Network Security Essentials: Defend & Protect

Duration: 4 days (32 hours)

1: Network Security Essentials & Architecture

Module 1: Fundamentals of Network Security

- Core concepts of confidentiality, integrity, and availability (CIA)
- Types of network-based attacks
- Importance of layered security
- Common roles in network defense

Module 2: Secure Network Design

- Network segmentation and isolation
- Demilitarized zones (DMZ)
- Secure topologies and design principles
- Network zones and trust levels

Module 3: Network Security Controls

- Types of security controls: administrative, technical, physical
- Access control models (DAC, MAC, RBAC)
- Overview of security devices (firewalls, proxies, etc.)
- Basics of secure configuration and hardening

2: Protocols, Monitoring & Administrative Security

Module 4: Secure Protocols and Services

- Overview of insecure vs secure protocols
- Secure alternatives: HTTPS, SFTP, SNMPv3, SSH
- Common port numbers and services
- Network protocol behaviors

Module 5: Network Traffic Basics

- Introduction to traffic monitoring and analysis
- Understanding network logs
- Common indicators of scanning or probing
- Basic concepts of anomaly detection

Module 6: Administrative Network Security

- Role-based access control and privilege separation
- Secure user management practices
- Policy-based device configurations
- Secure handling of credentials and passwords

3: Device, Endpoint & Wireless Security

Module 7: Securing Network Devices

- Basic switch and router security concepts
- Disabling unused services and ports
- Firmware updates and patching
- Physical security of networking equipment

Module 8: Endpoint Security Basics

- Importance of endpoint protection
- Common endpoint threats
- Device management policies (USBs, local admin rights)
- Importance of software updates

Module 9: Wireless Network Security

- Basics of wireless encryption (WEP, WPA2, WPA3)
- Authentication methods for Wi-Fi
- Risks with open and misconfigured wireless setups
- Best practices for secure wireless access

4: Response Readiness & Governance

Module 10: Introduction to Incident Handling

- What is an incident?
- Steps in the incident response process
- Roles and responsibilities during an incident
- Common communication protocols

Module 11: Fundamentals of Continuity and Recovery

- Importance of backups

- Key terms: RTO, RPO, BIA (explained simply)
- Redundancy vs resilience
- Understanding failover concepts

Module 12: Security Governance & Policy Overview

- Importance of written security policies
- Acceptable use, remote access, and email policies
- Introduction to standards and frameworks (ISO 27001, NIST, etc.)
- Roles of audit and compliance in network environments