

Introduction to Network Security

Introduction to Network Security

Key concepts, goals, and foundational practices for protecting computer networks.

1. What Is Network Security?

- **Definition** – The set of policies, procedures, and technologies designed to protect the confidentiality, integrity, and availability (CIA) of data and resources as they travel across or reside within a network.
- **Scope** – Includes hardware, software, data, users, and the communication channels that connect them.
- **Why It Matters** – Cyberattacks can lead to data breaches, financial loss, reputational damage, and legal penalties.

2. Core Objectives (CIA Triad)

Objective	What It Means	Typical Controls
Confidentiality	Ensure only authorized parties can view data.	Encryption, access controls, VPNs, VLAN segmentation
Integrity	Prevent unauthorized alteration of data.	Checksums, digital signatures, hashing, intrusion detection
Availability	Keep services and data accessible when needed.	Redundancy, load balancing, DDoS mitigation, backups

3. Major Threat Vectors

Threat Type	Description	Example
Malware	Malicious software that infiltrates or damages systems.	Ransomware, trojans, worms
Phishing & Social Engineering	Deception techniques to steal credentials.	Fake login pages, spear phishing emails

Introduction to Network Security

Threat Type	Description	Example
Man-in-the-Middle (MitM)	Intercepting and possibly altering traffic.	ARP spoofing, SSL stripping
Denial-of-Service (DoS/DDoS)	Overwhelming resources to make services unavailable.	Botnet-driven traffic floods
Insider Threats	Malicious or careless actions by authorized users.	Data exfiltration, privileged account abuse
Zero-Day Exploits	Attacks exploiting unknown vulnerabilities.	Targeted exploits before patches are released

4. Fundamental Security Controls

4.1 Perimeter Defense

- **Firewalls** – Packet filtering, stateful inspection, next-generation firewalls (NGFW) with deep packet inspection.
- **Demilitarized Zone (DMZ)** – Isolated subnet for public-facing services (web, mail, DNS).

4.2 Access Management

- **Authentication** – Passwords, multi-factor authentication (MFA), certificates.
- **Authorization** – Role-based access control (RBAC), least-privilege principle.
- **Accounting** – Logging and audit trails for user activity.

4.3 Encryption

- **In-Transit** – TLS/SSL, IPsec VPNs, SSH.
- **At-Rest** – Full-disk encryption, database encryption, file-level encryption.

4.4 Intrusion Detection & Prevention

- **IDS** – Signature-based, anomaly-based, or hybrid sensors that alert on suspicious activity.
- **IPS** – Actively blocks or throttles malicious traffic based on IDS findings.

4.5 Endpoint Protection

Introduction to Network Security

- Antivirus/anti-malware, host-based firewalls, endpoint detection and response (EDR) agents.

4.6 Secure Configuration & Patch Management

- Harden OS/network devices (disable unnecessary services, change default credentials).
- Apply security patches promptly; use automated patch management tools.

4.7 Monitoring & Logging

- Centralized log collection (SIEM – Security Information and Event Management).
 - Real-time alerts, correlation rules, and incident response playbooks.
-

5. Network