EC-Council Certified Network Defender (CND)

Course Overview

View Course Dates & Register Today

This is a 5-day class

Certified Network Defender (CND) 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 of 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.

Who Should Attend

- Network Administrators
- Network security Administrators
- Network Security Engineer
- Network Defense Technicians
- CND Analyst
- Security Analyst
- Security Operator
- Anyone who involves in network operations

Course Objectives

The program prepares network administrators on network security technologies and operations to attain Defense-in-Depth network security preparedness. It covers the protect, detect 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 10 GB of network security best practices, assessments and protection tools. The kit also contains templates for various network policies and a large number of white papers for additional learning.

Course Outline

1 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

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

3 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

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 Federal Information Security Management Act (FISMA) ? Other Information Security Acts and Laws

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

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)

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

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

9 SECURE VPN CONFIGURATION AND MANAGEMENT

Understanding Virtual Private Network (VPN) ? How VPN works? ? Why to Establish VPN ? ? VPN Component 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

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

EC-Council Certified Network Defender (CND)

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

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

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

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