Module Title : EC-Council Certified Network Defender (ECND)
Duration : 5 days

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 akin to learning math instead of just using a calculator.

This program will be akin 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 networks operate, the processes software is automating, and how to analyze the subject material.

You will learn how to mitigate, harden, and defend from the attacks. You will learn network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN, and firewall configuration. You will then learn the intricacies of network traffic signature, analysis and vulnerability scanning which will help you when you design greater network security policies and successful incident response plans. These skills will help you foster resiliency and continuity of operations during attacks.

What typical students would benefit most from this class?

- 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

Course Outline

This program will take a typical Network/SysAdmin and immerse them in the world of Hackers and Cyber Defense. CND participants will be exposed to the following Domains of CND:

Module 01: Computer Network 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 Federal Information Security Management Act (FISMA)
- Other Information Security Acts and Laws

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 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 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 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
- 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 WiFi 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 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

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