JCC كلية المجتمع بجدة
Jeddah Community College

King Abdulaziz University

CND
Certified Network Defender

Certified Network Defender

Certificate: Certified Network Defender	**Accreditor:** EC-Council
Duration: 5 Days (9:00 AM – 5:00 PM)	**Language:** English
Course Delivery: Classroom	**Credits:** N/A

Course Description:

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.

Audience:
This course will significantly benefit Network Administrators, Network Defense Technicians, Network Engineers, Security Analysts, Security Operators, Network Defender Analysis or anyone involved in network operations.

Aftab Alam
CEHv9, CCNA, CNE, MCP

Learning Objectives:

Individuals certified at this level will be able to understand:

- Design and implement the network security policies and procedures
- Troubleshoot their network for various network problems
- Identify various threats on an organization’s network
- Determine and implement various physical security controls for their organizations
- Harden the security of various individual hosts in the organization’s network
- Select an appropriate firewall solution, topology, and configuration to harden security through the firewall
- Determine the appropriate location for IDS/IPS sensors, tuning IDS for false positives and false negatives, and configurations to harden security through IDPS technologies
- Implement a secure VPN implementation for their organization
- Identify various threats to a wireless network and mitigate them
- Maintain the inventory of computers, servers, terminals, modems and other access devices
- Provide security awareness guidance and training
- Manage, assign, and maintain the list of network addresses
- Perform a risk assessment, vulnerability assessment/scanning through various scanning tools and generate detailed reports
- Identify the critical data, choose an appropriate back up method, media and technique to perform a successful backup of an organization’s data on a regular basis
- Provide first response to a network security incident and assist the IRT team and forensics investigation team in dealing with an incident
- Add, remove, or update user account information
- Apply operating system updates, patches and make configuration changes
- Update system configurations to maintain an updated security posture using current patches, device and operating system hardening techniques, and Access Control Lists.
- Manage network Authentication, Authorization, Accounting (AAA) for network devices
- Monitor and ensure the security of the network traffic
- Manage Proxy and Content filtering
- Review audit logs from the Firewall, IDS/IPS, servers and hosts on the internal, protected network
- Analyze, troubleshoot, and investigate security-related, information system’s anomalies based on the security platform

- Maintain, configure, and analyze network and host-based security platforms
- Use File integrity verification and monitoring solutions
- Implement Network Access Control (NAC)
- Implement Data Loss Prevention (DLP) solutions
- Evaluate security products as well as security operations procedures and processes.
- Manage and maintain Windows Security Administration
- Manage and maintain Linux Security Administration
- Harden Routers and Switches

Benefits of Taking This Course:

- The course covers all three approaches to network security, i.e. PREVENTIVE, REACTIVE and RETROSPECTIVE
- The course validates your security skills across a wide range of network security domains at an intermediate level
- The course adds weight to your resume, increases your employability and helps you stay a step ahead of the crowd

Prerequisites:

You should have fundamental knowledge of networking concepts.

Follow-on Courses:

- Certified Ethical Hacker (CEH)
- Computer Hacking Forensic Investigator (CHFI)
- EC-Council Certified Security Analyst/Licensed Penetration Tester (ECSA/LPT)

Course Materials:

As part of this course, you will receive the following items:

- 2 x Courseware Books
- 1 x Lab Manual Book

Examination:

- Exam Format: Web-Based
- Questions: 100 Interactive Multiple Choice
- Passing Score: 70%
- Exam Duration: 240 minutes
- Proctoring: Accredited Training Center (ATC)

Technical Requirements:

For eBooks:

- Internet for downloading the eBook
- Windows and Mac based systems
- Android, iOS, and Windows Phone based Tablet and Smart Phones
- Adobe Reader 10

For eLearning:

- Web Browser (IE, Mozilla, or Chrome)

Agenda:

Day 1:

Start	End	Module
9:00	9:15	Module 00: Student Introduction
9:15	10:45	Module 01: Computer Network and Defense Fundamentals
10:45	11:00	Break
11:00	12:30	Module 01: Computer Network and Defense Fundamentals
12:30	1:30	Lunch Break
1:30	2:45	Module 02: Network Security Threats, Vulnerabilities, and Attacks
2:45	3:15	Break
3:15	5:00	Module 03: Network Security Controls, Protocols, and Devices

Day 2:

Start	End	Module
9:00	10:45	Module 04: Network Security Policy Design and Implementation
10:45	11:00	Break
11:00	12:30	Module 05: Physical Security
12:30	1:30	Lunch Break
1:30	2:45	Module 06: Host Security
2:45	3:15	Break
3:15	5:00	Module 06: Host Security

Day 3:

Start	End	Module
9:00	10:45	Module 07: Secure Firewall Configuration and Management
10:45	11:00	Break
11:00	12:30	Module 07: Secure Firewall Configuration and Management
12:30	1:30	Lunch Break
1:30	2:45	Module 08: Secure IDS Configuration and Management

2:45	3:15	Break
3:15	5:00	Module 08: Secure IDS Configuration and Management

Day 4:

Start	End	Module
9:00	10:45	Module 09: Secure VPN Configuration and Management
10:45	11:00	Break
11:00	12:30	CND Module 10 Wireless Network Defense
12:30	1:30	Lunch Break
1:30	2:45	Module 11: Network Traffic Monitoring and Analysis
2:45	3:15	Break
3:15	5:00	Module 11: Network Traffic Monitoring and Analysis

Day 5:

Start	End	Module
9:00	10:45	Module 12: Network Risk and Vulnerability Management
10:45	11:00	Break
11:00	12:30	Module 13: Data Backup and Recovery
12:30	1:30	Lunch Break

1:30	**2:45**	**Module 14: Network Incident Response and Management**
2:45	**3:15**	**Break**
3:15	**7:25**	**CND Exam(Optional)**

For more information and enrolment to this course, kindly contact
Aftab Alam
205-Cisco Lab,2nd Floor,
CIT Dept , Jeddah Community College
King Abdulaziz University
Email: aabdussami@kau.edu.sa Mobile: 056 11 77861