Cyber Gate
ACADEMY

EC-CND

CERTIFIED NETWORK DEFENDER COURSE

Course Overview

Certified Network Defender (CNDv2) certification is aimed at IT professionals who intend to obtain network security skills and knowledge. It focuses on creating Network Administrators who are trained in protecting, detecting, and responding to threats on the network. These certified defenders know how to devise policies and frameworks, and also understand the mechanisms of how to protect a network. They understand network technologies, traffic, performance, and network utilization, which are important in maintaining an efficient and secure network. Industries use CNDv2 certified individuals to ensure their IT infrastructure is robust and safe from network security threats.

Certified Network Defender (CNDv2) certification training is a professional course that aims to educate individuals on network defense strategies. The curriculum largely encompasses recognizing and managing vulnerabilities within a network, and implementing security measures to prevent cyber threats. The course covers a wide range of topics, which include network security controls, protocols, and devices, security policy design and implementation, perimeter security, incident response and handling, VPN and wireless security, and physical security co-ordination. This training ensures that individuals are well-versed in detecting and mitigating risks to maintain a secure network environment.

Course Duration

5 Days (40 Hours).

Target Audience

- IT professionals seeking to enhance network security skills
- Network administrators aiming to understand potential cyber threats
- Cybersecurity officers needing certification
- System administrators interested in network defense strategies
- IT security analysts requiring a comprehensive defense approach
- Network security engineers and consultants
- Individuals interested in pursuing a career in network defense.

Learning Objectives

After completing Certified Network Defender (CNDv2) certification training, an individual will gain skills in network security technologies and operations, security policies development, traffic analysis, risk identification, and incident response. They will be proficient in firewall, intrusion detection and prevention systems. They will understand the architecture of secure networks and how to create and maintain secure networks. Additionally, they will acquire knowledge in VPNs, wireless network security, and network traffic signatures and anomalies. They will also become adept at identifying and mitigating network threats and vulnerabilities.

The Certified Network Defender (CNDv2) course aims to equip students with the practical skills and theoretical knowledge required to protect, detect and respond to network attacks. Learning objectives include understanding the fundamentals of network security, familiarizing with various network security policies and protocols, mastering network data and vulnerability assessment methods, learning how to manage equipment and perform risk assessment, and gaining proficiency in creating incident response plans. The course also aims to improve students' ability to identify potential threats and vulnerabilities and devise strategies to mitigate them.

Course Content

- Module 1: Network Attacks and Defense Strategies.
- Module 2: Administrative Network Security.
- Module 3: Technical Network Security.
- Module 4: Network Perimeter Security.
- Module 5: Endpoint Security-Windows Systems.
- Module 6: Endpoint Security-Linux Systems.
- Module 7: Endpoint Security-Mobile Devices.
- Module 8: Endpoint Security-IoT Devices.
- Module 9: Administrative Application Security.
- Module 10: Data Security.
- Module 11: Enterprise Virtual Network Security.
- Module 12: Enterprise Cloud Network Security.
- Module 13: Enterprise Wireless Network Security.
- Module 14: Network Traffic Monitoring and Analysis.
- Module 15: Network Logs Monitoring and Analysis.
- Module 16: Incident Response and Forensic Investigation.
- Module 17: Business Continuity and Disaster Recovery.
- Module 18: Risk Anticipation with Risk Management.
- Module 19: Threat Assessment with Attack Surface Analysis.
- Module 20: Threat Prediction with Cyber Threat Intelligence.

Prerequisites

Attendees should meet the following prerequisites:

- Basic understanding of network security protocols.
- Knowledge of firewall configuration and IDS/IPS systems.
- Familiarity with different types of malware and security attacks.
- Understanding of VPN and wireless infrastructure securities.
- Experience in managing first response to network security incidents
- Good grasp of Windows/Linux operating systems.

Course Agenda

Day 1	Module 1: Network Attacks and Defense Strategies Module 2: Administrative Network Security Module 3: Technical Network Security Module 4: Network Perimeter Security
Day 2	Module 5: Endpoint Security-Windows Systems Module 6: Endpoint Security-Linux Systems Module 7: Endpoint Security-Mobile Devices Module 8: Endpoint Security-IoT Devices
Day 3	Module 9: Administrative Application Security Module 10: Data Security Module 11: Enterprise Virtual Network Security Module 12: Enterprise Cloud Network Security
Day 4	Module 13: Enterprise Wireless Network Security Module 14: Network Traffic Monitoring and Analysis Module 15: Network Logs Monitoring and Analysis Module 16: Incident Response and Forensic Investigation
Day 5	Module 17: Business Continuity and Disaster Recovery Module 18: Risk Anticipation with Risk Management Module 19: Threat Assessment with Attack Surface Analysis Module 20: Threat Prediction with Cyber Threat Intelligence

Technical Requirement

1. Laptop with minimum 8GB Ram.
2. Connected Monitor for iLabs.
3. Hi speed Internet Connection as All the labs it will be accessed through EC-Council Cloud.

Exam Voucher Validity

It will be valid for 12month starting from the last day of the course.

Certification Expiry

It will be valid for 3 years.

CyberGate
ACADEMY

YOUR TRUSTED DEFENDERS

ADDRESS

CyberGate Academy
ADPOLY, MBZ City

WEB

academy@cybergate.tech
training@cybergate.tech