Ec-Council-Certified Network Defender (CND)

Certificate: Ec-council-Certified Network Defender (CND)	Accreditor: EC-Council
Duration: 5 Days	Language: English
Course Delivery: Classroom	

Overview:
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 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.
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 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.

Who Should Attend?

Network Administrators, Network security Administrators, Network Security Engineer, Network Defense Technicians, CND Analyst, Security Analyst and Security Operator, Anyone who involves in network operations

Exam Information:

The CND certification exam will be conducted on the last day of training. Students need to pass the online ECC exam 312-38 to receive the CND certification.

Course 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.