Session 8 Firewalls & IDS/IPS Basics

1. Firewall Basics

A firewall is a security device (hardware or software) that controls network traffic based on predefined rules.
Main job: allow good traffic, block bad or suspicious traffic.

Types of Firewalls:

1. Packet-Filtering Firewall
    - Works at Layer 3 (Network).
    - Inspects headers (IP, port, protocol).
    - Simple, fast, but limited (cannot analyze content deeply).
2. Stateful Firewall
    - Tracks active connections (state table).
    - More secure than packet-filtering.
    - Operates at Layer 3 & 4.
3. Application/Proxy Firewall
    - Works at Layer 7 (Application).
    - Understands application protocols (HTTP, DNS, etc.).
    - Can block malicious requests like SQL injections.
4. Next-Generation Firewall (NGFW)
    - Combines stateful firewall + IDS/IPS + application awareness.
    - Provides advanced security features (SSL inspection, malware detection).

2. IDS (Intrusion Detection System)

IDS is like a security camera.
Monitors network traffic and alerts if something suspicious is detected.
Does not block traffic, only detects and alerts.

- Types:
- NIDS (Network IDS): Monitors network traffic.
- HIDS (Host IDS): Monitors activity on a specific host (files, logs, processes).

3. IPS (Intrusion Prevention System)

IPS is like a security guard.
Detects malicious traffic and can block/drop it in real-time.
Usually placed inline (directly in traffic path).

4. Key Difference (IDS vs IPS):

IDS = Detects, Alerts.
IPS = Detects, Blocks.

4. Why These Matter for SOC Analysts

Firewalls:SOC analysts often check alerts about blocked or allowed connections.
IDS/IPS: Analysts review alerts like port scans, brute force attempts, malware traffic.
Knowing the basics helps understand why an alert triggered and whether to escalate.

Key Takeaway

Firewalls control access with rules.
IDS detects suspicious activity.
IPS blocks malicious activity.
For L1 SOC, the goal is to identify alerts, understand severity, and escalate if required.