CA402: Network Security

35 Instructional Hours 58 CPEs 23 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

INTERMEDIATE

This course provides a comprehensive and practical foundation in network security, combining core networking principles with modern defensive strategies. It begins with essential networking concepts such as network architecture, devices, protocols, and addressing, then progresses into security-focused topics including segmentation, firewall management, intrusion detection, and secure network design. The material emphasizes real-world application by integrating defensive techniques, monitoring strategies, and incident response practices. Learners develop both theoretical understanding and operational skills required to design, secure, and troubleshoot modern network environments.

You Will Be Able To

- Analyze network architectures using OSI and TCP/IP models to understand data flow and security implications
- Configure and secure network components including firewalls, NAT/PAT, and access controls
- Design secure network architectures using segmentation, DMZs, and defense-in-depth strategies
- Identify and mitigate common network-based attacks such as ARP poisoning, DHCP attacks, and DNS spoofing
- Monitor and investigate network activity using logging, telemetry, and packet analysis tools

Who Should Attend

This course is designed for individuals seeking a strong foundation in both networking and network security. It is suitable for beginners entering cybersecurity, IT students, and professionals transitioning into network defense roles. It is also valuable for system administrators and IT support personnel who want to deepen their understanding of how networks operate and how to secure them against modern threats. The course accommodates learners with basic technical knowledge and progressively builds toward more advanced defensive concepts.

Relevant Combat Roles

- Network Security Analyst
- SOC (Security Operations Center) Analyst
- Network Engineer (Security-focused)
- Cyber Defense Analyst
- Incident Response Analyst

Topics Covered

Network Fundamentals & Models
Network types (LAN/WAN/MAN), devices (switches, routers, NICs), and core concepts like encapsulation. Includes OSI vs TCP/IP models and data flow across layers.

Ethernet & Infrastructure
Ethernet standards, switching, frame structure, and cabling types (UTP, fiber, coax) with categories (Cat5e–Cat8).

Protocols & Addressing
Key protocols (HTTP, DNS, SMTP, TCP/UDP), plus IPv4/IPv6, subnetting, CIDR, ARP, and NAT/PAT.

Secure Architecture & Defense
Segmentation, DMZ, trust boundaries, and traffic flow (north-south vs east-west) with defense-in-depth design.

Security Controls & Monitoring
Firewalls, NAC, VPNs, DHCP snooping, ARP defense, plus logging (Syslog), NetFlow, SIEM, IDS/IPS.

Troubleshooting & Wireless
Tools (Wireshark, ping, traceroute), monitoring, and Wi-Fi security (WPA2/WPA3, common attacks).

Labs

Network Traffic Analysis & Wireshark Operations
(packet capture, protocol analysis, anomaly detection, and traffic inspection using Wireshark)

Firewall Configuration & Policy Enforcement
(Linux iptables/firewalld, Windows Defender Firewall, inbound/outbound filtering, and rule auditing)

Secure Network Architecture & Segmentation
(VLAN design, DMZ implementation, trust boundaries, east-west vs north-south traffic control, and bastion host placement)

Network Attack Simulation & Defensive Analysis
(ARP poisoning, DHCP spoofing/starvation simulations, IDS/IPS detection, telemetry collection, and incident response workflows)

Network Monitoring & Detection Engineering
(Syslog, NetFlow/sFlow/IPFIX, SPAN/TAP capture strategies, SIEM integration, and PCAP-based investigations)