Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

# CND - Certified Network Defender

SecureNinja's CND (Certified Network Defender) training and certification boot camp in Alexandria, VA, Dulles, VA and San Diego, CA 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. This course prepares you for EC-Council’s CND (Certified Network Defender) exam 312-38.

CND (Certified Network Defender) 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.

## Course Objectives

- How to protect, detect and respond to network attacks
- Network defense fundamentals
- The application of network security controls, protocols, perimeter appliances, secure IDS, VPN, and firewall-config
- The intricacies of network traffic signature, analysis, and vulnerability scanning

## Course Mappings

- CND 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 is mapped to the Department of Defense (DoD) job roles for system/network administrators.

## Why Certified Network Defender?

An organizational focus on cyber defense is more important than ever as cyber breaches have a far greater financial impact and can cause broad repetitional damage.

Despite the best efforts to prevent breaches, many organizations are still being compromised. Therefore, organizations must have, as part of their defense mechanisms, trained network engineers who are focused on protecting, detecting, and responding to the threats on their networks.

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

Network administrators spend a lot of time with network environments and are familiar with network components, traffic, performance and utilization, network topology, the location of each system, security policy, etc.

Organizations can be much better in defending themselves from vicious attacks if the IT and network administrators equipped with adequate network security skills. Thus Network administrators can play a significant role in network defense and become the first line of defense for any organization.

There is no proper tactical network security training that is made available for network administrators which provides them core network security skills.

Students enrolled in the Certified Network Defender course, will gain a detailed understanding and hands-on ability to function in real-life situations involving network defense. They will gain the technical depth required to actively design a secure network in your organization. This program will begin learning math instead of just using a calculator. This course gives you the fundamental understanding of the true construct of data transfer, network technologies, software technologies so that you understand how networks operate, understand what software is automating, and how to analyze the subject material.

You will learn how to protect, detect, and respond to the network 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 You Will Learn

- Students will learn about various network security controls, protocols, and devices
- Students will able to troubleshoot their network for various network problems
- Students will able to identify various threats on the organization network
- Students will learn how to design and implement various security policies for their organizations
- Students will learn the importance of physical security and the ability to determine and implement various physical security controls for their organizations
- Students will able to harden the security of various hosts individually in the organization’s network
- Students will able to choose the appropriate firewall solution, topology, and configurations to harden security through a firewall
- Students will 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
- Students will able to implement secure VPN implementation for their organization
- Students will able to identify various threats to a wireless network and learn how to mitigate them
- Students will able to monitor and conduct signature analysis to detect various types of attacks and policy violation activities.

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Students will able to perform risk assessment, vulnerability assessment/scanning through various scanning tools and generate detailed reports on it
- Students will able to identify the critical data, choose an appropriate backup method, media, and technique to perform a successful backup of organization data on a regular basis
- Students will 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.

## Who Should Attend

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

## CND (Certified Network Defender) Exam Info

- Number of Questions: 100
- Passing score: 70%
- Test Duration: 4 Hours
- Test Format: Interactive Multiple Choice Questions
- Test Delivery: Prometric Prime / VUE /  ECCEXAM
- Exam Code: 312-38

## Courseware

- Official Certified Network Defender Courseware

## Course Length

- 40 hours

## Course Modules

- **Module 1 - 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

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- **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

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- 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 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

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- 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 a 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

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- 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 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

- **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

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- 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