Certified Network Defender (CND) Certification Training

Course: **00054**
Filter: **Beginner**
Duration: **5 days**
Category:: **Systems & Network Security**
Price: **2000,00 €**

About Course

In this Certified Network Defender (CND) training course, you will get prepped to pass the EC-Council CND 312-38 exam and learn the tactical skills needed to design and manage a secure network. Gain a solid understanding of defensive security and hands-on capability to handle all types of network defense. You will learn to ensure data security, properly configure networking technologies, and install defensive software to enhance confidentiality, integrity, and availability. The network is the front line in the cyber security war, and network administrators need to be ready to defend it. Get certified with EC-Council's Certified Network Defender (CND) certification and demonstrate you have a solid foundation of network security and the tactical expertise to secure data and build defenses in an enterprise network. Passing the CND Certification Exam meets U.S. DoD Directive 8140/8570.01 Technical (IAT) Level-I, Technical (IAT) Level-II, Management (IAM) Level-I, and CSSP Infrastructure Support. Reinforce your skills while practicing the CND exam objectives with CYBRScore Lab Bundles: Network Essentials Labs

What you'll learn

- Install, configure, and manage network security controls and devices.
- Design, implement, and monitor security policies.
- Harden hosts to secure them against intrusions.
- Implement and configure VNPs and wireless network technologies.
- Perform risk, threat, and vulnerability assessments.

Pre-requisites

- You should have the basic network and host operations knowledge and experience commensurate with one to five years of network, host, or application administration.

Curriculum

Module 1: Network Defender Fundamentals

- Classifying threats, vulnerabilities, and attacks
- Reducing risk
- Identifying and assessing measures
- Designing and implementing security policies
- Understanding the hierarchy of security policies
- Enforcing and promoting policies effectively

Module 2: Deploying Security Devices

- Configuring wireless security
- Choosing secure and scalable protocols
- Testing wireless security
- Monitoring and managing defenses
- Installing patches for hardening
- Analyzing logs

Module 3: Implementing Host Security

- Preventing malware infestations
- Hardening Systems
- Defending with antivirus and safelists
- Managing configuration
- Evaluating baselines and monitoring
- Patching and remediating hosts
- Investigating types of authentication and authorization
- Enforcing centralized access controls

Module 4: Securing the Network Perimeter

- Restricting access with a firewall
- Designing the DMZ
- Implementing deep inspection and filters
- Encrypting data with a VPN
- Selecting secure protocols
- Authenticating encryption endpoints

Module 5: Responding to Incidents

- Monitoring traffic
- Deploying IDS and IPS
- Examining forensic artifacts
- CND On-Demand Course Outline
- Network Defender Fundamentals
- Classifying threats, vulnerabilities, and attacks
- Reducing risk
- Identifying and assessing measures
- Designing and implementing security policies
- Understanding the hierarchy of security policies
- Enforcing and promoting policies effectively
- Deploying Security Devices
- Configuring wireless security
- Choosing secure and scalable protocols
- Testing wireless security
- Monitoring and managing defenses
- Installing patches for hardening
- Analyzing logs
- Implementing Host Security
- Preventing malware infestations
- Hardening Systems
- Defending with antivirus and safelists
- Managing configuration
- Evaluating baselines and monitoring
- Patching and remediating hosts

- Investigating types of authentication and authorization
- Enforcing centralized access controls
- Securing the Network Perimeter
- Restricting access with a firewall
- Designing the DMZ
- Implementing deep inspection and filters
- Encrypting data with a VPN
- Selecting secure protocols
- Authenticating encryption endpoints
- Responding to Incidents
- Monitoring traffic
- Examining forensic artifacts