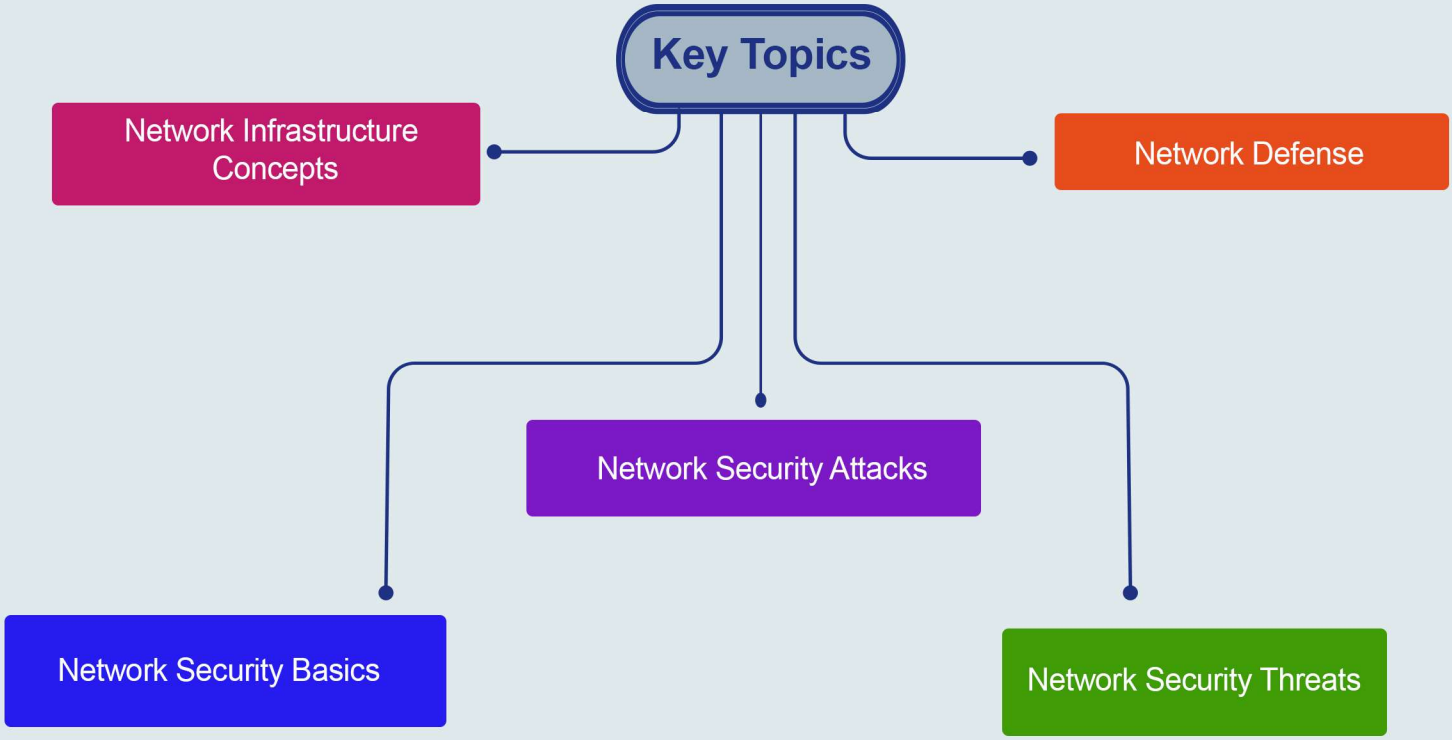
About the Course

A company's network is its information infrastructure. If you can keep the network secure, you can keep the systems on that network secure. This course provides the skills needed to secure a modern LAN network. It teaches how to enforce security on firewalls, routers, and switches and how to monitor the overall network to detect and prevent against attacks.

Learning Objectives

1. Understanding Network Security Concepts
2. Understanding Network Security Risks & Threats
3. Fixing Network Vulnerabilities
4. Developing and Designing a Secure Network
5. Configure Security Policies over Network Devices
6. Secure Configuration of Network Devices

Key Topics



Pre Requisites

A powerful knowledge about network concepts and understanding of information security topics is necessary for students attending this class.

- Information Security Concepts & Principles Course

Terminus System

What You Will Receive

- Course Presentation File
- Complementary Files
- Network Security eBook

Who Should Attend

- Network Administrator
- Security Engineers
- CTOs
- System Administrators
- System Engineers
- Network administrators
- Security Engineers
- System Administrators
- IT Managers
- Information Security Professionals
- Penetration Testers

Syllabus

Network Infrastructure Concepts

- Hardware architecture
- Memory Protection
- OSI Reference Model
- Common TCP Protocols
- TCP 3-way Handshake
- Types of Digital Subscriber Lines (DSL)
- LAN Packet Transmission
- LAN / WAN Media
- Port Ranges
- Network Types
- Remote Access Services
- Networking Methods & Standards
- Hardware Devices
- Communication Hardware Devices
- WAN Transmission Types
- Wireless Networking
- Leased Lines
- Types of Digital Subscriber Lines (DSL)
- LAN Packet Transmission
- LAN / WAN Media
- Network Protocols

Syllabus

Network Security Basics

- Security Policy
- Standards
- Procedures
- Baselines
- Guidelines
- Security Models
- The OSI Model & the Domino Effect
- Security Wheel
- Security Threats
- Secure Network Design
- Secure Network Device Configurations
- Secure Network Device Management
- Security Monitoring and Maintenance
- Attack Detection and Response

Network Security Threats

- Malware
- Social Engineering
- Phishing Attacks
- Man-In-The-Middle
- DNS Poisoning
- Denial-of-Service attack
- DDoS Attacks
- Spam
- Malware
- Worm
- Trojan
- Drive-by Download

Syllabus

- Spyware
- Keystroke logging
- Adware
- BOT
- Social engineering
- Tabnabbing
- Email spoofing
- Password cracking
- Buffer Overflow
- Network scanning
- Information gathering
- Port Scanning
- Vulnerability Scanning
- Man-in-the Middle (MiTM)
- MITM Attack tools
- MITM Proxy only tools

Network Defense

- Secure Network Design
- Email Security
- VoIP Security
- Messaging Security
- Access Control Systems
- Network Policy Server
- Security Protocols
- VPN
- Hashing
- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)
- UTM
- Router Security

Syllabus

- Switch Security
- Network Monitoring
- Encryption, Cryptography & Digital Signatures

Hands-on Training

- Lab 1 – Firewall Security Configuration
- Lab 2 – Router Secure Configuration
- Lab 3 – Switch Secure Configuration
- Lab 4 - Cryptography