INFOSECTRAIN

EC-Council

CND v2

Certified Network Defender

Course Agenda

sales@infosectrain.com | www.infosectrain.com

Index

Overview

Certified Network Defender (CND) by EC-Council strengthens the fundamentals of network security. It provides an in-depth understanding of network security issues and trains network defenders on dealing with them.

CND v2 is the first course in the new Vulnerability Assessment and Penetration Testing (VAPT) Track developed by EC-Council. In the latest version, EC-Council has added and removed domains to focus on a comprehensive approach to deal with current network security issues. The course authenticates your understanding of critical and core concepts of network and information security.

Why CND v2

CND is globally recognized and most sought-after credentials in the field of network security. The new version is based on the cybersecurity education framework and work-role task analysis presented by the National Initiative of Cybersecurity Education (NICE).

The new concept of following the “Predict, Protect, Detect, Respond” cycle by EC-Council has enhanced the learning takeaways by providing a complete package required to defend a network.

Successful completion of CND program and passing the certification exam not only optimize your career opportunities but also provides you an edge over existing competition.

Target Audience

- Network administrator
- Network security professional
- Security professional or auditor
- Site administrator
- Any individual working towards the enterprise and network infrastructure security

Pre-requisite

Basic idea of networking and its components

Exam Information

Test Duration: 4 Hours
Test Format: Multiple Choice
Number of Questions: 100
Test Delivery: ECC EXAM
Exam Prefix: 312-38 (ECC EXAM)
Passing Score: EC council provides exam in the form of various question banks with different difficulty levels. Passing scores can range from 60% to 85%, depending on which form is challenged.

Course Objectives

The courseware of CND is designed to develop a strong and deep understanding of various verticals of networking, talking first about various network and defense strategies proceeding to incident detection and response and advancing to threat assessments and intelligence. Below is the list of modules with a brief description of what they talk about.

Module 01: Network Attacks and Defense Strategies: This module introduces you to different network-based attacks faced by the organization to understand their working and develop defense strategies.

Module 02: Administrative Network Security: It involves developing or updating security infrastructure and continuously monitoring networks for any suspicious actions or unauthorized access

Module 03: Technical Network Security: Implementing authentication and protection controls for user verification to avoid theft of sensitive information or data. Introducing the concept of zero trust and its effectiveness in maintaining a better security posture

Module 04: Network Perimeter Security: Implementation and management of perimeter devices like firewalls, Intrusion Detection Systems, Intrusion Prevention Systems

Module 05: Endpoint Security-Windows Systems: Security of end-user devices and entry points by implying endpoint security on Windows devices.

Module 06: Endpoint Security-Linux Systems: Securing entry points or end-user devices by ensuring endpoint security on Linux devices

Module 07: Endpoint Security- Mobile Devices: Securing entry points or end-user devices by ensuring endpoint security on mobile devices

Module 08: Endpoint Security-IoT Devices: Fundamentals of IoT, IoT threats and security using endpoint security implementation

Module 09: Administrative Application Security: Understanding the methodologies of administrative application security and its importance to minimize the security-related vulnerabilities in the application

Module 10: Data Security: Implementing policies to safeguard data from unauthorized access using various techniques like encryption, hashing, tokenization and other key management practices. Concept of data storage, data classification, data masking, retention and destruction

Module 11: Enterprise Virtual Network Security: In-depth understanding of virtualization, related threats and security. Essentials of software-defined network (SDN) security, network function virtualization (NFV) security

Module 12: Enterprise Cloud Network Security: Introduction to cloud computing, threats, challenges and security across cloud platforms, concepts of container security, docker security, and Kubernetes security

Module 13: Enterprise Wireless Network Security: Understanding of wireless network security essentials, threats, attacks and countermeasures.

Module 14: Network Traffic Monitoring and Analysis: Analysis and monitoring of logs from various perimeter network devices to identify any anomalies in the traffic.

Module 15: Network Logs Monitoring and Analysis: Analyzing the events generated by various devices in the network to identify signs of any suspicious activity or a potential incident

Module 16: Incident Response and Forensic Investigation: Understanding of incident management response process and methodologies to be followed in case of security incidents. Understanding of forensics investigation techniques and tools used for analysis.

Module 17: Business Continuity and Disaster Recovery: Understanding the importance of BCP and DR, related concepts and procedures required to allow smooth functioning of operations in case of a disaster

Module 18: Risk Anticipation with Risk Management: Risk management process, analyzing various risks that the organization is susceptible to and developing policies to manage them.

Module 19: Threat Assessment with Attack Surface Analysis: Analyzing the threats and attack vectors to develop solutions for their countermeasures

Module 20: Threat Prediction with Cyber Threat Intelligence: Developing a proactive approach by understanding various frameworks aiding in threat intelligence to anticipate the kinds of attacks hackers could use to gain access to the network.

INFOSECTRAIN

sales@infosectrain.com | www.infosectrain.com