
WEEK 1 – DAY 2

NETWORKING FOR SECURITY

(Ultra-Detailed, Easy-to-Explain Notes)

---

1. Why Networking Is Important for Security

Cyber attacks **travel through networks**.

If you do not understand:

- how data moves
- where data flows
- what normal traffic looks like

👉 you **cannot protect systems properly**.

Security professionals must understand **network behavior** to:

- detect attacks
- block malicious traffic
- investigate incidents

---

2. TCP/IP Model (Foundation of Networking)

The **TCP/IP model** explains **how data travels from one computer to another**.

TCP/IP has 4 layers:

1. **Application Layer**
2. **Transport Layer**
3. **Internet Layer**
4. **Network Access Layer**

2.1 Application Layer (What Users See)

This layer handles **user-level communication**.

Examples:

- HTTP / HTTPS → websites
- DNS → domain name lookup
- FTP → file transfer

- SMTP → email

Security View:

- Most attacks target this layer
- Web attacks, phishing, API abuse happen here

2.2 Transport Layer (How Data Is Delivered)

Controls **how data is sent**.

Two Main Protocols:

TCP (Transmission Control Protocol)

- Reliable
- Ensures data arrives correctly
- Uses **3-way handshake**

Used by:

- HTTP/HTTPS
- Email
- File transfers

UDP (User Datagram Protocol)

- Faster but unreliable
- No guarantee of delivery

Used by:

- DNS
- Streaming
- VoIP

Security View:

- UDP is easier to abuse for **DDoS attacks**

2.3 Internet Layer (IP Addressing)

Handles **routing data** between networks.

Protocol:

- IP (Internet Protocol)

Security View:

- IP spoofing
- Network scanning
- Routing attacks

2.4 Network Access Layer (Physical Transmission)

Handles:

- Ethernet
- Wi-Fi
- MAC addresses

Security View:

- ARP spoofing
- Man-in-the-Middle attacks

---

3. DNS (Domain Name System)

Simple Meaning:

DNS converts **domain names** into **IP addresses**.

Example:

google.com → 142.250.xxx.xxx

DNS Process (Step-by-Step)

1. User types a website name
2. Browser asks DNS server
3. DNS server replies with IP address
4. Browser connects to that IP

Security Risks in DNS

- DNS spoofing
- DNS cache poisoning
- Phishing attacks

Security Controls

- DNSSEC
- Secure resolvers
- Monitoring DNS logs

---

4. HTTP vs HTTPS (Very Important)

HTTP (Insecure)

- Data is sent in **plain text**
- Attackers can read credentials

HTTPS (Secure)

- Uses **TLS encryption**
- Data is encrypted
- Prevents eavesdropping

Interview Line

“HTTPS ensures confidentiality and integrity of data in transit using TLS.”

---

5. Ports and Protocols

What Is a Port?

A port identifies **which service** on a computer is communicating.

Think of:

- IP address → building address
- Port → apartment number

Common Ports

Port	Service
80	HTTP

Port	Service
443	HTTPS
22	SSH
21	FTP
25	SMTP
53	DNS

Security Importance

- Open ports increase attack surface
- Unused ports should be closed

---

6. Firewalls (Network Security Gatekeepers)

What Is a Firewall?

A firewall controls **which traffic is allowed or blocked**.

Types of Firewalls

1. **Packet-Filtering Firewall**
    - Filters by IP, port, protocol
2. **Stateful Firewall**
    - Tracks active connections
3. **Application Firewall (WAF)**
    - Protects web applications

Firewall Rules Example

- Allow HTTPS traffic
- Block unknown IPs
- Restrict admin access

Interview Line

“Firewalls reduce attack surface by controlling network traffic.”

---

7. TLS (Transport Layer Security) – Basics

What Is TLS?

TLS encrypts data **between client and server**.

Used in:

- HTTPS
- Secure email
- APIs

Why TLS Is Important

- Prevents data interception
- Prevents tampering
- Ensures server authenticity

TLS Handshake (Simple Flow)

1. Client says: “Hello”
2. Server sends certificate
3. Client verifies certificate
4. Encryption keys exchanged
5. Secure communication begins

Interview Line

“TLS ensures confidentiality, integrity, and authentication for data in transit.”

---

8. Hands-On: Wireshark Traffic Analysis

What Is Wireshark?

A network packet analyzer.

Used to:

- Capture network traffic
- Analyze packets
- Investigate incidents

What You Learn Using Wireshark

- How packets look
- Difference between HTTP and HTTPS
- TCP handshakes
- DNS queries

Basic Filters to Know

http

https

dns

tcp

---

9. Inspect HTTPS Handshake (Conceptual)

What You Will See in Wireshark

- Client Hello
- Server Hello
- Certificate exchange
- Encrypted traffic

Important Observation

- Data content is encrypted
- Metadata (IP, ports) is visible