EC-Council Certified Network Defender (CND)

Duration: 5 Days
Method: Instructor-Led

Certification: *Certified Network Defender*

Course Description

This course is a vendor-neutral, hands-on, instructor-led comprehensive network security certification training program. It is a skills-based, lab intensive program based on a job-task analysis and cybersecurity education framework presented by the National Initiative for Cybersecurity Education (NICE). The course has also been mapped to global job roles and responsibilities and the Department of Defense (DoD) job roles for system/network administrators. The course is designed and developed after extensive market research and surveys.

The program prepares network administrators on network security technologies and operations to attain Defense-in-Depth network security preparedness. It covers the "protect, detects and respond" approach to network security. The course contains hands-on labs, based on major network security tools and techniques which will provide network administrators real-world expertise on current network security technologies and operations.

Target Audience

This course is intended for:

- Network Administrators
- Network Security Administrators
- Network Security Engineers
- Network Defense Technicians
- CND Analysts
- Security Analysts
- Security Operators
- IT Administrators
- Anyone who is involved in network operations.

Prerequisites

To attend this course, participants should have:

- Fundamental knowledge of Networking Concepts.
- Fundamental knowledge of Cyber Security.

Exam Details

Exam Tile:	• Certified Network Defender (CND)
Exam Code:	• 312-38
Length of Exam:	• 4 hours
Number of Questions:	• 100
Availability:	• ECCEXAM
Question Format:	• Interactive Multiple Choice Questions

Course Objectives

Upon successful completion of this course, participants will have learned:

- About various network security controls, protocols, and devices.
- To determine the appropriate location for IDS/IPS sensors, tuning IDS for false positives and false negatives, and configurations to harden security through IDPS technologies.
- To troubleshoot their network for various network problems.
- To implement secure VPN implementation for their organization.
- To identify various threats to organization network.
- To identify various threats to wireless network and learn how to mitigate them.
- How to design and implement various security policies for their organizations.
- To monitor and conduct signature analysis to detect various types of attacks and policy violation activities.
- The importance of physical security and the ability to determine and implement various physical security controls for their organizations.
- To perform risk assessment, vulnerability assessment/scanning through various scanning tools and generate detailed reports on it.
- To harden the security of various hosts individually in the organization's network.
- To identify the critical data, choose an appropriate backup method, media and technique to perform a successful backup of organization data on regular basis.
- To choose appropriate firewall solution, topology, and configurations to harden security through the firewall.
- To provide the first response to the network security incident and assist IRT team and forensics investigation team in dealing with an incident.

Course Content

Module 01: Computer Network and Defense Fundamentals

- Network Fundamentals
- Network Components
- TCP/IP Networking Basics
- TCP/IP Protocol Stack
- IP Addressing
- Computer Network Defense (CND)
- CND Triad
- CND Process
- CND Actions
- CND Approaches

Module 02: Network Security Threats, Vulnerabilities, and Attacks

- Essential Terminologies
- Network Security Concerns
- Network Security Vulnerabilities
- Network Reconnaissance Attacks
- Network Access Attacks
- Denial of Service (DoS) Attacks
- Distributed Denial-of-Service Attack (DDoS)
- Malware Attacks

Module 03: Network Security Controls, Protocols, and Devices

- Fundamental Elements of Network Security
- Network Security Controls
- User Identification, Authentication, Authorization and Accounting
- Types of Authorization Systems
- Authorization Principles
- Cryptography
- Security Policy
- Network Security Devices
- Network Security Protocols

Module 04: Network Security Policy Design and Implementation

- What is Security Policy?
- Internet Access Policies
- Acceptable-Use Policy
- User-Account Policy
- Remote-Access Policy
- Information-Protection Policy
- Firewall-Management Policy
- Special-Access Policy
- Network-Connection Policy
- Business-Partner Policy
- Email Security Policy
- Passwords Policy
- Physical Security Policy
- Information System Security Policy
- Bring Your Own Devices (BYOD) Policy
- Software/Application Security Policy
- Data Backup Policy
- Confidential Data Policy
- Data Classification Policy
- Internet Usage Policies
- Server Policy
- Wireless Network Policy
- Incidence Response Plan (IRP)
- User Access Control Policy
- Switch Security Policy
- Intrusion Detection and Prevention (IDS/IPS) Policy
- Personal Device Usage Policy
- Encryption Policy
- Router Policy
- Security Policy Training and Awareness
- ISO Information Security Standards
- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Information Security Acts: Sarbanes Oxley Act (SOX)
- Information Security Acts: Gramm-Leach-Bliley Act (GLBA)
- Information Security Acts: The Digital Millennium Copyright Act (DMCA) and the Federal Information Security Management Act (FISMA)
- Other Information Security Acts and Laws

Course Content, *Continued*

Module 05: Physical Security

- Physical Security
- Access Control Authentication Techniques
- Physical Security Controls
- Other Physical Security Measures
- Workplace Security
- Personnel Security: Managing Staff Hiring and Leaving Process
- Laptop Security Tool: EXO5
- Environmental Controls
- Physical Security: Awareness/Training
- Physical Security Checklists

Module 06: Host Security

- Host Security
- OS Security
- Linux Security
- Securing Network Servers
- Hardening Routers and Switches
- Application/Software Security
- Data Security
- Virtualization Security

Module 07: Secure Firewall Configuration and Management

- Firewalls and Concerns
- What Firewalls Do?
- What should you not Ignore?: Firewall Limitations
- How Does a Firewall Work?
- Firewall Rules
- Types of Firewalls
- Firewall Technologies
- Firewall Topologies
- Firewall Rule Set & Policies
- Firewall Implementation
- Firewall Administration
- Firewall Logging and Auditing
- Firewall Anti-Evasion Techniques
- Why Are Firewalls Bypassed?
- Full Data Traffic Normalization
- Data Stream-based Inspection
- Vulnerability-based Detection and Blocking
- Firewall Security Recommendations and Best Practices
- Firewall Security Auditing Tools

Module 08: Secure IDS Configuration and Management

- Intrusions and IDPS
- IDS
- Types of IDS Implementation
- IDS Deployment Strategies
- Types of IDS Alerts
- IPS
- IDPS Product Selection Considerations
- IDS Counterparts

Module 09: Secure VPN Configuration and Management

- Understanding Virtual Private Network (VPN)
- How VPN works?
- Why Establish VPN?
- VPN Components
- VPN Concentrators
- Types of VPN
- VPN Categories
- Selecting Appropriate VPN
- VPN Core Functions
- VPN Technologies
- VPN Topologies
- Common VPN Flaws
- VPN Security
- Quality of Service and Performance in VPNs

Course Content, *Continued*

Module 10: Wireless Network Defense

- Wireless Terminologies
- Wireless Networks
- Wireless Standard
- Wireless Topologies
- Typical Use of Wireless Networks
- Components of Wireless Network
- WEP (Wired Equivalent Privacy) Encryption
- WPA (Wi-Fi Protected Access) Encryption
- WPA2 Encryption
- WEP vs. WPA vs. WPA2
- Wi-Fi Authentication Method
- Wi-Fi Authentication Process Using a Centralized Authentication Server
- Wireless Network Threats
- Bluetooth Threats
- Wireless Network Security
- Wi-Fi Discovery Tools
- Locating Rogue Access Points
- Protecting from Denial-of-Service Attacks: Interference
- Assessing Wireless Network Security
- Wi-Fi Security Auditing Tool: AirMagnet Wi-Fi Analyzer
- WPA Security Assessment Tool
- Wi-Fi Vulnerability Scanning Tools
- Deploying Wireless IDS (WIDS) and Wireless IPS (WIPS)
- WIPS Tool
- Configuring Security on Wireless Routers
- Additional Wireless Network Security Guidelines

Module 11: Network Traffic Monitoring and Analysis

- Network Traffic Monitoring and Analysis (Introduction)
- Network Monitoring: Positioning your Machine at Appropriate Location
- Network Traffic Signatures
- Packet Sniffer: Wireshark
- Detecting OS Fingerprinting Attempts
- Detecting PING Sweep Attempts
- Detecting ARP Sweep/ ARP Scan Attempts
- Detecting TCP Scan Attempts
- Detecting SYN/FIN DDOS Attempts
- Detecting UDP Scan Attempts
- Detecting Password Cracking Attempts
- Detecting FTP Password Cracking Attempts
- Detecting Sniffing (MITM) Attempts
- Detecting the Mac Flooding Attempts
- Detecting the ARP Poisoning Attempts
- Additional Packet Sniffing Tools
- Network Monitoring and Analysis
- Bandwidth Monitoring

Module 12: Network Risk and Vulnerability Management

- What is Risk?
- Risk Levels
- Risk Matrix
- Key Risk Indicators(KRI)
- Risk Management Phase
- Enterprise Network Risk Management
- Vulnerability Management

Course Content, *Continued*

Module 13: Data Backup and Recovery

- Introduction to Data Backup
- RAID (Redundant Array of Independent Disks) Technology
- Storage Area Network (SAN)
- Network Attached Storage (NAS)
- Selecting Appropriate Backup Method
- Choosing the Right Location for Backup
- Backup Types
- Conducting Recovery Drill Test
- Data Recovery
- Windows Data Recovery Tool
- RAID Data Recovery Services
- SAN Data Recovery Software
- NAS Data Recovery Services

Module 14: Network Incident Response and Management

- Incident Handling and Response
- Incident Response Team Members: Roles and Responsibilities
- First Responder
- Incident Handling and Response Process
- Overview of IH&R Process Flow
- Forensic Investigation
- Eradication and Recovery
- Post-incident Activities
- Training and Awareness

LABS INCLUDED