Intrusion Detection & Protection Systems

IDS (Intrusion Detection System)

A tool that watches a network for suspicious or harmful activity and alerts security teams. It does **not** stop the activity, only reports it.

Types:

- **NIDS** (Network IDS) - Monitors network traffic.
- **HIDS** (Host IDS) - Monitors activity on a specific device.

IPS (Intrusion Prevention System)

Similar to IDS but takes action to stop threats when detected.

Types:

- **NIPS** (Network IPS) - Stops network threats.
- **HIPS** (Host IPS) - Stops threats on a device.

SIEM (Security Information and Event Management)

A tool that collects, organizes, and analyzes security data from different sources. It helps security teams find and understand threats.

EDR (Endpoint Detection & Response)

A security tool that monitors devices (laptops, phones, etc.) for malware and automatically stops it.

SOAR (Security Orchestration Automation & Response)

A system that automates security tasks like scanning for weaknesses and responding to threats. It helps security teams work faster.

Honeyport

A **trap** designed to attract hackers. It helps security teams detect attacks and learn about hacker behavior.

Securing the Network

1. Building Security from the Ground Up

What's in My Network?

- Networks have many devices and connections that need protection.
- Wireless networks and remote access make security even harder.

How Do You Build a Secure Network?

- **Defense-in-Depth:** Protect every part of the network, not just the edges.
- **Zero Trust:** Never trust any device or user by default. Always verify.
- **Segmentation:** Divide the network into smaller, more secure sections.
    - **DMZ (Demilitarized Zone):** A buffer area between the internet and private networks. Often used for email and web servers.
- **VLAN (Virtual LAN):** A way to separate devices on a network without needing extra physical hardware.
- **VPN (Virtual Private Network):** Encrypts internet traffic for security.

How Do You Defend Your Network?

Detecting & Preventing Threats

- **Detection Tools:** IDS, SIEM
- **Prevention Tools:** Antivirus, Scanners, Firewalls, IPS

Virtualization & The Cloud

On-Premises vs. Cloud

- Like **CDs vs. Spotify** – Instead of storing everything yourself, you use a service.
- No need for physical servers; everything runs in the cloud.
- Cloud services reduce costs and maintenance.

Cloud Deployment Models

1. **Public Cloud:** Services like AWS, Google Cloud, and Azure that multiple companies share.
2. **Private Cloud:** A cloud system used only by one company.
3. **Hybrid Cloud:** A mix of public cloud and private infrastructure.
4. **Community Cloud:** A shared cloud for multiple organizations with similar needs.

Cloud Service Models

1. **SaaS (Software as a Service):** The provider manages everything (e.g., Google Drive, Gmail).
2. **PaaS (Platform as a Service):** The provider manages infrastructure and OS (e.g., Google App Engine).
3. **IaaS (Infrastructure as a Service):** The provider only provides the hardware, and the company manages the rest (e.g., Amazon EC2).

Summary of Secure Network Building & Cloud Computing

1. **How to Build Secure Networks:** Defense-in-depth, zero trust, segmentation, VLANs, VPNs.
2. **Common Cloud Models:** Public, private, hybrid, and community clouds. Cloud services include SaaS, PaaS, and IaaS.