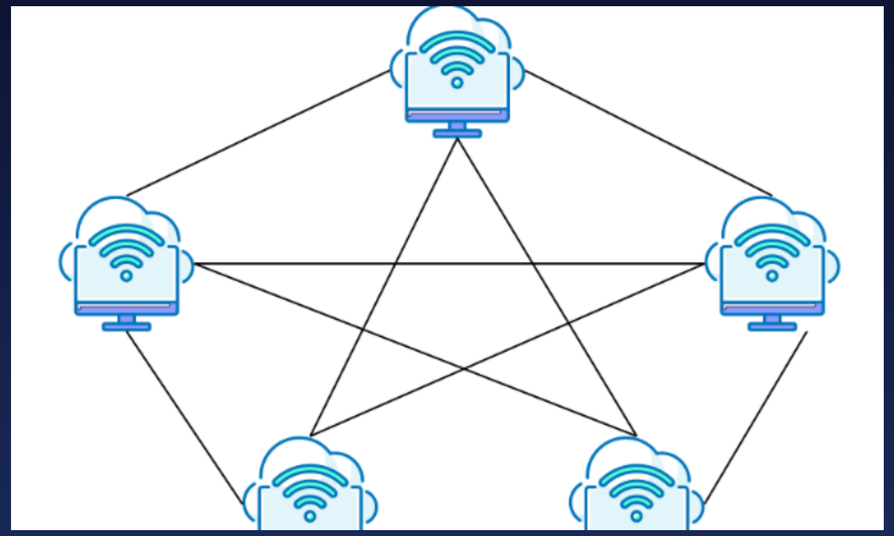
Network Topologies

- **3. Ring Topology**
- **Structure:** Each node is connected to exactly two other nodes, forming a closed loop.
- **Pros:**
- Data flows in one direction, reducing the chance of collisions.
- **Cons:**
- A break in the ring can disrupt the entire network unless a dual ring is used.



Network Topologies

- **4. Mesh Topology**
- **Structure:** Every node is connected to every other node.
- **Pros:**
- High redundancy and fault tolerance.
- Reliable, as data can be rerouted if one path fails.
- **Cons:**
- Expensive and complex to install due to the number of connections required.



IP Addressing

Definition:

IP (Internet Protocol) is a fundamental network layer protocol used for identifying devices and routing data across networks, especially the Internet.

🧠 Key Concepts of IP:

Term	Description
IP stands for	Internet Protocol
Layer	Network Layer (Layer 3 in OSI model; Internet layer in TCP/IP model)
Function	Addressing and routing packets between computers
Works with	TCP, UDP, ICMP, and other protocols

IPv4 vs IPv6

- IPv4: 192.168.1.1
- IPv6: longer, newer format

Aspect	IPv4	IPv6
Security	Less secure by default	Better security features (IPSec, NDP)
Addressing	Limited (32-bit), needs NAT	Huge (128-bit), no NAT needed
Scanning Risk	Easy to scan networks	Very hard to scan due to huge space
Spoofing Risk	High (ARP spoofing)	Lower (NDP + Secure NDP)
Firewall/IDS Support	Mature	Still developing in some tools
Transition Risks	N/A	Tunnels like 6to4 can be exploited

Public vs Private IPs

- Private: for local use
- Public: connects to internet

Feature	Private IP	Public IP
Used In	Local networks (home, office)	Internet (globally routable)
Reachable From Internet?	❌ No (without port forwarding or NAT)	✅ Yes
Assigned By	Local admin / router	ISP (Internet Service Provider)
Security Risk	Lower (not directly exposed)	Higher (directly reachable)
NAT Required?	✅ Yes	❌ No
Example Ranges	192.168.0.0 – 192.168.255.255 10.0.0.0 – 10.255.255.255 172.16.0.0 – 172.31.255.255	Varies (e.g., 8.8.8.8, 142.250.72.4

Subnetting Basics

What is Subnetting

- Subnetting is the process of dividing a larger IP network into smaller, more manageable subnetworks (subnets). This helps improve network performance, organization, and security by limiting broadcast domains and making IP address allocation more efficient.

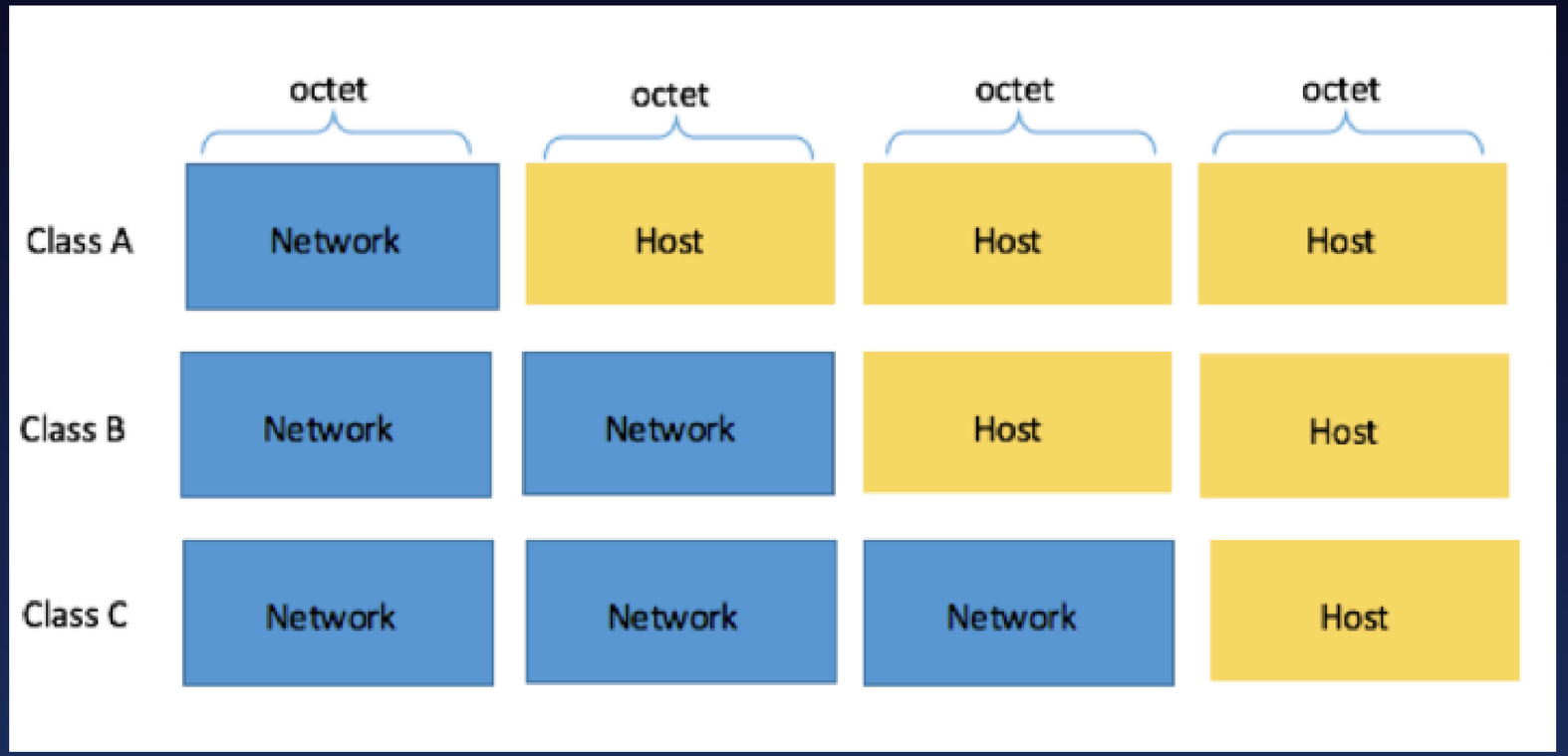
Why ?

- Efficient use of IP addresses.
- Reduce network congestion by isolating traffic.
- Improve security by separating network segments.
- Easier management of large networks.

How Subnetting Works:

- An IP address has two main parts:
- Network portion (identifies the network)
- Host portion (identifies devices on that network)

Subnetting Basics



Subnetting Basics

Class	IP Range	Default Subnet Mask	Network Bits	Host Bits	Max Networks	Max Hosts per Network
A	1.0.0.0 to 126.255.255.255	255.0.0.0 (/8)	8	24	128	16,777,214
B	128.0.0.0 to 191.255.255.255	255.255.0.0 (/16)	16	16	16,384	65,534
C	192.0.0.0 to 223.255.255.255	255.255.255.0 (/24)	24	8	2,097,152	254
D	224.0.0.0 to 239.255.255.255	Multicast addresses	N/A	N/A	N/A	N/A
E	240.0.0.0 to 255.255.255.255	Experimental, research	N/A	N/A	N/A	N/A

MAC Addresses

A MAC address (Media Access Control address) is a unique identifier assigned to a network interface card (NIC) of a device, used for communication on the local network (e.g., within a Wi-Fi or Ethernet network).

Feature	Description
Stands for	Media Access Control address
Layer	Data Link Layer (Layer 2 of OSI model)
Format	48-bit hexadecimal (e.g., `00:1A:2B:3C:4D:5E`)
Scope	Works within a local network (LAN)
Uniqueness	Intended to be globally unique per device interface

MAC Addresses

Structure of a MAC Address:

- Typically written as 6 pairs of hexadecimal digits (12 characters).
- Example: F8:27:93:6A:1C:EF
- First 3 bytes (OUI): Identify the manufacturer (e.g., Intel, Apple).
- Last 3 bytes: Unique identifier assigned by the manufacturer.

MAC vs. IP Address:

Feature	MAC Address	IP Address
Level	Data Link Layer (L2)	Network Layer (L3)
Purpose	Unique device ID in a local network	Address for routing over Internet
Changeable	Usually fixed (can be spoofed)	Assigned dynamically or statically
Format	Hexadecimal (e.g., `00:1B:44:11:3A:B7`)	Decimal (e.g., `192.168.1.1`)

MAC Addresses

What is OUI in a MAC Address?

OUI (Organizationally Unique Identifier) is the first 24 bits (3 bytes) of a MAC address, and it identifies the manufacturer or vendor of the network interface card (NIC)

Structure of a MAC Address: F0-A6-54-7C-2A-89

First 3 bytes (F0:A6:54) → OUI: Assigned to the manufacturer.

Last 3 bytes (7C:2A:89) → Unique identifier for the device from that manufacturer.

MAC Addresses

How to Identify the Manufacturer Using a MAC Table

A MAC table (usually from a switch) lists the MAC addresses of connected devices and their associated ports. To identify the manufacturer, follow these steps:

Step-by-Step Method:

1. Get the MAC address from your machine.

Example: F0-A6-54-7C-2A-89

2. Extract the OUI:

First 3 bytes: F0-A6-54

3. Use an OUI lookup tool:

Online OUI lookup tools:

IEEE OUI Lookup Tools

macvendors.com

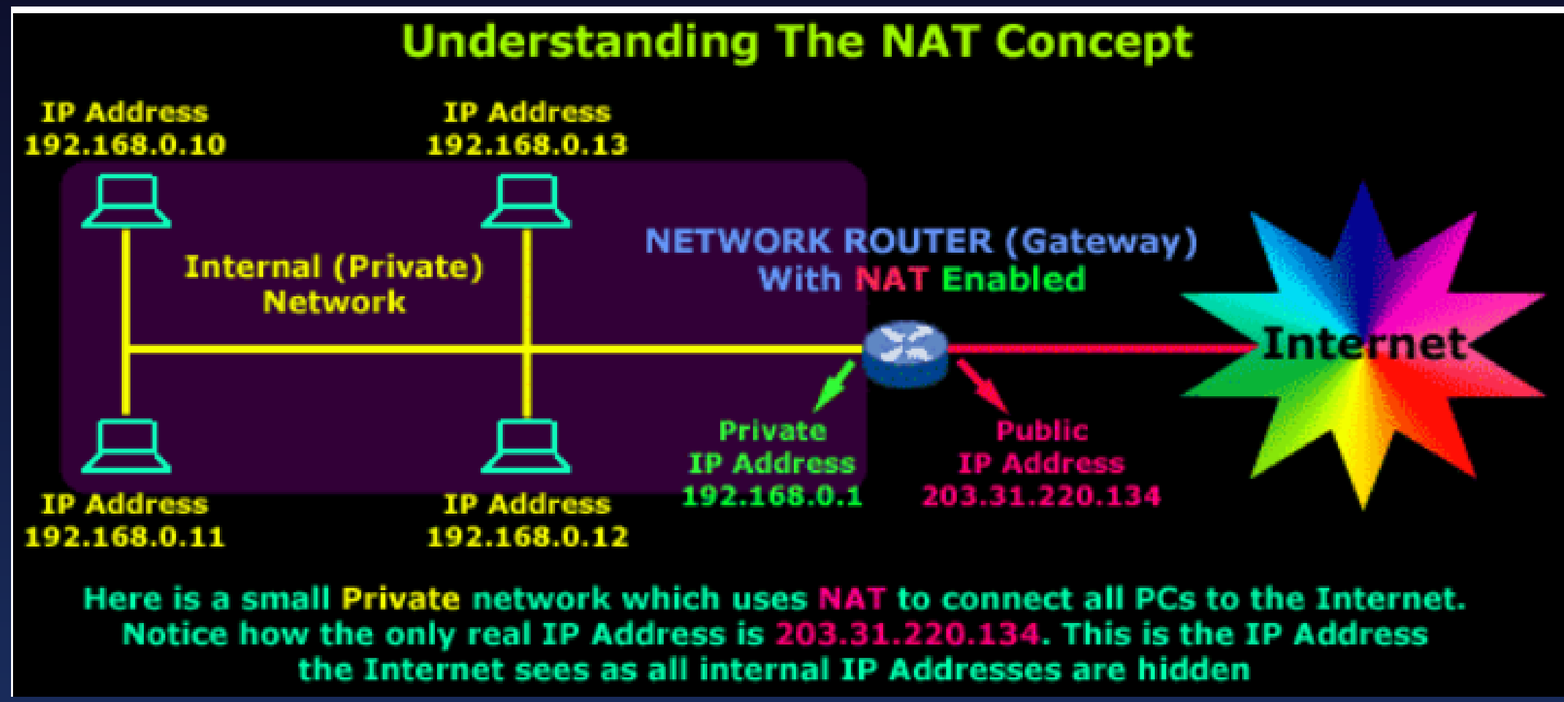
Wireshark OUI list

4. Look up the OUI:

D4:6A:6A → Apple, Inc.

NAT

- **Network Address Translation (NAT)**
- **Purpose:**
- Translates private IP addresses (used inside a local network) to a public IP address (used on the internet).
- Allows multiple devices to share a single public IP address.
- Adds a layer of security by hiding internal IP addresses from the outside world.



Ports

A port is a logical communication endpoint that helps direct data to the right application or service on a device.
When data reaches a device (via its IP address), the port number tells the device which specific service or application should handle the data — just like an apartment number in a building.

Concept

Term	Description
IP Address	Identifies a device on a network.
Port Number	Identifies a specific process or service on that device.
Socket	Combination of IP address + port number (e.g., `192.168.1.10:80`).

Ports

Port Ranges

Port Range	Type	Examples
0 – 1023	**Well-Known Ports**	HTTP (80), HTTPS (443), FTP (21), SSH (22)
1024 – 49151	**Registered Ports**	Assigned to user processes/apps like databases
49152 – 65535	**Dynamic/Private Ports**	Temporary ports for outbound traffic (e.g., browser sessions)

Common Well-Known Ports

Service	Protocol	Port Number
HTTP	TCP	80
HTTPS	TCP	443
FTP	TCP	21
SSH	TCP	22
DNS	UDP	53
SMTP (Email)	TCP	25
DHCP	UDP	67/68
RDP (Remote Desktop)	TCP	3389

Ports

Commands to check Open Ports

Tool	OS	Command Example	Description
`netstat`	Windows/Linux	`netstat -an` or `netstat -tuln`	Show open ports and states
`ss`	Linux	`ss -tuln`	Modern replacement for netstat
`nmap`	Linux	`nmap -sT localhost`	Scan open ports on a target
`lsof`	Linux	`lsof -i -P -n`	List open files/ports
PowerShell	Windows	`Get-NetTCPConnection`	PowerShell way to list ports

Ports

Commands to close Open Ports

Method	Windows	Kali Linux
Stop service	`services.msc` or `sc stop`	`systemctl stop <service>`
Kill process	`taskkill /PID`	`kill -9 <PID>`
Block port via firewall	GUI or `New-NetFirewallRule`	`ufw deny` or `iptables`
View open ports	`netstat -aon`	`lsof -i`, `ss -tuln`

TCP vs UDP

TCP – Transmission Control Protocol

- **Connection-Oriented:** Establishes a connection before data transfer (handshake process).
- **Reliable:** Ensures data is delivered correctly and in order.
- **Error Checking:** Includes error recovery and retransmission.
- **Flow Control:** Manages how much data is sent at a time to prevent overload.
- **Use Cases:** Web browsing (HTTP/HTTPS), email (SMTP), file transfers (FTP).

UDP – User Datagram Protocol

- **Connectionless:** Sends data without establishing a connection.
- **Unreliable:** No guarantee that data arrives or arrives in order.
- **Low Overhead:** Faster and more efficient for small or time-sensitive data.
- **No Flow Control:** Simply sends data as it is.
- **Use Cases:** Video streaming, online gaming, VoIP, DNS lookups.

TCP vs UDP

Feature	TCP	UDP
Connection	Connection-oriented	Connectionless
Reliability	Reliable (guaranteed delivery)	Unreliable (best-effort)
Speed	Slower due to overhead	Faster due to simplicity
Error Checking	Yes, with correction	Yes, but no correction
Data Order	Ensures ordered delivery	No guarantee of order
Use Cases	HTTP, FTP, Email	Streaming, DNS, Gaming

TCP vs UDP

- TCP: reliable, slower
- UDP: fast, less reliable

```
sudo nmap -sT 192.168.1.10      # TCP Scan
sudo nmap -sU 192.168.1.10      # UDP Scan
```

Firewalls

A firewall is a critical security layer that controls traffic based on rules to protect systems and networks from unauthorized access, malware, and other threats. It's one of the first lines of defense in cybersecurity.

✅ Purpose	🔍 Description
Traffic Control	Allows or blocks data packets based on rules (e.g., allow port 443 for HTTPS, block port 23 for Telnet).
Threat Prevention	Blocks malicious traffic such as viruses, worms, hackers, and unauthorized access.
Policy Enforcement	Ensures users and devices follow organization's network policies.
Monitoring and Logging	Tracks and logs network activity for auditing and troubleshooting.
Segmentation	Isolates network segments (e.g., guest vs. corporate networks) to limit exposure in case of attacks.

Firewalls

Types of Firewall

Type	Description	Example Use
Packet-Filtering Firewall	Inspects IP headers; allows/blocks based on source, destination, port.	Basic network security
Stateful Firewall	Tracks state of connections; more intelligent filtering.	Business networks
Application Layer Firewall (Proxy)	Filters based on specific applications (e.g., HTTP, FTP).	Web filtering, email security
Next-Gen Firewall (NGFW)	Includes IDS/IPS, malware scanning, deep packet inspection.	Enterprise-level protection
Host-Based Firewall	Runs on individual devices (Windows Defender Firewall).	Personal computers, endpoints
Cloud Firewall	Deployed in the cloud to protect cloud-based resources.	AWS/Azure security groups

Firewalls

Examples of Firewall Software & Tools

Platform	Example
Windows	Windows Defender Firewall
Linux	`iptables`, `ufw`, `firewalld`
Hardware/Enterprise	Fortinet, Cisco ASA, Palo Alto, pfSense, Sophos

Firewall Rules

Rule #	Action	Protocol	Port	Description
1	Allow	TCP	443	Allow HTTPS traffic
2	Allow	TCP	80	Allow HTTP traffic
3	Deny	TCP	23	Block Telnet (insecure)
4	Deny	All	All	Block everything else

VPNs

- A VPN is a secure tool that encrypts your internet connection, protects your privacy, and allows you to safely access remote or restricted content. It is widely used by both individuals and organizations to enhance security, anonymity, and freedom online

Purpose

✅ Purpose	🔍 Description
Privacy Protection	Hides your IP address and encrypts traffic to prevent ISPs, hackers, or governments from tracking your online activity.
Secure Remote Access	Allows employees to securely access internal company resources from remote locations.
Data Encryption	Encrypts all data sent over public networks (e.g., Wi-Fi), preventing interception.
Bypass Geo-Restrictions	Allows access to region-blocked content (e.g., streaming services, websites).
Avoid Censorship	Enables users in restricted countries to access open internet content.
Protect Public Wi-Fi Users	Secures your data on insecure networks like hotels, cafes, and airports.

VPNs

Components of VPN

Component	Purpose
Encryption Protocols	Secures the data (e.g., OpenVPN, IPSec, IKEv2, WireGuard).
VPN Server	Endpoint you connect to that masks your identity.
Tunnel	Encrypted connection between client and server.

Types of VPN

Type	Use Case	Example
Remote Access VPN	Individual connects to a private network remotely	Employees working from home
Site-to-Site VPN	Connects entire networks (e.g., branch offices)	Large enterprises
Client-based VPN	Requires software on the user's device	NordVPN, Cisco AnyConnect
Cloud VPN	Secure connection to cloud resources	AWS VPN, Azure VPN Gateway

VPNs

Examples of VPN Services/Software

Platform	Examples
Personal Use	NordVPN, ExpressVPN, Surfshark, ProtonVPN
Business/Enterprise	Cisco AnyConnect, Fortinet VPN, OpenVPN Access Server

DNS

DNS is a critical backbone of the internet, making web browsing human-friendly, efficient, and scalable by mapping domain names to IP addresses. It is fundamental to the operation of both small and large networks.

Purpose

✅ Purpose	🔍 Description
Name Resolution	Converts domain names into IP addresses so browsers and systems can connect to websites.
Ease of Use	Allows humans to use memorable names instead of hard-to-remember IPs.
Network Efficiency	Speeds up connections with cached DNS data.
Load Distribution	Can balance traffic among multiple servers (e.g., content delivery networks).

DNS

Components

Component	Role
DNS Resolver	Receives queries from users, performs lookup.
Root Server	First step in translation; points to TLD servers.
TLD Server	Directs queries to authoritative servers based on domain extension (.com, .org, etc.).
Authoritative Server	Holds actual IP address information for the domain.

DNS

Components

Root DNS Server

Role: The top of the DNS hierarchy. Knows where to find Top-Level Domain (TLD) servers like .com, .org, .net, .pk, etc.

Example Query: "Where do I find the .com servers?"

Response: "Go to these .com TLD servers."

There are 13 sets of root servers (A to M), each mirrored globally:

TLD (Top-Level Domain) DNS Server

Role: Manages domains under a specific extension like .com, .org, .edu, .gov, etc. Knows which authoritative server handles a specific domain like example.com.

Example Query: "Where is example.com hosted?"

Response: "Check with the authoritative server for example.com."

🔍 **Examples of TLDs:**

.com → for commercial websites

.org → for organizations

.pk → Pakistan-specific domains

.edu → educational institutions

Authoritative DNS Server

Role: This server holds the actual DNS records for the domain (like A, MX, CNAME, TXT).

Answers: "Here is the IP address for www.example.com."

Can be managed by hosting providers, CDN providers, or internal DNS servers

DNS

Bifurcation (Breakdown Summary)

Layer	Role	Example Question	Example Answer
Root DNS	Directs to TLD DNS	"Where is `.com`?"	"Here are the `.com` servers."
TLD DNS	Directs to authoritative DNS for domain	"Where is `example.com`?"	"Ask at ns1.exampledns.com"
Authoritative DNS	Final answer — gives IP address	"What is IP of `www.example.com`?"	"It's 104.18.6.183"

DHCP

A critical networking protocol that automates IP address allocation, ensuring devices can quickly and reliably connect to the network without manual setup. It's essential for modern, scalable, and mobile-friendly networks.

Purpose

✅ Purpose	🔍 Description
Automatic IP Assignment	Assigns IP addresses dynamically to devices (clients) without manual configuration.
Efficient IP Management	Avoids conflicts by tracking which IPs are in use or available.
Reduces Admin Effort	Eliminates manual setup of IP, subnet mask, DNS, etc., on every device.
Supports Mobility	Easily connects roaming or mobile devices (e.g., laptops, phones).

DHCP

How DHCP Works (Functionality)

The DHCP process is known as DORA — a 4-step sequence:

Step	Message	Description
1	**Discover**	Client broadcasts a message: "Is there any DHCP server out there?"
2	**Offer**	DHCP server replies: "I have an IP for you: 192.168.1.50."
3	**Request**	Client responds: "Yes, I'd like to use that IP, please."
4	**Acknowledgment**	Server confirms: "You're assigned 192.168.1.50 for 8 hours."

DHCP

What Does DHCP Assign?

- IP address
- Subnet mask
- Default gateway
- DNS server
- Lease duration
- Other options (e.g., NTP servers, domain name)

Importance of DHCP in a Network

Key Benefit	Explanation
Saves Time	Automatically assigns settings to thousands of devices.
Reduces Errors	Minimizes risk of IP conflicts or incorrect settings.
Scalability	Easily handles IP allocation in growing networks.
User Convenience	Devices can connect automatically (plug-and-play).

Bandwidth vs Latency

⚙️ Term	📌 Definition	🧠 Think of It As
Bandwidth	The **maximum amount of data** that can be transferred over a network in a given time. Measured in **Mbps**, **Gbps**, etc.	The **width of a highway** (how many cars can travel side-by-side)
Latency	The **time it takes** for a data packet to travel from source to destination. Measured in **milliseconds (ms)**.	The **speed limit or delay** (how long it takes to reach your destination)

Bandwidth vs Latency

Detailed Comparison

Feature	Bandwidth	Latency
What it Measures	Data **volume per second**	Data **delay or response time**
Unit	Mbps, Gbps, Kbps	ms (milliseconds)
Higher Is...	**Better** – More capacity	**Worse** – More delay
Affected By	Network infrastructure, connection type, congestion	Distance, routing, hardware, quality of links
Examples	100 Mbps fiber connection	10 ms ping to Google
Analogy	A **wider pipe** moves more water	A **faster pipe** delivers water sooner

Bandwidth vs Latency

Summary

✅ Bandwidth	✅ Latency
How **much** data can move	How **fast** data travels
Bigger is better	Smaller is better
Like a **pipe's width**	Like the **speed of flow**
Useful for downloads, video	Important for VoIP, gaming, real-time apps

Cybersecurity in TCP/IP and OSI Models

Protocol	Layer	Common Attacks
HTTP/HTTPS	Application	MITM, XSS, CSRF
DNS	Application	DNS spoofing, cache poisoning
TCP	Transport	SYN flood, session hijacking
IP	Internet	IP spoofing, packet sniffing
ARP	Data Link	ARP poisoning

Cybersecurity Threats Related to IP Addressing

- **IP Spoofing:** Attacker disguises as a trusted IP to bypass controls
- **Reconnaissance Scans:** Attackers map IP ranges to identify targets
- **Unauthorized Access:** Poor IP allocation can expose sensitive systems
- **DDoS Attacks:** Massive traffic floods to target IP addresses

How Subnetting Enhances Security

Network Isolation: Limits access between departments/segments
Containment of Breaches: Restricts lateral movement of attackers
Access Control: ACLs and firewalls based on subnet
Easier Monitoring: Log filtering and traffic analysis simplified

Best Practices

- Use private IPs internally (RFC1918 ranges)
- Enable reverse path filtering to prevent spoofing
- Monitor IP usage and subnet utilization
- Implement logging and alerts for unusual IP activity

Packet Flow

- Packet flow refers to the journey that data packets take from a source device (like your computer) to a destination (like a web server), passing through various network devices along the way.

Securing Home Networks

- Change default passwords
- Enable firewall
- Turn off unused services

Wi-Fi Security

A method to protect wireless networks from intrusions, data theft, and misuse. With proper protocols (like WPA3), strong passwords, and awareness of attack methods, you can secure your network effectively.

Purpose

✅ Purpose	🔍 Explanation
Prevent Unauthorized Access	Stop hackers or unauthorized users from joining the network.
Protect Confidential Data	Encrypt communication to prevent data leakage or spying.
Ensure Device Safety	Block malware spread over open or compromised Wi-Fi.
Limit Network Abuse	Prevent bandwidth theft and illegal activities from your IP.

Wi-Fi Security

Common Wi-fi Attacks

🧨 Attack Type	📌 Description
Evil Twin Attack	A fake Wi-Fi hotspot mimics a real one to capture user data.
Deauthentication Attack	Forces devices to disconnect, allowing attackers to capture handshake packets (used in cracking passwords).
Packet Sniffing	Attackers intercept unencrypted data using tools like Wireshark.
Password Cracking	Brute-force or dictionary attacks to guess weak Wi-Fi passwords.
Man-in-the-Middle (MITM)	Attacker intercepts and possibly alters communication between the device and the router.
Rogue Access Point	A malicious access point placed inside a network to trick users into connecting.
WPS PIN Exploit	WPS (Wi-Fi Protected Setup) can be brute-forced to gain access.

Wi-Fi Security

Wi-fi Security Protocols

Protocol	Status	Notes
WEP (Wired Equivalent Privacy)	❌ Insecure	Obsolete and easily crackable. Avoid using.
WPA (Wi-Fi Protected Access)	❌ Weak	Better than WEP, but still vulnerable.
WPA2	✅ Common	Still widely used, but susceptible to some attacks (like KRACK).
WPA3	✅ Recommended	More secure with better encryption and protection from brute-force attacks.

Wi-Fi Security

Methods to secure

🔒 Method	📌 Description
Use WPA3	Always use WPA3 or WPA2-AES for stronger encryption.
Strong Password	Use long, complex Wi-Fi passwords with uppercase, lowercase, symbols, and numbers.
Disable WPS	Turn off WPS to prevent brute-force PIN attacks.
Hide SSID (optional)	Prevent broadcasting the network name. Not bulletproof but adds obscurity.
MAC Address Filtering	Only allow specific device MAC addresses (not very strong alone).
Disable Guest Network (or isolate it)	Keep visitors on a separate, limited network.
Firewall on Router	Enable built-in firewall to block unwanted traffic.
Regular Firmware Updates	Keep router firmware updated to fix known vulnerabilities.
Limit Signal Range	Reduce the wireless signal range to cover only needed areas.

Wi-Fi Security

Wi-fi Testing Tools

Tool	Use
Aircrack-ng	Cracks WEP/WPA passwords using captured packets.
Wireshark	Packet sniffer for analyzing network traffic.
Kismet	Wireless network detector and intrusion detection.
Reaver	Brute-force WPS PINs to gain access.
Fern WiFi Cracker	GUI tool for Wi-Fi hacking and testing.

Safe Network Practices

- **Close unused ports**
- **Monitor logs**
- **Patch systems**

What we Learned Today

- Introduction to Networking
- Understand networks, devices, IPs, etc
- Practice with basic tools

Edversity.

CYBERSECURITY SPECIALIZATION PROGRAM WEEK 2 - DAY 2

Instructor: Muddassir Shafique

TA: Suleiman Taj

What will we learn Today

- What are Security Fundamentals
- What is Network Security?
- Focus on threats, scanning, defense

Cybersecurity Fundamentals

Cybersecurity is not a one-time solution but an ongoing process. Every organization, government, and individual must understand its fundamentals and adopt a proactive security culture. As cyber threats grow more complex in 2025, security must be embedded across people, processes, and technology.

Purpose

The primary goals of cyber security are:

- **Confidentiality –** Ensuring information is accessible only to authorized individuals.
- **Integrity –** Preventing unauthorized modification of data and systems.
- **Availability –** Ensuring reliable access to information and resources when needed.

These are collectively known as the CIA Triad, the foundation of cyber security.

Cybersecurity Fundamentals

Principles of Cyber Security

Confidentiality

- Only authorized individuals have access to data.
- Involves encryption, access control, and authentication.

Integrity

- Ensures that data remains accurate and unaltered.
- Involves checksums, hashing, and version control.

Availability

- Information and systems are accessible when needed.
- Protected through backup systems, redundancy, and robust network designs.

Cybersecurity Fundamentals

Principles of Cyber Security

Authentication

- Verifying the identity of users and systems.
- Common methods: Passwords, biometrics, two-factor authentication (2FA).

Authorization

- Granting users appropriate access levels based on roles.

Non-repudiation

- Ensures that a sender cannot deny having sent a message.
- Achieved through digital signatures and logs.

Accountability

- Users and systems must be traceable through logs and monitoring.

Fundamentals of Cyber Security

Network Security

Protects internal networks from intruders using firewalls, IDS/IPS, etc.

Information Security

Protects data integrity and privacy in storage and transit.

Application Security

Secures software against vulnerabilities throughout its lifecycle.

Endpoint Security

Protects individual devices like PCs, mobiles, and tablets.

Fundamentals of Cyber Security

Cloud Security

Ensures security in cloud-based infrastructures and SaaS platforms.

Identity & Access Management (IAM)

Manages who can access what resources.

Disaster Recovery & Business Continuity

Ensures quick recovery from attacks or failures.

Security Awareness Training

Educating users on recognizing phishing, using strong passwords, etc.

Modern cybersecurity requirements

Zero Trust Architecture

“Never trust, always verify” model to minimize risk across devices and users.

AI-Driven Threat Detection

Using machine learning for anomaly detection and threat intelligence.

Compliance with Regulations

Adherence to GDPR, HIPAA, NIST, ISO 27001, and local laws.

Cybersecurity in Remote Work

Securing endpoints, VPNs, and remote access tools.

Cloud-native Security Tools

Implementing CSPM, CIEM, and other modern cloud security solutions.

Modern cybersecurity requirements

Multi-Factor Authentication (MFA)

MFA is now essential, not optional, across all critical systems.

Security-as-Code & DevSecOps

Integrating security into development pipelines from the start.

Incident Response & Cyber Resilience

Rapid response frameworks and tabletop exercises to handle breaches.

Protection against Ransomware

Strong backup strategies, endpoint security, and user awareness.

What is Network Security?

Network Security refers to the policies, practices, and technologies used to protect the integrity, confidentiality, and availability of data and resources across computer networks. It ensures that the network is secure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure.

Purpose of Network Security

The main objectives of network security are:

- Protect data in transit between systems and users.
- Prevent unauthorized access to network resources.
- Ensure service availability and prevent disruptions like DDoS attacks.
- Monitor and control network traffic to detect and respond to threats in real-time.
- Support compliance with cybersecurity standards and regulations.

Principles of Network Security

Confidentiality

- Prevents unauthorized users from accessing sensitive data.
- Achieved via encryption, access control lists (ACLs), and VPNs.

Integrity

- Ensures data is not altered or tampered with in transit.
- Protected through hashing, digital signatures, and checksum methods.

Availability

- Keeps the network and services up and running, even during attacks.
- Managed through firewalls, load balancers, redundancy, and failover systems.

Authentication

- Verifies the identity of devices and users on the network.

Accountability

- Maintains logs and audits to trace actions back to individuals.

Common Threats

MITM (Man-in-the-Middle)

An attack where the attacker secretly intercepts and possibly alters the communication between two parties without their knowledge.

Sniffing

The process of capturing and reading network traffic, often to collect sensitive data like passwords or messages.

Spoofing

Faking or disguising your identity to appear as someone else, such as using a fake IP address or MAC address to gain unauthorized access.

Scanning – What Is It?

process of systematically examining a network, system, or application to identify vulnerabilities, open ports, live hosts, services, and potential security risks. It is a crucial part of the reconnaissance and assessment phase in ethical hacking, penetration testing, and network monitoring.

Purpose of Scanning

- Identify open ports and running services on devices and servers.
- Detect vulnerabilities that could be exploited by attackers.
- Map the network structure including hosts, routers, and firewalls.
- Ensure compliance with security policies and standards.
- Assist in threat modeling and risk assessment.

Scanning – What Is It?

Types of Scanning

Scanning is broadly categorized into three types:

1. Port Scanning

- Detects open, closed, or filtered ports on a system.
- Determines which services (HTTP, FTP, SSH, etc.) are running.
- **Tools:** Nmap, Netcat, Angry IP Scanner

2. Vulnerability Scanning

- Checks for known vulnerabilities, misconfigurations, and outdated software.
- Uses vulnerability databases (e.g., CVEs).
- **Tools:** Nessus, OpenVAS, Qualys, Rapid7 InsightVM

Scanning – What Is It?

Network Scanning

- Identifies active hosts and devices on a network.
- Maps the network topology and lists IP addresses, MAC addresses, etc.
- Useful for asset discovery and monitoring.

Tool Name	Type	Interface	Best For
Nmap	Port/Host Scanning	CLI/GUI	In-depth scanning, scripting
Angry IP Scanner	IP/Port Scanner	GUI	Quick, lightweight scans
Advanced IP Scanner	Device Discovery	GUI	Windows-based scanning
Netcat	Port Scanning	CLI	Manual checks, debugging
SolarWinds NPM	Enterprise Monitor	GUI	Corporate network monitoring
OpenVAS	Vulnerability Scan	GUI	Open-source vuln detection
Masscan	High-speed Scanner	CLI	Bulk IP/port scanning
Nessus	Vuln & Net Scan	GUI	Security audits
Wireshark	Packet Analyzer	GUI	Packet-level analysis
Fing	Device Scanner	GUI	Mobile-friendly network overview

Scanning – What Is It?

Ethical vs Malicious Scanning

Ethical Scanning	Malicious Scanning
Done by security professionals	Done by hackers or attackers
Requires permission	Performed illegally without consent
Aims to fix and protect systems	Aims to exploit systems

OS Fingerprinting

Process of determining the operating system (OS) of a remote host or device by analyzing characteristics of its network traffic, responses to specific probes, or open ports. It's commonly used during network reconnaissance by both ethical hackers and attackers.

Purpose of OS Fingerprinting

- Identify the operating system (e.g., Windows, Linux, macOS, iOS).
- Detect version details (e.g., Windows Server 2019, Ubuntu 22.04).
- Tailor exploits to known OS vulnerabilities.
- Help system admins ensure inventory accuracy and patch compliance.
- Improve incident response and threat modeling.

OS Fingerprinting

Methods of OS Fingerprinting

There are two main methods:

Active OS Fingerprinting

- Sends custom network packets to the target system and analyzes how it responds.
- Focuses on TCP/IP stack behavior, flags, TTL values, window sizes, etc.

Example: Nmap's OS detection (nmap -O <target>)**.**

Advantages:

- More accurate and detailed.

Disadvantages:

- Easily detected (noisy), may trigger security alerts.

OS Fingerprinting

Methods of OS Fingerprinting

Passive OS Fingerprinting

- Monitors existing network traffic without sending probes.
- Analyzes patterns in packets (TTL, DF flag, options) as they pass by.

Tools: p0f, Wireshark with OS fingerprinting plugins.

Advantages:

Stealthy and undetectable.

Disadvantages:

Less accurate if insufficient traffic is observed.

OS Fingerprinting

Tools for OS Fingerprinting

Tool	Method	Notes
Nmap	Active	Widely used, `-O` flag for OS detection
XProbe2	Active	Focuses on ICMP-based fingerprinting
p0f	Passive	Silent OS detection from live traffic
NetScanTools	Active	Windows GUI-based network scanner
Wireshark	Passive	Can analyze OS traits from packet data

OS Fingerprinting

✓ Ethical Use:	✗ Malicious Use:
Security audits.	Attackers use it to find vulnerable OS versions.
Asset management and compliance.	Enables targeted exploits or zero-day attacks.
Tailoring penetration testing.	

OS Fingerprinting

How to Defend Against OS Fingerprinting

- Use firewalls to filter and block unnecessary ports and responses.
- Enable packet normalization on IDS/IPS systems.
- Use intrusion detection systems (IDS) to detect active fingerprinting attempts.
- Implement proxy and VPN solutions to mask system details.
- Patch and update systems to minimize exploitation risks.

Vulnerability Scanning

An automated process of identifying security weaknesses, misconfigurations, and known vulnerabilities in systems, networks, applications, and devices. It is typically conducted using specialized tools that compare system details with databases of known vulnerabilities (e.g., CVEs - Common Vulnerabilities and Exposures).

Purpose of Vulnerability Scanning

- Detect exploitable flaws in systems and applications.
- Assess security posture and risk exposure.
- Support patch management by identifying outdated software or firmware.
- Help organizations comply with security standards and regulations (e.g., ISO 27001, PCI-DSS).
- Aid in penetration testing and continuous monitoring.

Vulnerability Scanning

How Vulnerability Scanning Works

- **Discovery**
  Identify active hosts, open ports, and running services.
- **Enumeration**
  Gather system details (OS version, software versions, configurations).
- **Vulnerability Matching**
  Compare identified data with known vulnerabilities (from databases like CVE, NVD, etc.).
- **Reporting**
  Generate a detailed report with risk levels (e.g., critical, high, medium, low) and remediation suggestions.

Vulnerability Scanning

Types of Vul Scanning

Type	Description	Example Use Case
Network-based	Scans devices and systems on a network for weaknesses	Checking open ports and outdated services
Host-based	Scans individual systems (workstations, servers) for internal issues	Identifying unpatched software, weak settings
Application-based	Tests web apps and software for security flaws (e.g., SQL injection)	Web app security testing
Database Scanning	Checks for misconfigured or vulnerable databases	Assessing Oracle, MySQL, or SQL Server risks
Credentialed Scan	Uses admin/user credentials for deeper insight	Internal audits with system access
Non-Credentialed Scan	Scans from the outside without logging into the system	External attack simulation

Vulnerability Scanning

Tools

Tool	Type	Notes
Nessus	Network/Host	Industry-leading scanner with deep vulnerability coverage
OpenVAS	Network/Host	Open-source alternative to Nessus
QualysGuard	Cloud-based	Scalable enterprise-grade scanning and compliance tool
Nexpose (by Rapid7)	Network/Host	Integrated with Metasploit for advanced testing
Burp Suite	Web App	Manual and automated web application scanning
Acunetix	Web App	Focused on web application vulnerabilities
Microsoft Defender for Endpoint	Host-based	Includes vulnerability scanning in Windows environments

Vulnerability Scanning

Limitations of Vulnerability Scanning

- May produce false positives or false negatives.
- Doesn’t confirm exploitable vulnerabilities (requires penetration testing).
- Needs regular updates to detect newly discovered vulnerabilities.
- Can cause minor performance impact on systems during scans.

Best Practices

- Scan regularly (e.g., weekly, monthly, after updates).
- Use credentialed scans for deeper insight.
- Prioritize remediation based on CVSS score and business risk.
- Combine with penetration testing for thorough validation.
- Maintain and update the vulnerability database.

Vulnerability Scanning

Vulnerability Scanning Report

Vulnerability Name	CVSS Score	Risk Level	Affected Asset	Description	Remediation
Apache HTTP Server XSS	7.5	High	192.168.1.10	A cross-site scripting vulnerability in Apache	Update Apache to version 2.4.54 or later
SMBv1 Enabled	5.0	Medium	192.168.1.12	Outdated protocol vulnerable to WannaCry attack	Disable SMBv1 in Windows features
OpenSSH Weak Ciphers	6.2	Medium	192.168.1.5	Server allows deprecated encryption algorithms	Update SSH config to disable weak ciphers
Outdated WordPress Version	9.8	Critical	mysite.com	Known RCE vulnerability in WP version 5.6	Update to WordPress 6.5.2

Defense: IDS/IPS

IDS (Intrusion Detection System)

A monitoring system that detects malicious or suspicious activity on a network or host but does not take direct action to stop it.

Purpose

- Detect known attack signatures (like malware, brute-force).
- Alert security teams about possible breaches.
- Help investigate and respond to threats.

Defense: IDS/IPS

Types of IDS

Type	Description
NIDS	Network-based IDS – monitors entire network traffic (e.g., Snort)
HIDS	Host-based IDS – monitors activity on individual systems (e.g., OSSEC)

Defense: IDS/IPS

IPS (Intrusion Prevention System)

An active security system that detects and blocks malicious activity in real time, often by dropping packets, resetting connections, or modifying traffic.

Purpose

- Prevent attacks by blocking harmful traffic.
- Enforce security policies.
- Act as a first line of defense against zero-day exploits and DoS attacks.

Defense: IDS/IPS

IDS vs IPS – Key Differences

Feature	IDS	IPS
Action	Detects and alerts	Detects and blocks
Position	Often passive (monitoring only)	Inline with network traffic
Latency Impact	Minimal	May introduce slight delay (inline)
Best Use Case	Post-event analysis, forensic auditing	Real-time threat prevention
Examples	Snort (IDS mode), Suricata, OSSEC	Snort (IPS mode), Suricata, Cisco Firepower

Defense: IDS/IPS

How They Work

1. Traffic enters your network.
2. IDS/IPS inspects the traffic using:
    - Signature-based detection
    - Anomaly detection
    - Behavior analysis
3. Based on rules:
    - IDS → Sends alert to admin (e.g., log or email)
    - IPS → Drops packet or blocks IP immediately

Defense: IDS/IPS

Tools

Tool	Type	Notes
Snort	IDS / IPS	Open-source, very popular
Suricata	IDS / IPS	Multi-threaded, supports deep packet inspection
OSSEC	HIDS	Host-based, great for logs and integrity checking
Zeek (Bro)	IDS	Network analysis framework, flexible scripting
Cisco Firepower	IPS	Commercial appliance with advanced threat protection

DMZ (Demilitarized Zone)

A DMZ is a perimeter network that sits between an internal network and an external network (usually the internet). It acts as a buffer zone to expose public-facing services (like websites or email servers) while keeping your internal network protected from direct access.

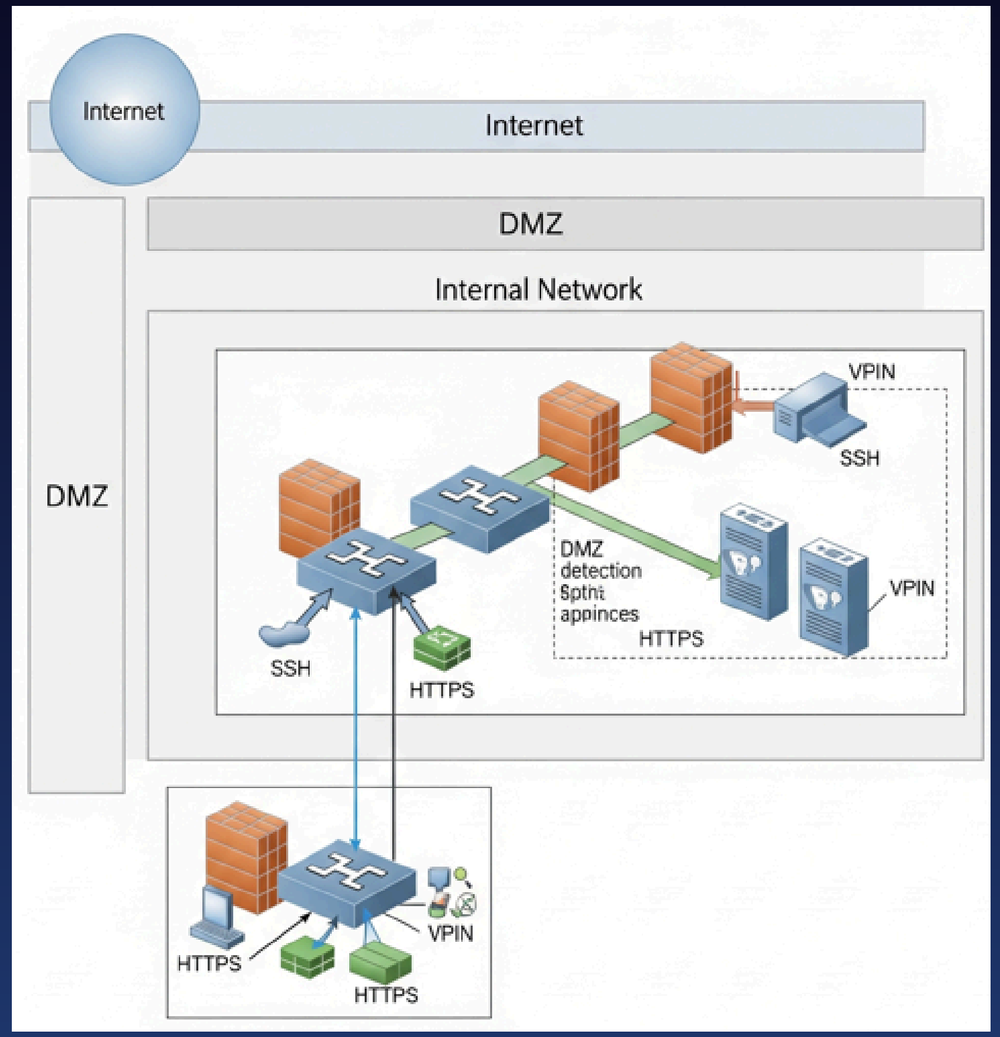
Purpose of a DMZ

Goal	Description
🎯 **Protect internal network**	Prevent direct external access to your LAN
🌐 **Host public services**	Place web, FTP, DNS, or mail servers in the DMZ to serve internet users
🧱 **Limit attack surface**	Even if a DMZ server is compromised, internal systems remain isolated
📊 **Security segmentation**	Enforces layered security (defense-in-depth strategy)

DMZ (Demilitarized Zone)

How a DMZ Works

- External users access only the DMZ services.
- Internal network is protected behind an additional firewall.
- Firewalls control what traffic is allowed into and out of the DMZ.



DMZ (Demilitarized Zone)

Which Services are Typically in DMZ?

Service	Why It's in the DMZ
Web Server	Must be accessed by the public
Mail Server	Sends/receives email from the internet
FTP Server	File transfers to/from external users
VPN Gateway	Allows secure remote access
DNS Server	Resolves domain names for internet users
Reverse Proxy	Forwards external requests to internal apps

Wireshark

- Used by SOC analysts, network engineers, ethical hackers, and forensic investigators.
- 🔍 Packet sniffing
- See every data packet sent/received on a network
- 🕵️‍♂️ Troubleshooting
- Diagnose slow networks, errors, or dropped packets
- 🔐 Security analysis
- Detect suspicious traffic or malware
- 👨‍🏫 Learning tool
- Understand how TCP/IP, DNS, HTTP, etc. work
- 💣 Attack detection
- Spot port scans, ARP spoofing, and MITM attacks

Practical

OS Fingerprinting and Reconnaissance

- nmap -O -T2 --scan-delay 100ms --max-retries 2 192.168.1.30 # OS detection via Nmap
- nmap -sV -T2 --max-retries 1 --scan-delay 100ms 192.168.1.30 # Service version detection
- nmap --script vuln --script-args vulns.showall -T2 192.168.1.30 # Vulnerability scan

Packet Filtering with iptables

- sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT # Allow HTTP
- sudo iptables -A INPUT -p tcp --dport 23 -j DROP # Block Telnet

Save rules persistently

- sudo apt install iptables-persistent
- sudo netfilter-persistent save

Practical

Host Discovery and Scanning

- nmap -sP 192.168.1.0/24 # Ping sweep to find active hosts
- nmap -sV 192.168.1.10 # Detailed service scan
- sudo arp-scan --interface=eth0 --localnet # ARP scan for local devices
- sudo tcpdump -i eth0 # Capture packets on eth0
- wireshark # GUI packet analyzer

Network Interface and IP Info

- ip a # Show IP address info
- ifconfig # Show network interfaces
- ping google.com # Test internet connectivity
- route -n # Show routing table

Practical

Manual Networking and Connection Testing

- nc -lvp 4444 # Listen on port 4444 (server)
- nc 192.168.1.10 4444 # Connect to listener (client)

- netstat -an # Show all connections
- sudo netstat -tuln # Show listening ports
- ss -tuln # Show TCP/UDP listeners

- telnet <target-ip> 8080 # Test connection on port 8080
- traceroute google.com # Show path to destination
- nslookup google.com # DNS resolution

- sudo iptables -F # Flush iptables rules
- sudo ufw reset # Reset ufw configuration

Practical

Open a Port:

Open Windows Defender Firewall with Advanced Security.

Click Inbound Rules → New Rule.

Select Port, click Next.

Choose TCP or UDP, enter the port number (e.g., 8080), click Next.

Allow the connection, apply to Domain/Private/Public, click Finish.

Close a Port:

Find the corresponding rule in Inbound Rules, right-click → Disable or Delete.

What we've learned

- Introduction to Networking
- Understand networks, devices, IPs, etc
- Practice with basic tools
- What are Security Fundamentals
- What is Network Security?
- Focus on threats, scanning, defense

Challenge: Scan & Report

🎯 **Objective:**

- Identify the target's OS and services without being detected by IDS/IPS, enumerate vulnerabilities, and prepare a detailed security assessment report.

Bonus (Extra Challenge)

- Capture packets with Wireshark during scanning to see if any IDS triggers alerts.
- Try to evade detection by modifying packet headers or fragmenting packets (using --mtu or --data-length in Nmap).
- Use tools like Metasploit auxiliary modules for OS detection and vulnerability scanning.