Module 2: Securing Networks

ENDPOINT SECURITY | CISCO NETWORKING ACADEMY

PREPARED BY: **KUDZAISHE MAJEZA**

Agenda

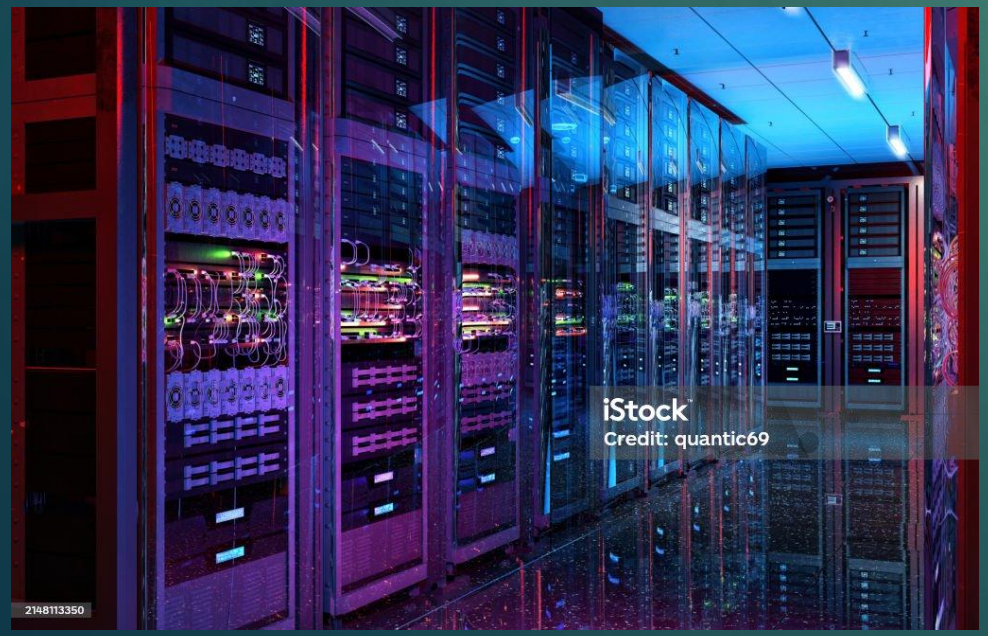
- Introduction to Network Security
- Devices & Tools (firewalls, IDS/IPS, routers, switches)
- Firewalls & Access Control
- Network Segmentation & Zero Trust
- Wireless Security Best Practices
- Secure Protocols & Remote Access
- Monitoring & Incident Detection
- Real-life network incident
- Summary & takeaway

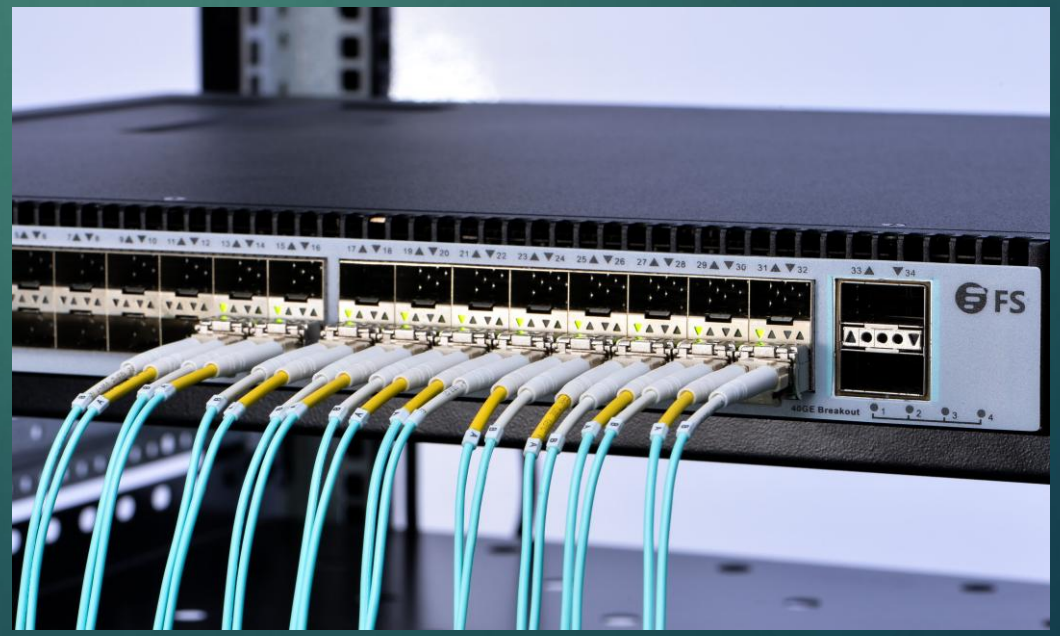
What is Network Security?

- Protect networks, systems and data from unauthorized access.
- Maintain CIA: Confidentiality, Integrity, Availability.
- Covers policies, hardware, software, and human factors.
- Endpoint security is the last line of defence often the target.

Network Security Devices & Tools

- Firewalls (packet-filtering, stateful, NGFW)
- Routers & ACLs (filtering at network edge)
- Switches: VLANs, port security, 802.1X
- IDS/IPS for detection/prevention
- VPN / IPsec for secure remote access
- EDR & EPP on endpoints





Firewalls & Access Control

- Packet-filter vs stateful vs application (NGFW)
- ACLs = first line of traffic filtering on routers
- Stateful inspection retains connection context
- NGFWs inspect application layer (HTTP, DNS)
- Principle of least privilege

Network Segmentation & Zero Trust

- VLANs and subnets to isolate groups
- Micro-segmentation for workloads (data centers/cloud)
- Zero Trust: “never trust, always verify”
- Limit lateral movement to reduce blast radius

Wireless Network Security

- Use WPA3 (or WPA2-Enterprise with 802.1X)
- Disable WPS; strong passphrase + unique SSID naming
- Guest networks separated from internal NICs
- Monitor for rogue APs and use RF scanning
- Use certificate-based authentication (EAP-TLS) when possible

Secure Protocols & Remote Access

- HTTPS / TLS for web traffic
- SSH not Telnet for remote management
- SFTP/FTPS vs FTP
- VPNs or IPsec for remote workers
- Avoid plaintext protocols on the LAN

Monitoring & Incident Detection

- Use SIEM for log aggregation & correlation
- NetFlow / sFlow for traffic baselining
- IDS/IPS: signature & anomaly detection
- File integrity monitoring and endpoint telemetry (EDR)
- Playbooks & runbooks for incident response

Human Factors & Hardening

- MFA for privileged accounts
- Strong password policies and password managers
- Regular patching and vulnerability scanning
- Least-privilege access for user accounts
- Security awareness training & phishing simulations

Real-Life Incident

- 2024–2025: LockBit Ransomware

In early 2025, the **LockBit ransomware group** launched a major cyberattack against several global manufacturing companies. The attackers exploited an **unpatched VPN appliance**, which allowed them to break into the internal network. Once inside, they moved laterally, encrypted production servers, and shut down factory operations for days. The incident caused millions in damages and demonstrated how critical **patch management, network segmentation, and multi-factor authentication (MFA)** are in defending modern networks.

Case Study: How the Attack Could Have Been Prevented

- Patch VPN appliance firmware immediately
- Restrict management interfaces to management subnet (no public access)
- Enforce MFA for remote logins
- Network segmentation so production systems not directly reachable
- Offline/immutable backups to recover without paying ransom

Summary & Key Takeaways

- Secure protocols, segmentation and monitoring are critical
- Keep devices patched and limit management exposure
- Endpoints need EDR + user training
- Real incidents reinforce layered defenses & backups

References & Further Reading

- Cisco Networking Academy materials (Endpoint Security)
- CERT/US posts on recent ransomware incidents
- News sources (Reuters/BBC/CNN) for the attack cited
- MITRE ATT&CK framework (for attacker tactics)