EC-Council Certified Network Defender (CND)

Overview

The CND certification aims to equip you with hands-on training to function in real life situations involving network defense. You will gain the technical skills required to proactively design a secure network with future threats in mind. This program will be taking to learning math instead of just using a calculator. This program teaches a fundamental understanding of the true construct of data transfer, network technologies, and software technologies so that you understand how network operate, the process software is automating, and how to analyze the subject material.

Course Objectives

You will learn the following skills on:

- Mitigate, harden, and defend from the attacks.
- Network defense fundamentals
- The application of network security controls
- Protocols
- Perimeter appliances
- Secure IDS
- VPN, and firewall configuration
- The intricacies of network traffic signature
- Analysis and vulnerability scanning

These skills will help you when you design grater network security policies and successful incident response plans. They will also help you foster resiliency and continuity of operations during attacks.

Duration

5 Days – 35 Hours (instructor Led Training / Remote Online Training)

EC-Council Certified Network Defender (CND)

Who Should Attend

This course is intended for the following professionals:

- System Administrators
- System Engineers
- Firewall Administrators
- Network Managers
- IT Managers
- IT Professionals
- Anyone interested in network security technologies
- Managers who want to understand cyber security core principles and practices
- Operations personnel, who although do not have security as their primary job function, need an understanding of cyber security core principles and practices.

EC-Council Certified Network Defender (CND)

Course Topics

Module 1	**Computer Network Defense Fundamental** • Network Fundamentals • Network Components • TCP/IP Networking Basics • TCP/IP Protocol Basics • IP Addressing • Computer Network Defense (CND) • CND Triad CND Process • CND Actions • CND Approaches
Module 2	**Network Security Threats, Vulnerabilities and Attack** • Essential Terminologies • Network Security Concerns • Network Security Vulnerabilities • Network Reconnaissance Attacks • Network Access Attacks • Denial of Service (DoS) Attacks • Distributed Denial-of-Attack (DDoS) • Malware Attacks
Module 3	**Network Security Controls, Protocols and Devices** • Fundamentals 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 Protocols
Module 4	**Network Security Policy Design and Implementation** • What is Security Policy? • Internet Access Policies • Acceptable-Use Policy

EC-Council Certified Network Defender (CND)

Module 4	**Network Security Policy Design and Implementation** • 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 Federal Information Security Management Act (FISMA) • Other Information Security Acts and Laws

EC-Council Certified Network Defender (CND)

Module 5	**Physical Security** • Physical Security • Access Control Authentication Techniques • Physical Security Controls • Other Physical Security Measures • Workplace Security • Personnel Security: Managing Sta Hiring and Leaving Process • Laptop Security Tool: EXO5 • Environmental Controls • Physical Security: Awareness/Training • Physical Checklists
Module 6	**Host Security** • Host Security • OS Security • Linux Security • Securing Network Servers • Hardening Routers and Switches • Application/software Security • Data Security • Virtualization Security

EC-Council Certified Network Defender (CND)

Module 7	**Secure Firewall Configuration and Management** • Firewalls and Concerns • What Firewalls Does? • 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 Firewalls are 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

EC-Council Certified Network Defender (CND)

Module 9	**Secure VPN Configuration and Management** • Understanding Virtual Private Network (VPN) • How VPN works? • Why to 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
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

EC-Council Certified Network Defender (CND)

Module 11	**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
Module 12	**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 13	**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

SKILL
Accelerate Your Talent with Skill

5-Day Course Agenda

Time	Day 1	Day 2	Day 3	Day 4	Day 5
9:00am - 10:30am	Ice Breaking Session + Introduction + Lesson 1	Lesson 4	Lesson 7	Lesson 9 +Lab Practice	Lesson 12
10:30am - 10:45am	Morning Break				
10:45am - 12:30pm	Lesson 2	Lesson 5 + Lab practice	Lesson 7 + Lab practice	Lesson 10	Lesson 12 + 13
12:30pm - 1:30pm	Lunch Break				
1:30pm - 3:30pm	Lesson 2 + Lesson 3	Lesson 6	Lesson 8	Lesson 11	Lesson 13 + Lab Practice
3:30pm - 3:45pm	Afternoon Break				
3:45pm - 5:00pm	Lab Practice	Lesson 6 + Lab Practice	Lesson 8	Lesson 11	Final Wrap & Closing for Training