

**Network Security for Developers**

**Course Number:** SEC-150  
**Duration:** 3 days

**Overview**

Securing network communication is critical in today's interconnected world. This network security training teaches developers how to leverage cryptographic techniques like hashing, encryption, digital signatures, TLS, and PKI in a TCP/IP environment.

By the end of this training, learners have a solid understanding of network attacks across all OSI layers, from classic attacks like ARP and NDP spoofing to modern threats like DNS cache poisoning. They also learn how to prevent these attacks through secure switch configuration, operating system settings, and proper protocol usage.

**Prerequisites**

All learners must have general network application development experience.

**Materials**

All attendees receive comprehensive courseware.

**Software Needed on Each Student PC**

Attendees will not need to install any software on their computers for this class. The class will be conducted in a remote environment that Accelebrate will provide; students will only need a local computer with a web browser and a stable Internet connection. Any recent version of Microsoft Edge, Mozilla Firefox, or Google Chrome will work well.

**Objectives**

* Gain a foundational understanding of essential cybersecurity concepts
* Understand how cryptography supports security
* Learn the most common attacks from OSI Layer 2 to Layer 7
* Implement secure protocols and configurations to mitigate attacks
* Explore various Denial of Service (DoS) attack vectors and how to defend against them
* Leverage network traffic manipulation tools
* Understand the principles of secure design and apply them to build robust and resilient network applications

**Outline**

* Cyber Security Basics
  + What is security?
  + Threat and risk
  + Cyber security threat types – the CIA triad
  + Cyber security threat types – the STRIDE model
  + Consequences of insecure software
  + Constraints and the market
  + The dark side
* Cryptography for Developers
  + Cryptography basics
  + Elementary algorithms
    - Random number generation
    - Hashing
    - Hash algorithms for password storage
  + Confidentiality protection
    - Symmetric encryption
    - Asymmetric encryption
    - Combining symmetric and asymmetric algorithms
    - Key exchange and agreement
  + Integrity protection
    - Authenticity and non-repudiation
    - Message Authentication Code (MAC)
* Network Security
  + Network security overview
  + The communication layers
  + Threats against TCP/IP
  + The Data Link layer
    - ARP spoofing and ARP poisoning
    - Lab – ARP spoofing
    - Protecting against ARP spoofing
    - Attacks against the Spanning Tree Protocol
    - Mitigating Spanning Tree Protocol attacks
    - MAC flooding and MAC table overflow
    - Port stealing
    - Port protection
    - Data link attacks and IPv6
    - Lab – IPv6 NDP spoofing
    - DHCP threats
    - Lab – DHCP starvation
    - Protecting against DHCP attacks
    - DHCPv6 security
    - VLAN issues
    - Securing VLANs
    - Sniffing
    - Protecting your network against sniffing and MitM
  + The network layer
    - Spoofing IP addresses
    - Protecting against IP spoofing
    - IP fragmentation and the teardrop attack
    - IPv6-specific attacks and defenses
    - Smurf attack against ICMP
    - Lab – Smurf attack
    - Case study – Ping of death
    - Redirecting ICMP – route hijacking
    - Lab – Route hijacking
    - Black hole attacks and selective forwarding in ad hoc networks
    - Attacks against ICMPv6
    - Routing protocol threats
    - Securing routing protocols
    - IPsec overview
    - IPsec usage scenarios and typical mistakes
    - IPsec cryptographic requirements
  + The transport layer
    - The TCP protocol
    - The UDP protocol
    - SYN flooding
    - Lab – SYN flooding
    - Protecting against SYN floods
    - UDP flooding
    - TCP session hijacking and other attacks
    - Fingerprinting via TCP, UDP, and ICMP
    - Lab – Fingerprinting and service detection
    - Firewalls and IDS
    - Lab – Using a NIDS
  + The application layer
    - The Domain Name System
    - DNS cache poisoning
    - Lab – DNS cache poisoning
    - DNS rebinding
    - DNS amplification
    - DoS targeting DNS
    - Securing DNS systems
    - Lab – DNSSEC
    - Case study – MaginotDNS attack
    - Secure protocols
    - Securing email protocols
    - Web application firewalls and IDS
  + Transport security
    - The TLS protocol
    - Securing HTTP
* Denial of Service
  + Flooding
  + Resource exhaustion
  + Sustained client engagement
  + Infinite loop
  + Case study – DoS against Tesla GUI via malicious web page
  + Economic Denial of Sustainability (EDoS)
  + Amplification
    - Some amplification examples
  + Algorithmic complexity issues
    - Regular expression denial of service (ReDoS)
    - Hash table collision
* Security by Design
  + Secure design principles of Saltzer and Schroeder
    - Economy of mechanism
    - Fail-safe defaults
    - Complete mediation
    - Open design
    - Separation of privilege
    - Least privilege
    - Least common mechanism
    - Psychological acceptability
    - Additional principles
* Wrap Up
  + Secure coding principles
    - Principles of robust programming by Matt Bishop
  + And now what?
    - Software security sources and further reading
    - Network security resources