ISDM (INDEPENDENT SKILL DEVELOPMENT MISSION)

📌 UNDERSTANDING NETWORKS & TCP/IP PROTOCOLS

📌 CHAPTER 1: INTRODUCTION TO NETWORKING

1.1 WHAT IS NETWORKING?

NETWORKING REFERS TO THE PRACTICE OF CONNECTING MULTIPLE COMPUTING DEVICES TO SHARE DATA AND RESOURCES EFFICIENTLY. NETWORKS ENABLE **COMMUNICATION, DATA TRANSFER,** AND **RESOURCE SHARING,** ALLOWING BUSINESSES, GOVERNMENTS, AND INDIVIDUALS TO OPERATE MORE EFFECTIVELY.

KEY FEATURES OF A NETWORK:

✓ **DATA SHARING** – ENABLES MULTIPLE USERS TO ACCESS AND EXCHANGE INFORMATION.

✓ **RESOURCE SHARING** – MULTIPLE DEVICES CAN SHARE PRINTERS, STORAGE, AND SOFTWARE APPLICATIONS.

✓ **REMOTE ACCESS** – USERS CAN ACCESS FILES, APPLICATIONS, AND SYSTEMS FROM ANYWHERE IN THE WORLD.

✓ **SECURITY & MANAGEMENT** – NETWORKS PROVIDE ENCRYPTION, FIREWALLS, AND MONITORING TOOLS TO PROTECT DATA.

🖼 Diagram: Basic Network Structure

[Computer A] --- [Router] --- [Computer B]

- **Computer A & B** are network nodes.
- **Router** connects the devices to communicate efficiently.
- **Internet** allows global connectivity.

1.2 Types of Networks

Network Type	Description	Example
LAN (Local Area Network)	A small network covering a single office, school, or home.	Office Wi-Fi, home networks
MAN (Metropolitan Area Network)	Connects multiple LANs across a city or large area.	City-wide Wi-Fi, cable TV networks
WAN (Wide Area Network)	Connects multiple networks across countries and continents.	The Internet, multinational corporate networks
PAN (Personal Area Network)	A very small network that connects personal devices.	Bluetooth connections, smartwatches

🖼 Diagram: Network Types

LAN ──▶ Home Network

MAN ──▶ City-wide ISP

WAN ──▶ Global Internet

PAN ──▶ Bluetooth Earphones

📌 Example of a LAN:

A university where classrooms, libraries, and faculty offices are connected under a **single network**.

📌 Chapter 2: Network Topologies & Components

2.1 Network Topologies

Network topology refers to the **layout of devices** in a network. Different network topologies impact **performance, reliability, and scalability**.

Topology	Description	Advantages	Disadvantages
Bus	Devices are connected in a single line (backbone cable).	Simple setup, cost-effective.	If the main cable fails, the network stops.
Star	All devices connect to a central	Easy to troubleshoot, scalable.	Central hub failure disrupts the network.

	SWITCH OR HUB.		
MESH	EVERY DEVICE CONNECTS TO EVERY OTHER DEVICE.	HIGHLY RELIABLE, NO SINGLE POINT OF FAILURE.	EXPENSIVE, COMPLEX WIRING.
RING	DEVICES FORM A CLOSED LOOP.	PREDICTABLE DATA FLOW.	A SINGLE FAILURE CAN STOP THE NETWORK.

🖼 DIAGRAM: NETWORK TOPOLOGIES

BUS ──► [DEVICE]──[DEVICE]──[DEVICE]

STAR ──► [DEVICE]──[SWITCH]──[DEVICE]

RING ──► [DEVICE]──[DEVICE]──[DEVICE]

📌 EXAMPLE OF A STAR TOPOLOGY:

A **CORPORATE OFFICE** WHERE ALL COMPUTERS CONNECT TO A CENTRAL **ROUTER**.

2.2 NETWORK COMPONENTS

NETWORKS CONSIST OF VARIOUS **HARDWARE AND SOFTWARE COMPONENTS** THAT ENABLE COMMUNICATION.

✓ **ROUTER** – DIRECTS TRAFFIC BETWEEN NETWORKS.
✓ **SWITCH** – CONNECTS MULTIPLE DEVICES WITHIN A LAN.
✓ **MODEM** – CONVERTS DIGITAL SIGNALS FOR INTERNET ACCESS.

✓ **Firewall** – Protects the network from threats.

✓ **Access Point (AP)** – Provides wireless connectivity.

🖼 Diagram: Network Components

[Internet]——▶ [Modem]——▶ [Router]——▶ [Switch]——▶ [Computers]

📌 Example:

A **business network** using a **router, switch, and firewall** to ensure security and performance.

📌 Chapter 3: Understanding TCP/IP Model & OSI Model

3.1 What is TCP/IP?

The **Transmission Control Protocol/Internet Protocol (TCP/IP)** is the backbone of internet communication, ensuring **secure and reliable data transfer**.

✓ **Ensures end-to-end data transmission.**

✓ **Standardized model** used across all networks.

✓ **Works across different devices and networks.**

3.2 Layers of TCP/IP Model

TCP/IP follows a **layered approach,** breaking network functions into **four key layers**:

Layer	Function	Protocols Used

Application Layer	Handles user applications and data exchange.	HTTP, FTP, SMTP, DNS
Transport Layer	Ensures reliable communication between devices.	TCP, UDP
Internet Layer	Routes packets across networks.	IP, ICMP, ARP
Network Access Layer	Manages physical connections.	Ethernet, Wi-Fi

🖼 Diagram: TCP/IP Model

Application ⟶ Web Services

Transport ⟶ Reliable Delivery

Internet ⟶ Routing

Network Access ⟶ Hardware Communication

📌 Example:

When sending an email, **SMTP (Application Layer)** formats the message, **TCP (Transport Layer)** ensures delivery, and **IP (Internet Layer)** routes it.

📌 Chapter 4: TCP & UDP – Transport Layer Protocols

4.1 Transmission Control Protocol (TCP)

TCP PROVIDES **RELIABLE, CONNECTION-ORIENTED** COMMUNICATION.

✓ USES A **THREE-WAY HANDSHAKE** (SYN, SYN-ACK, ACK).
✓ ENSURES **DATA IS DELIVERED IN ORDER**.
✓ USED IN **WEB BROWSING, EMAIL, AND FILE TRANSFERS**.

📌 **EXAMPLE:**
A **WEBPAGE DOWNLOAD** USING TCP ENSURES ALL PACKETS ARRIVE CORRECTLY.

4.2 USER DATAGRAM PROTOCOL (UDP)

UDP IS **FASTER BUT LESS RELIABLE** THAN TCP.

✓ **NO CONNECTION SETUP** – DATA IS SENT IMMEDIATELY.
✓ **NO ERROR CHECKING,** SO LOST PACKETS ARE NOT RETRANSMITTED.
✓ USED IN **LIVE STREAMING, GAMING, AND VOIP CALLS**.

📌 **EXAMPLE:**
A **VIDEO CALL** USING UDP CONTINUES EVEN IF SOME PACKETS ARE LOST.

📌 CHAPTER 5: IP ADDRESSING & SUBNETTING

5.1 IP ADDRESSING

AN **IP ADDRESS** IS A UNIQUE IDENTIFIER ASSIGNED TO A DEVICE ON A NETWORK.

TYPE	DESCRIPTION	EXAMPLE

IPv4	32-BIT ADDRESS	192.168.1.1
IPv6	128-BIT ADDRESS	2001:DB8::FF00:42:8329

🖼 DIAGRAM: IPV4 VS IPV6

IPV4 ⟶ 192.168.1.1

IPV6 ⟶ 2001:DB8::FF00:42:8329

📌 **EXAMPLE:**

YOUR **HOME ROUTER ASSIGNS IP ADDRESSES** TO CONNECTED DEVICES.

5.2 SUBNETTING

SUBNETTING DIVIDES A LARGE NETWORK INTO **SMALLER SECTIONS**.

✓ **REDUCES CONGESTION** AND IMPROVES EFFICIENCY.

✓ USED IN **CORPORATE NETWORKS AND DATA CENTERS**.

📌 **EXAMPLE:**

A COMPANY USING 192.168.1.0/24 DIVIDES IT INTO **TWO DEPARTMENTS**.

📌 CHAPTER 6: NETWORK SECURITY

✓ **FIREWALLS** – BLOCK UNAUTHORIZED ACCESS.

✓ **ENCRYPTION** – SECURES DATA USING HTTPS AND VPNS.

✓ **STRONG PASSWORDS** – PREVENTS BRUTE-FORCE ATTACKS.

📌 **EXAMPLE:**

BANKS USE **SSL ENCRYPTION** TO SECURE ONLINE TRANSACTIONS.

📌 Chapter 7: Exercises & Practical Tasks

📌 Exercise:

1. **Explain the difference between TCP and UDP.**
2. **Describe how subnetting improves network efficiency.**
3. **How does a firewall protect a network?**

📌 Network Scanning & Reconnaissance Techniques

📌 Chapter 1: Introduction to Network Scanning & Reconnaissance

1.1 What is Network Scanning?

Network scanning is a technique used to discover active hosts, open ports, and services running on a network. It is commonly used by:

✓ **Ethical hackers** – To identify vulnerabilities before attackers exploit them.
✓ **System administrators** – To monitor and manage network security.
✓ **Cybercriminals** – To gather information for launching attacks.

🖼 Diagram: Network Scanning Process

[Attacker] ──► [Network] ──► [Host Discovery] ──► [Port Scanning] ──► [Service Enumeration]

📌 Real-World Example:

A **penetration tester** uses network scanning to check **which devices and services** are running on a corporate network to identify security weaknesses.

1.2 What is Reconnaissance?

RECONNAISSANCE IS THE **FIRST PHASE OF CYBER ATTACKS,** WHERE AN ATTACKER GATHERS INFORMATION ABOUT A TARGET NETWORK BEFORE LAUNCHING AN ATTACK.

✓ **PASSIVE RECONNAISSANCE** – GATHERING INFORMATION **WITHOUT DIRECTLY INTERACTING** WITH THE TARGET.
✓ **ACTIVE RECONNAISSANCE** – ACTIVELY ENGAGING WITH THE TARGET TO OBTAIN MORE DETAILS.

📌 **EXAMPLE:**

- **PASSIVE RECONNAISSANCE:** SEARCHING FOR COMPANY IP ADDRESSES AND EMAILS ON **GOOGLE, LINKEDIN, AND WHOIS DATABASES**.
- **ACTIVE RECONNAISSANCE:** USING **NMAP OR SHODAN** TO SCAN A TARGET NETWORK FOR OPEN PORTS.

📌 CHAPTER 2: TYPES OF NETWORK SCANNING TECHNIQUES

NETWORK SCANNING IS BROADLY CATEGORIZED INTO DIFFERENT TECHNIQUES DEPENDING ON THE **DEPTH AND INTENT** OF THE SCAN.

TYPE OF SCAN	PURPOSE	EXAMPLE TOOLS
HOST DISCOVERY (PING SWEEP)	IDENTIFIES LIVE DEVICES ON A NETWORK.	NMAP, ANGRY IP SCANNER
PORT SCANNING	CHECKS FOR OPEN PORTS ON A SYSTEM.	NMAP, NETCAT

Service & Version Detection	Identifies running services and software versions.	Nmap, Netcat
Operating System Detection	Determines the OS running on a host.	Nmap, Xprobe2
Vulnerability Scanning	Finds security weaknesses in systems.	Nessus, OpenVAS

2.1 Host Discovery (Ping Sweep)

Host discovery, also known as **ping sweeping,** is used to determine which devices are **active** on a network.

Methods of Host Discovery:

✓ **ICMP Ping** – Sends an ICMP Echo Request to check if a device responds.
✓ **ARP Scan** – Used in **local networks** to detect devices even if ICMP is blocked.
✓ **Traceroute** – Identifies network paths between the source and target.

🖼 Diagram: Host Discovery Process

[Scanner] ──► [Network] ──► [Response Received?] ──► [Active Host]

📌 Example:

nmap -sn 192.168.1.0/24

This command checks **which hosts are online** in a local network.

2.2 Port Scanning

Port scanning identifies **open ports** on a target system to determine which network services are accessible.

Common Port Scanning Techniques:

✓ **TCP Connect Scan (-sT)** – Establishes a full connection with the target.
✓ **SYN Scan (-sS)** – Sends a **half-open** connection request (stealth scan).
✓ **UDP Scan (-sU)** – Detects open UDP ports (used for VoIP, DNS, etc.).
✓ **Idle Scan (-sI)** – Hides the attacker's identity by spoofing another host.

📌 **Example:**

```
nmap -sS -p 22,80,443 192.168.1.10
```

This scans **ports 22, 80, and 443** on the target.

🖼 **Diagram: TCP SYN Scan**

[Attacker] ——▶ [SYN Packet] ——▶ [Target]

[Target] ——▶ [SYN-ACK Response] ——▶ [Attacker]

[Attacker] ——▶ [RST (Scan Complete)] ——▶ [Target]

✓ **If SYN-ACK is received,** the port is **open**.
✓ **If RST is received,** the port is **closed**.

2.3 Service & Version Detection

Service scanning determines **what software is running** on open ports.

📌 **Example:**

nmap -sV 192.168.1.10

✓ Detects **Apache, SSH, MySQL,** and other running services.

🖼 **Diagram: Service Enumeration Process**

[Attacker] ──► [Service Request] ──► [Target Server] ──► [Response: Apache 2.4.41]

📌 **Real-World Scenario:**

A hacker scans a **banking website** to see **which versions of software** are running to find potential vulnerabilities.

📌 Chapter 3: Reconnaissance Techniques

3.1 Passive Reconnaissance Techniques

Passive reconnaissance does **not** involve direct interaction with the target.

✓ **Google Dorking** – Using **Google Search Operators** to find sensitive information.

✓ **Whois Lookup** – Checking domain information (e.g., owner, IP address, nameservers).

✓ **Social Media Scraping** – Gathering company data from **LinkedIn, Facebook, and Twitter**.

✓ **Shodan Search** – Scanning the internet for **publicly exposed devices**.

📌 Example of Google Dorking:

site:example.com filetype:pdf "confidential"

This searches for **confidential PDFs** on a website.

3.2 Active Reconnaissance Techniques

Active reconnaissance **interacts directly** with the target to extract information.

✓ **Port Scanning** – Scanning for **open ports** on a target system.
✓ **DNS Enumeration** – Extracting **subdomains and DNS records**.
✓ **Brute-Force Attacks** – Trying multiple credentials to **gain access**.
✓ **Email Harvesting** – Collecting email addresses from websites.

📌 Example of DNS Enumeration:

nslookup -query=ANY example.com

This retrieves **DNS records** of a target domain.

📌 Chapter 4: Tools Used in Network Scanning & Reconnaissance

Tool	Purpose	Common Usage
Nmap	Port scanning, host discovery	Finding open ports and services

Wireshark	Packet analysis	Monitoring network traffic
Shodan	Internet-wide scanning	Finding exposed IoT devices
Metasploit	Exploit development	Testing network security
Nessus	Vulnerability scanning	Detecting security flaws

📌 **Example:**

A **security analyst** uses **Nmap** to scan an organization's **firewall settings** before an internal audit.

📌 Chapter 5: Preventing Network Scanning & Reconnaissance Attacks

5.1 How to Defend Against Network Scanning?

✓ **Use Firewalls** – Block unauthorized scanning attempts.
✓ **Disable Unnecessary Services** – Reduce attack surfaces.
✓ **Enable Intrusion Detection Systems (IDS)** – Detects suspicious activities.
✓ **Use Network Address Translation (NAT)** – Hides internal IPs from attackers.

📌 **Example:**

A **company firewall** blocks all **external traffic on non-essential ports** to prevent unauthorized scans.

📌 Chapter 6: Conclusion & Exercises

6.1 Summary of Key Takeaways

✅ **Network scanning** helps identify active devices and security vulnerabilities.

✅ **Reconnaissance techniques** include both **passive and active methods**.

✅ **Nmap, Wireshark, and Shodan** are commonly used tools for scanning.

✅ **Firewalls and intrusion detection systems** help prevent unauthorized scanning.

📌 6.2 Exercise Questions:

1. **What is the difference between passive and active reconnaissance?**
2. **How does a SYN scan work?**
3. **What steps can organizations take to prevent unauthorized network scanning?**

Firewalls & Intrusion Detection Systems (IDS/IPS) – In-Depth Study Material

📌 Chapter 1: Introduction to Network Security

1.1 What is Network Security?

Network security is the practice of protecting digital communication systems, network devices, and data from unauthorized access, attacks, and threats. It involves implementing policies, hardware devices, and software solutions to **safeguard data integrity, confidentiality, and availability**.

Why is Network Security Important?

- Prevents **data breaches** and cyberattacks.
- Ensures **business continuity** by protecting critical infrastructure.
- Complies with **legal and regulatory requirements** (e.g., GDPR, ISO 27001).
- Protects sensitive **personal and corporate data** from being compromised.
- Reduces risks of **financial losses** due to cybercrimes.

🖼️ Diagram: CIA Triad (Confidentiality, Integrity, Availability)

Confidentiality

▲

Integrity ◄► Availability

Common Network Threats

Threat Type	Description
Malware	Viruses, worms, ransomware that harm systems.
Phishing	Deceptive emails/messages to steal sensitive information.
DoS/DDoS Attacks	Overloading a system with excessive traffic to disrupt services.
Man-in-the-Middle (MITM) Attack	Intercepting and altering communications between two parties.
SQL Injection	Injecting malicious SQL queries to manipulate databases.

📌 Example of Network Security in Action

- **Banks** implement multi-layered firewalls to **prevent unauthorized access** to their systems.
- **Government agencies** deploy **Intrusion Detection Systems (IDS)** to **monitor cyber threats**.

- **Corporations** use **Intrusion Prevention Systems (IPS)** to **automatically block malicious attacks**.

📌 Chapter 2: Understanding Firewalls

2.1 What is a Firewall?

A **firewall** is a network security system designed to **monitor, filter, and control** incoming and outgoing network traffic based on security rules. It serves as the **first line of defense** against cyber threats by allowing legitimate traffic and blocking unauthorized access.

🖼️ Diagram: How a Firewall Works

Internet ---> Firewall ---> Internal Network

(Blocks Unauthorized Traffic)

Functions of a Firewall

✓ **Traffic Filtering:** Blocks malicious or suspicious data packets.
✓ **Access Control:** Restricts unauthorized users from accessing sensitive systems.
✓ **Monitoring & Logging:** Tracks network activities for security audits.
✓ **Protection Against Threats:** Prevents **malware, phishing, and DDoS** attacks.
✓ **Prevents Data Exfiltration:** Stops confidential data from being stolen or leaked.

📌 Example of Firewall Usage

- **An enterprise configures a firewall** to restrict employee access to **non-work-related websites**.
- **A cloud provider uses firewalls** to prevent **malware from spreading across virtual networks**.

2.2 Types of Firewalls

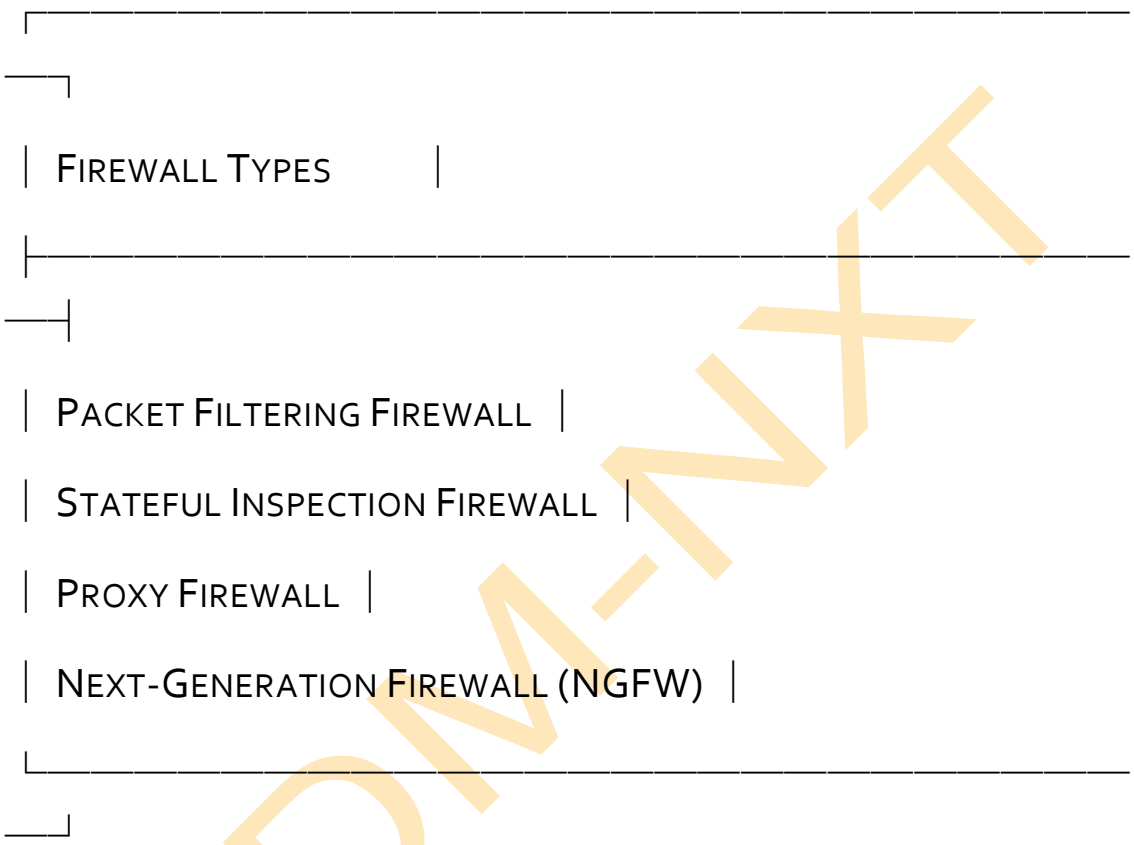
Firewalls can be classified based on **deployment location** and **traffic filtering techniques**.

Types of Firewalls

Firewall Type	Description	Example Use Case
Packet Filtering Firewall	Filters network packets based on predefined rules (IP, port, protocol).	Small businesses, routers.
Stateful Inspection Firewall	Monitors active connections and makes filtering decisions.	Enterprise security solutions.
Proxy Firewall	Acts as an intermediary between users and the internet, ensuring secure web access.	Web filtering in organizations.
Next-Generation Firewall (NGFW)	Combines traditional firewall functions with deep packet inspection (DPI), intrusion	Large enterprises, cloud environments.

	PREVENTION, AND APPLICATION-LEVEL FILTERING.	

🖼️ DIAGRAM: TYPES OF FIREWALLS



✓ CHOOSING THE RIGHT FIREWALL

- **FOR ENTERPRISES** → **NGFWS** PROVIDE ADVANCED SECURITY FEATURES.
- **FOR HOME USERS** → SOFTWARE-BASED **FIREWALLS** (WINDOWS DEFENDER, MACOS FIREWALL) OFFER PROTECTION.
- **FOR CLOUD ENVIRONMENTS** → **VIRTUAL FIREWALLS** LIKE AWS SECURITY GROUPS ENSURE **SECURE CLOUD ACCESS**.

📌 Example of Next-Generation Firewall (NGFW) Usage

- **Cisco ASA and Palo Alto NGFWs** are deployed in **corporate networks** to prevent cyberattacks.

📌 Chapter 3: Intrusion Detection Systems (IDS)

3.1 What is an IDS?

An **Intrusion Detection System (IDS)** is a security solution that **monitors network or system activities** for malicious activities, potential intrusions, or policy violations. Unlike firewalls, which **prevent** unauthorized access, IDS detects threats **after they occur**.

🖼️ Diagram: How an IDS Works

Internet ---> IDS ---> Alert System

(Monitors & Reports Threats)

✓ Functions of IDS

- **Monitors network traffic** for suspicious behavior.
- **Detects cyber threats** (e.g., malware, brute-force attacks).
- **Generates security alerts** for incident response teams.
- **Logs attack attempts** for forensic investigations.

📌 Example of IDS Usage

- **A financial institution deploys Snort IDS** to detect and analyze cyber threats targeting **customer transactions**.
- **A government agency uses IDS logs** to **trace cybercriminal activities**.

3.2 Types of IDS

IDS is classified based on **monitoring approach** and **deployment strategy**.

📌 Types of IDS

IDS Type	Description	Example
Network-Based IDS (NIDS)	Monitors traffic across an entire network segment.	Snort, Suricata.
Host-Based IDS (HIDS)	Runs on individual systems and monitors OS activities.	OSSEC, Tripwire.
Signature-Based IDS	Detects attacks using known attack signatures.	Antivirus engines.
Anomaly-Based IDS	Uses AI to detect deviations from normal behavior.	Machine learning-based security tools.

✓ Choosing the Right IDS

- **For large networks** → NIDS is preferable.

- **For endpoint security** → HIDS provides deeper system insights.

📌 Example of Anomaly-Based IDS Usage

- AI-powered **Zeek IDS** detects **zero-day attacks** in cloud environments.

📌 Chapter 4: Intrusion Prevention Systems (IPS)

4.1 What is an IPS?

An **Intrusion Prevention System (IPS)** is an advanced security solution that **not only detects but also blocks malicious traffic** in real-time.

🖼️ Diagram: How an IPS Works

Internet ---> IPS ---> Internal Network

(Detects & Blocks Threats)

✓ Functions of IPS

- **Automatically blocks cyber threats** before they cause harm.
- **Prevents Denial-of-Service (DoS) attacks.**
- **Stops malware infections** before they spread.

📌 Example of IPS Usage

- **An e-commerce website** deploys **Suricata IPS** to prevent cyberattacks on customer transactions.

📌 Chapter 5: IDS vs. IPS – Key Differences

Feature	IDS (Intrusion Detection)	IPS (Intrusion Prevention)
Function	Detects threats	Detects & blocks threats
Response	Generates alerts	Blocks malicious traffic
Deployment	Passive monitoring	Active defense mechanism

📌 Chapter 6: Best Practices for Implementing Firewalls & IDS/IPS

✓ Configure **strict access control rules** for firewalls.

✓ Use **AI-powered IDS/IPS** to detect zero-day threats.

✓ Conduct **regular security audits** to enhance defense.

📌 Chapter 7: Summary

✅ Firewalls **block unauthorized access**.

✅ IDS **detects attacks,** while IPS **prevents them**.

✅ Proper security implementation **mitigates cyber threats**.

📌 Chapter 8: Next Steps

- Learn **firewall configurations** (Cisco ASA, Palo Alto).
- Explore **IDS/IPS tools** (Snort, Zeek, Suricata).
- Get **certified** (CEH, CISSP, CompTIA Security+).

Wi-Fi Security & Wireless Hacking Techniques

📌 Chapter 1: Introduction to Wi-Fi Security

1.1 What is Wi-Fi Security?

Wi-Fi security refers to the **protection of wireless networks from unauthorized access, hacking attempts, and data interception**. Unlike wired networks, where physical access is required to connect, wireless networks transmit data through radio signals, making them vulnerable to cyber attacks.

Wireless networks are used everywhere, from **homes and offices** to **public hotspots in airports, coffee shops, and hotels**. Attackers often target these networks due to their **accessibility and lack of strong security configurations**.

1.2 Why is Wi-Fi Security Important?

🚨 Real-World Example: Public Wi-Fi Risks

- When you **connect to public Wi-Fi** at a coffee shop or airport, you may unknowingly expose your data to cybercriminals.
- Attackers can launch **Man-in-the-Middle (MITM) attacks** to intercept your credentials and banking details.
- Hackers create **fake Wi-Fi hotspots** to trick users into connecting, allowing them to steal passwords, credit card numbers, and personal information.

🔍 Common Wi-Fi Security Threats

Threat	Description
Weak Passwords	Simple passwords make it easy for hackers to guess and gain access.
Rogue Access Points	Fake Wi-Fi networks trick users into connecting, leading to data theft.
Packet Sniffing	Hackers use tools to capture and read network traffic.
Deauthentication Attacks	Forces devices to disconnect and reconnect to a malicious access point controlled by hackers.

📌 Chapter 2: Understanding Wireless Encryption Standards

2.1 Types of Wi-Fi Security Protocols

Wi-Fi security relies on **encryption protocols** that scramble data, making it unreadable to unauthorized users. Over the years, several encryption standards have been developed, some of which are now obsolete due to security flaws.

🖼️ Diagram: Evolution of Wi-Fi Security Protocols

Wi-Fi Security Protocols

├── WEP (1999) – Weak, easily hackable

├── WPA (2003) – Improved, but still vulnerable

├── WPA2 (2004) – Stronger encryption, widely used

└—— WPA3 (2018) – Most secure, resistant to brute-force attacks

📌 Comparison of Wi-Fi Security Protocols

Protocol	Encryption Algorithm	Security Level
WEP (Wired Equivalent Privacy)	RC4	Weak (Easily broken in minutes)
WPA (Wi-Fi Protected Access)	TKIP	Medium (Still vulnerable to attacks)
WPA2 (Wi-Fi Protected Access 2)	AES-CCMP	Strong (Used in most networks today)
WPA3 (Wi-Fi Protected Access 3)	AES-GCMP	Very Strong (Resistant to brute-force attacks)

✓ **Best Practice:** Always use **WPA2 or WPA3** encryption for maximum security. Avoid **WEP and WPA** as they are outdated and easily hacked.

📌 Chapter 3: Common Wireless Hacking Techniques

3.1 Packet Sniffing (Eavesdropping)

Packet sniffing is a technique used by hackers to **capture and analyze unencrypted network traffic**. Attackers can intercept

sensitive data such as login credentials, emails, and credit card details if the network lacks encryption.

📌 Tools Used for Packet Sniffing

- **Wireshark** – Captures and analyzes network packets.
- **tcpdump** – Command-line tool for traffic analysis.
- **Kismet** – Wireless network detection and monitoring tool.

🖼️ Diagram: How Packet Sniffing Works

1. Attacker connects to an open Wi-Fi network.
2. Uses Wireshark to capture unencrypted traffic.
3. Extracts login credentials and personal data.

✓ Defense Mechanisms:

- Use **HTTPS websites** to encrypt sensitive data.
- Enable **VPN** to secure your traffic.
- Ensure **Wi-Fi networks use WPA2/WPA3 encryption**.

3.2 Deauthentication Attacks

A **deauthentication attack** forcibly disconnects users from a Wi-Fi network, tricking them into reconnecting to a malicious access point.

📌 Tools Used for Deauthentication Attacks

- **aireplay-ng** – Sends deauthentication packets to force devices offline.

- **mdk3** – Performs mass deauthentication attacks on multiple devices.

🖼️ Diagram: How Deauthentication Attacks Work

1. Attacker sends deauthentication packets to a Wi-Fi network.
2. Victim's device disconnects.
3. Victim reconnects to a fake network controlled by the hacker.

✓ Defense Mechanisms:

- Use **MAC address filtering** to restrict access.
- Enable **Intrusion Detection Systems (IDS)** to detect attacks.
- Implement **802.11w Management Frame Protection (MFP)** to prevent deauth attacks.

3.3 Evil Twin Attack

An **Evil Twin Attack** is when an attacker creates a **fake Wi-Fi network** with the same name as a legitimate one to trick users into connecting.

📌 Tools Used for Evil Twin Attacks

- **airbase-ng** – Creates fake access points.
- **Wireshark** – Captures victim traffic.
- **SSLStrip** – Downgrades HTTPS to HTTP to steal data.

✓ Defense Mechanisms:

- Always **verify the legitimacy** of a Wi-Fi network before connecting.
- Use a **VPN** to encrypt all traffic.
- Disable **auto-connect** to open networks.

📌 Chapter 4: Advanced Wireless Security Measures

4.1 Implementing MAC Address Filtering

- Restricts Wi-Fi access to specific device MAC addresses.
- Prevents unauthorized devices from connecting.

4.2 Using VPN for Secure Browsing

- Encrypts internet traffic, **preventing sniffing attacks**.
- Protects against **Evil Twin Attacks**.

4.3 Enabling WPA3 Security

- **Prevents offline password cracking**.
- Uses **Simultaneous Authentication of Equals (SAE)** to enhance security.

📌 Chapter 5: Case Study – KRACK Attack on WPA2 (2017)

📌 Attack Overview

- The **Key Reinstallation Attack (KRACK)** exploited a flaw in WPA2, allowing hackers to **decrypt Wi-Fi traffic**.

📌 Impact

- Millions of **routers, smartphones, and IoT devices were vulnerable**.
- Hackers could intercept sensitive information such as **passwords and credit card details**.

✓ **Lessons Learned:**

- Always **update router firmware** to patch vulnerabilities.
- Use **WPA3 encryption** to prevent future exploits.

📌 Chapter 6: Summary

✅ Key Takeaways

- **Wi-Fi security is crucial** to prevent cyber attacks and data theft.
- Always use **WPA2 or WPA3 encryption**.
- **Packet sniffing, deauthentication, and Evil Twin attacks** are common hacking techniques.
- **Strong passwords, VPNs, and MAC filtering** enhance wireless security.
- **KRACK exploit demonstrated the importance of keeping Wi-Fi security up to date**.

📌 Chapter 7: Next Steps

- **Experiment with penetration testing tools** like Aircrack-ng.
- **Stay updated on wireless security vulnerabilities**.
- **Explore advanced topics** like wireless penetration testing and network forensics.

ASSIGNMENT: IMPLEMENTING NETWORK SECURITY

TASK: SET UP A FIREWALL AND INTRUSION DETECTION SYSTEM (IDS) ON A VIRTUAL NETWORK.

OBJECTIVE: LEARN TO CONFIGURE NETWORK SECURITY TOOLS AND BLOCK CYBER THREATS.

📝 Assignment: Implementing Network Security

📌 Task: Set up a Firewall and Intrusion Detection System (IDS) on a Virtual Network

📌 Objective: Learn to configure network security tools and block cyber threats

---

📌 Step 1: Setting Up a Virtual Network

Before configuring network security tools, you need a **virtual network environment** where you can test firewall and IDS configurations.

1.1 Install Virtualization Software

Choose one of the following:

- **VirtualBox** (Free, Open-source)
- **VMware Workstation** (Paid, Advanced Features)

📌 Steps to Install VirtualBox

1. Download VirtualBox from here.
2. Install the software and add the "VirtualBox Extension Pack" for better network support.

1.2 Create Virtual Machines

Set up at least **two virtual machines**:

- **VM1: Security System** (Linux-based, running the firewall and IDS)
- **VM2: Attacker Machine** (Kali Linux for testing the security configuration)

✓ **Recommended OS:**

- **Ubuntu 22.04 LTS** (Lightweight and stable)
- **Kali Linux** (For penetration testing)

1.3 Configure Network Settings

To simulate real network environments, configure **Host-Only Adapter or Internal Network** in VirtualBox to isolate VMs.

📌 **How to Configure a Host-Only Network:**

1. Open VirtualBox → **File** → **Host Network Manager**.
2. Click **Create** → Assign an IP range (e.g., 192.168.1.1/24).
3. Assign each VM an IP within this range.

📌 Step 2: Installing and Configuring a Firewall (UFW)

A **firewall** is the first line of defense, filtering traffic and blocking unauthorized access.

2.1 Install UFW (Uncomplicated Firewall) on Ubuntu

1. Open the terminal and install UFW:

2. sudo apt update && sudo apt install ufw -y
3. Check the firewall status:
4. sudo ufw status
5. Enable the firewall:
6. sudo ufw enable

✓ **Default Rules:**

- **Allow SSH (Port 22)** to allow remote access:
- sudo ufw allow ssh
- **Allow HTTP/HTTPS (Ports 80 & 443)** for web traffic:
- sudo ufw allow 80
- sudo ufw allow 443
- **Block all incoming traffic except allowed rules**:
- sudo ufw default deny incoming
- sudo ufw default allow outgoing

4. **Verify firewall rules:**
5. sudo ufw status verbose

📌 Step 3: Installing an Intrusion Detection System (IDS)

An **IDS** monitors network traffic for suspicious activity and generates alerts.

3.1 Install Snort (Network-based IDS)

📌 Steps to Install Snort on Ubuntu:

1. Update system and install Snort:
2. sudo apt update && sudo apt install snort -y
3. Verify installation:
4. snort -V

3.2 Configure Snort

1. **Edit Snort Configuration File**:
2. sudo nano /etc/snort/snort.conf
3. **Set network variables** (Modify this section):
4. var HOME_NET 192.168.1.0/24
5. var EXTERNAL_NET any
6. **Enable Rules:** Uncomment or add basic rules in /etc/snort/rules/local.rules:
7. alert icmp any any -> $HOME_NET any (msg:"ICMP Ping detected"; sid:1000001; rev:1;)
8. **Run Snort in live mode**:
9. sudo snort -A console -q -c /etc/snort/snort.conf -i etho

📌 Step 4: Testing the Firewall and IDS

4.1 Testing Firewall Rules

On **VM2 (Attacker Machine)**:

1. Try to SSH into **VM1 (Security System)**:
2. ssh user@192.168.1.100

- If blocked: **Firewall is working.**
- If allowed: **Check UFW rules.**

3. Try to send pings:
4. ping 192.168.1.100
    - If blocked: **Firewall is configured correctly.**
    - If allowed: **Add a UFW rule to block ICMP**:
    - sudo ufw deny icmp

4.2 Testing IDS (Snort)

On **VM2 (Attacker Machine)**:

1. Run a simulated ping attack:
2. ping -c 5 192.168.1.100
3. On **VM1 (Security System),** check Snort alerts:
4. sudo tail -f /var/log/snort/alert
    - If an alert appears**, Snort is detecting attacks** successfully.
    - If no alerts appear**, check Snort configuration**.

📌 Step 5: Advanced Firewall & IDS Configurations

5.1 Block Specific IPs with UFW

If an attacker's IP is known, block it:

sudo ufw deny from 192.168.1.50

5.2 Configure Snort to Detect Brute Force Attacks

1. Open Snort's local rules file:
2. sudo nano /etc/snort/rules/local.rules
3. Add a rule to detect multiple SSH attempts:
4. alert tcp any any -> $HOME_NET 22 (msg:"Possible SSH Brute Force"; flags:S; threshold:type both, track by_src, count 5, seconds 60; sid:1000002; rev:1;)
5. Restart Snort:
6. sudo systemctl restart snort
7. **Test with multiple SSH login attempts** from VM2 to VM1.

📌 Step 6: Monitoring and Logging

6.1 Check Firewall Logs

View blocked connection attempts:

sudo journalctl -u ufw --since today

6.2 Monitor IDS Alerts

View latest Snort logs:

sudo tail -f /var/log/snort/alert

📌 Conclusion

✅ What You Learned

- How to **set up a firewall** with UFW to block unauthorized access.

- How to **install and configure Snort IDS** to detect cyber threats.
- How to **test security measures** using an attacker machine.
- How to **monitor network logs** and take security actions.

🚀 Next Steps

- Experiment with **advanced firewall rules** (blocking ports, rate limiting).
- Explore **other IDS tools like Suricata**.
- Set up a **Web Application Firewall (WAF)** for securing websites.