REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
"Training You Can Really Use"

EC-Council Certified Network Defender (CND)

Duration: 5 Days
Method: Instructor-Led Training (ILT) | Live Online Training

Certification: *Certified Network Defender (CND) —*
Exam: *312-38*

Course Description

This program prepares participants in network security technologies and operations to attain Defence-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. The study-kit provides you with over 10GB of network security best practices, assessments, and protection tools. The kit also contains templates for various network policies and many white papers for additional learning.

Participants enrolled in this course will gain a detailed understanding and hands-on ability to function in real-life situations involving network defence. They will gain the technical depth required to actively design a secure network in your organization. This course gives you the fundamental understanding of the true construct of data transfer, network technologies, software technologies so that participants understand how networks operate, understand what software is automating and how to analyse the subject material. These skills will help participants foster resiliency and continuity of operations during attacks.

Target Audience

This course is intended for:

- Network Administrators
- Network Security Administrators
- Network Security Engineer
- Network Defence Technicians
- CND Analyst
- Security Analyst
- Security Operator
- Persons involved in network operations
- Managers who want to understand cybersecurity core principles and practices
- Operations personnel, who although do not have security as their primary job function, will need an understanding of cybersecurity core principles and practices

Prerequisites

To attend this course, candidates must have:

- Well-versed in cybersecurity fundamentals.

Exam Details

Exam Code:	• 312-38
Length of Exam:	• 4 Hours
Number of Questions:	• 125
Passing Score:	•CEH exam does not have a set passing score. The passing score depends on the exam test form/ set of questions they receive.
Question Format:	• Multiple Choice

Course Objectives

Upon successful completion of this course, attendees will be able to:

- Have learned about various network security controls, and devices.
- Be able 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.
- Be able to troubleshoot their network for various network problems.
- Be able to implement secure VPN implementation for their organization.
- Be able to identify various threats to the organization network.
- Be able to identify various threats to a wireless network and learn how to mitigate them.
- Have learned how to design and implement various security policies for their organizations.
- Be able to monitor and conduct signature analysis to detect various types of attacks and policy violation activities.
- Have learned the importance of physical security and the ability to determine and implement various physical security controls for their organizations.
- Be able to perform risk assessment, vulnerability assessment/scanning through various scanning tools and generate detailed reports on it.
- Be able to harden the security of various hosts individually in the organization's network.

Course Objectives *Continued*

- Be able to identify the critical data, choose the appropriate backup method, media, and technique to perform a successful backup of organization data on regular basis.
- Be able to choose the appropriate firewall solution, topology, and configurations to harden security through the firewall.
- Be able to provide the first response to the network security incident and assist the IRT team and forensics investigation team in dealing with an incident.

Course Topics

Module 1: Computer Network and Defence Fundamentals

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

Module 2: 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

Course Topics *Continued*

Module 4: 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

Module 5: 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

Course Topics *Continued*

Module 6: Host Security

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

Module 7: 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 8: 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 9: Secure VPN Configuration and Management

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

Course Topics *Continued*

Module 10: Wireless Network Defence

- Wireless Terminologies
- Wireless Networks
- Wireless Standard
- Wireless Topologies
- Typical Use of Wireless Networks
- Components of Wireless Networks
- 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 an Appropriate Location
- Network Traffic Signatures
- Packet Sniffer — Wireshark
- Detecting OS Fingerprinting Attempts
- Detecting PING Sweep Attempt
- Detecting ARP Sweep/ ARP Scan Attempt
- Detecting TCP Scan Attempt
- Detecting SYN/FIN DDOS Attempt
- Detecting UDP Scan Attempt
- Detecting Password Cracking Attempts
- Detecting FTP Password Cracking Attempts
- Detecting Sniffing (MITM) Attempts
- Detecting the Mac Flooding Attempt
- Detecting the ARP Poisoning Attempt
- 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 Topics *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

LABS INCLUDED