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

# CND - Certified Network Defender

## Course Description

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

- Various network security controls, protocols, and devices.
- Troubleshooting network issues for various network problems.
- Identifying various threats on the organization’s network.
- Designing and implementing security policies for organizations.
- Understanding the importance of physical security and implementing various physical security controls.
- Hardening the security of individual hosts within the organization’s network.
- Choosing the appropriate firewall solution, topology, and configurations to enhance security.
- Determining the appropriate location for IDS/IPS sensors, tuning IDS for false positives and false negatives, and configuring IDPS technologies for improved security.
- Implementing secure VPN solutions for the organization.
- Identifying threats to a wireless network and applying mitigation strategies.
- Monitoring and conducting signature analysis to detect various types of attacks and policy violations.
- Performing risk assessments, vulnerability assessments, and scanning using various tools, and generating detailed reports.
- Identifying critical data, selecting appropriate backup methods, media, and

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

techniques to ensure regular and successful data backups.
- Providing first response to network security incidents and assisting the IRT and forensics investigation teams in handling incidents.

## 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: VUE /  ECCEXAM
- Exam Code: 312-38

## Courseware

- Official Certified Network Defender Courseware

## Course Length

- 5 Days
- 40 hours

## Course Outline

### Module 1: Network Attacks and Defense Strategies

•Understanding various network attacks such as reconnaissance, denial-of-service, and malware attacks.

•Implementing defense strategies to protect against these attacks.

•Recognizing different hacking techniques used to exploit vulnerabilities.

•Applying security controls to mitigate risks.

### Module 2: Administrative Network Security

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

•Developing and enforcing security policies and procedures.

•Ensuring compliance with regulatory frameworks and standards.

•Understanding the role of access control mechanisms.

•Implementing security awareness training for employees.

**Module 3: Technical Network Security**

•Implementing access control measures and authentication protocols.

•Configuring network devices to enhance security.

•Applying encryption techniques for secure communication.

•Utilizing intrusion detection and prevention systems (IDS/IPS).

**Module 4: Network Perimeter Security**

•Deploying and managing firewalls to control incoming and outgoing network traffic.

•Setting up demilitarized zones (DMZ) and intrusion detection/prevention systems (IDS/IPS).

•Implementing network segmentation for security.

•Securing remote access connections.

**Module 5: Endpoint Security – Windows Systems**

•Hardening Windows operating systems against threats.

•Implementing antivirus solutions and system monitoring tools.

•Configuring Windows security policies and settings.

•Performing patch management and vulnerability remediation.

**Module 6: Endpoint Security – Linux Systems**

•Securing Linux-based systems through configuration and patch management.

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

•Utilizing security modules and access controls specific to Linux environments.

•Implementing logging and monitoring for Linux systems.

•Applying secure shell (SSH) configurations for secure remote access.

**Module 7: Endpoint Security – Mobile Devices**

•Managing mobile device security policies, including Bring Your Own Device (BYOD) strategies.

•Implementing Mobile Device Management (MDM) solutions.

•Securing mobile applications and data storage.

•Preventing unauthorized access and mobile malware threats.

**Module 8: Endpoint Security – IoT Devices**

•Identifying security challenges unique to Internet of Things (IoT) devices.

•Applying security measures to protect IoT ecosystems.

•Configuring network access control for IoT devices.

•Monitoring IoT traffic for anomalies and potential threats.

**Module 9: Administrative Application Security**

•Managing application security through whitelisting and blacklisting.

•Implementing Web Application Firewalls (WAF) and secure coding practices.

•Identifying vulnerabilities in applications using security testing tools.

•Applying software updates and patches to prevent exploits.

**Module 10: Data Security**

•Classifying and protecting business-critical data.

•Implementing encryption and data loss prevention techniques.

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

•Securing databases and cloud-based data storage.

•Establishing access controls and permissions for sensitive data.

**Module 11: Enterprise Virtual Network Security**

•Securing virtualized network environments.

•Applying security measures in Software-Defined Networking (SDN) and Network Functions Virtualization (NFV).

•Isolating virtual network components to minimize security risks.

•Configuring firewalls and access controls within virtual environments.

**Module 12: Enterprise Cloud Network Security**

•Understanding cloud service models and associated security concerns.

•Implementing security best practices for cloud infrastructures.

•Ensuring compliance with cloud security standards.

•Managing identity and access controls in cloud environments.

**Module 13: Enterprise Wireless Network Security**

•Securing wireless networks against unauthorized access and attacks.

•Implementing robust encryption protocols and monitoring tools.

•Configuring Wireless Intrusion Prevention Systems (WIPS).

•Detecting rogue access points and wireless security threats.

**Module 14: Network Traffic Monitoring and Analysis**

•Utilizing tools to monitor network traffic for anomalies.

•Analyzing traffic patterns to detect potential security incidents.

•Detecting signs of intrusion through packet analysis.

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

•Implementing real-time monitoring and alerting systems.

**Module 15: Network Logs Monitoring and Analysis**

•Collecting and analyzing logs from various network devices.

•Identifying indicators of compromise through log analysis.

•Utilizing Security Information and Event Management (SIEM) solutions.

•Correlating log data to detect suspicious activities.

**Module 16: Incident Response and Forensic Investigation**

•Establishing incident response procedures.

•Conducting forensic investigations to determine the root cause of security incidents.

•Documenting evidence and preserving forensic data.

•Coordinating with law enforcement and regulatory agencies.

**Module 17: Business Continuity and Disaster Recovery**

•Developing and implementing business continuity plans.

•Establishing disaster recovery strategies to ensure organizational resilience.

•Performing risk assessments to identify critical business functions.

•Conducting disaster recovery drills and simulations.

**Module 18: Risk Anticipation with Risk Management**

•Identifying and assessing risks to network security.

•Implementing risk mitigation strategies to reduce potential impacts.

•Performing risk assessments and security audits.

•Establishing a risk management framework for continuous improvement.

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

**Module 19: Threat Assessment with Attack Surface Analysis**

•Evaluating the organization’s attack surface to identify vulnerabilities.

•Prioritizing security measures based on threat assessments.

•Using automated tools to analyze attack surfaces.

•Implementing proactive threat detection techniques.

**Module 20: Threat Prediction with Cyber Threat Intelligence**

•Leveraging threat intelligence to anticipate potential attacks.

•Implementing proactive measures to defend against emerging threats.

•Analyzing global threat trends and their impact on network security.

•Integrating threat intelligence into security operations.