EC-Council CND Bootcamp

Length: 5 days
Format: Bootcamp
Time: Day

About This Course

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 boot camp has also been mapped to global job roles and responsibilities and the Department of Defense (DoD) job roles for system/network administrators. The boot camp is designed and developed after extensive market research and surveys.

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 boot camp 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.

Required Exams

312-38 : Certified Network Defender (CND)

Audience Profile

This boot camp is intended for students seeking to earn their CND certification and who need an expert instructor to guide them throughout the training and exam preparation process. The CND certification is for:

* 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

This boot camp will cover the following topics:

* Student will learn about various network security controls, protocols, and devices
* Students will able to troubleshoot their network for various network problems
* Student will able identify various threats on organization network
* Student will learn how to design and implement various security policies for their organizations
* Student will learn the importance of physical security and able to determine and implement various physical security controls for their organizations
* Student will able to harden security of various hosts individually in the organization’s network
* Student will able to choose appropriate firewall solution, topology, and configurations to harden security through firewall
* Student will able to determine 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
* Student will able identify various threats to wireless network and learn how to mitigate them
* Student will able to monitor and conduct signature analysis to detect various types of attacks and policy violation activities
* Student will able to perform risk assessment, vulnerability assessment/scanning through various scanning tools and generate detailed reports on it
* Student will able to identify the critical data, choose appropriate back up method, media and technique to perform successful backup of organization data on regular basis
* Student will able to provide first response to the network security incident and assist IRT team and forensics investigation team in dealing with an incident

Outline

Module 01: Computer Network and Defense Fundamentals.

Module 02: Network Security Threats, Vulnerabilities, and Attacks.

Module 03: Network Security Controls, Protocols, and Devices.

Module 04: Network Security Policy Design and Implementation.

Module 05: Physical Security.

Module 06: Host Security.

Module 07: Secure Firewall Configuration and Management.

Module 08: Secure IDS Configuration and Management.

Module 09: Secure VPN Configuration and Management.

Module 10: Wireless Network Defense.

Module 11: Network Traffic Monitoring and Analysis.

Module 12: Network Risk and Vulnerability Management.

Module 13: Data Backup and Recovery.

Module 14: Network Incident Response and Management.