COURSE SYLLABUS

Networking Fundamentals for Security Course

Build the networking foundation every security role depends on, and learn the devices, protocols, and attacks you will defend.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/networking-fundamentals-for-security-course

support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1: Introduction to Networking for Security Professionals

- Lessons:
  - Why Networking Knowledge Matters in Security
  - How This Course Is Organized
  - A First Look at a Network: Hosts, Media, and Data Flow
- Applied activity: Learners trace a simple request, their own computer loading a web page, and identify, in plain language, every hop and component that request likely passes through, from their laptop to the web server and back.

Module 2: The OSI and TCP/IP Models

- Lessons:
  - The Seven Layers of the OSI Model
  - The TCP/IP Model and How It Maps to OSI
  - Encapsulation and De-encapsulation Walkthrough
  - Why Security Tools Are Organized by Layer
- Applied activity: Given a short, plain-text packet description, learners identify which OSI layer each listed field belongs to, for example a MAC address, an IP address, a port number, and an HTTP request line.

Module 3: IP Addressing and Subnetting Fundamentals

- Lessons:
  - IPv4 Addressing: Structure and Classes
  - Subnet Masks and CIDR Notation
  - Subnetting a Network, Step by Step
  - Public, Private, and NAT Addressing
- Applied activity: Learners are given a small organization's addressing requirement, a set number of hosts across three departments, and subnet a provided address block to fit, then identify which addresses in the range are unusable.

Module 4: Network Devices and Infrastructure

- Lessons:
  - Hubs, Switches, and How Switching Works
  - Routers and Routing Basics
  - Firewalls and Their Placement in a Network
  - Load Balancers, Proxies, and Other Intermediary Devices
- Applied activity: Learners label a simple, text-described network diagram, placing a router, switch, firewall, and DMZ segment correctly based on a short design scenario.

Module 5: Core Network Protocols and Services

- Lessons:
  - TCP and UDP: Connection-Oriented versus Connectionless
  - DNS: How Name Resolution Works
  - DHCP: How Hosts Get an Address
  - HTTP, HTTPS, and Common Application Protocols
- Applied activity: Learners walk through a short, annotated sequence describing a browser loading a secure website, including the DNS lookup, the TCP handshake, the TLS negotiation, and the HTTP request, and label each step with the protocol responsible.

Module 6: Network Topologies and Architecture

- Lessons:
  - Physical and Logical Topologies
  - Star, Mesh, and Hybrid Designs
  - Network Segmentation and VLANs
- Applied activity: Learners redesign a described flat network, with all devices on one segment, into a segmented design using VLANs, based on a short scenario involving a guest network and a finance department.

Module 7: Wireless Networking Fundamentals

- Lessons:
  - How Wireless Networking Works
  - Wireless Standards and Frequency Bands
  - Wireless Security Protocols: WEP, WPA, WPA2, and WPA3
  - Common Wireless Risks and Misconfigurations
- Applied activity: Learners review a short description of a small office's wireless setup and identify which choices, including protocol, SSID broadcast, and default credentials, create risk, and what they would change.

Module 8: Network Security Fundamentals and Defense in Depth

- Lessons:
  - Defense in Depth: Layered Security Concepts
  - Zero Trust Networking Principles
  - Access Control at the Network Layer
  - Putting It Together: A Layered Network Design
- Applied activity: Learners evaluate a short case description of an organization relying on a single perimeter firewall and propose at least two additional layers of defense, explaining the risk each addresses.

Module 9: Common Network Threats and Attack Techniques

- Lessons:
  - Reconnaissance and Scanning
  - Sniffing and Man-in-the-Middle Attacks
  - Spoofing Techniques: ARP, DNS, and IP
  - Denial-of-Service and Distributed Denial-of-Service
  - Recognizing Attack Patterns in Everyday Traffic
- Applied activity: Learners review a short, described sequence of unusual network activity, such as a spike in ARP replies or a host suddenly resolving a domain to an unexpected address, and identify which attack technique best matches the pattern.

Module 10: Network Monitoring and Basic Defense

- Lessons:
  - What Network Monitoring Tools Actually Do
  - Firewalls, IDS, and IPS: Roles and Differences
  - Building Security Habits: What to Watch For
- Applied activity: Learners review a short, simplified log excerpt, described in text rather than a live tool, and identify which entries warrant a closer look, based on concepts covered earlier in the course.