THINQTANK® LEARNING

EC-COUNCIL CERTIFIED NETWORK DEFENDER v2.0

Exam 312-38

Our Learning Exclusive

- Custom exam prep software and materials
- Exam delivery in classroom with 98% success
- Course specific thinQtank® Learning publications to promote fun exciting learning
- Extended hours of training including immersive hands-on exercises
- WE DO NOT "TEACH THE TEST" We always deliver valuable hands-on experience
- Receive all reading material and study guides when you register
- All courses taught by certified expert engineers

Course Duration

- Five days of instructor-led learning
- 60% lecture, 40% hands-on labs/demonstrations

Prerequisites

- You should be well-versed in cyber security fundamentals.

Target Audience

- System administrators
- System engineers
- Firewall administrators
- Network managers
- IT managers
- IT professionals
- Anyone interested in network security technologies
- Managers who want to understand cyber security core principles and practices
- Operations personnel, who although do not have security as their primary job function, will need an understanding of cyber security core principles and practices

Exam Information

- 312-38 – Certified Network Defender (CND v2.0)

Delivery Methods

- Instructor-Led Training
- Immersive Live-Online Training
- On-Site and Custom Delivery

Exclusive Tools and Learning Package

- Comprehensive video training package
- Virtual Debian-derived distribution package with tools and utilities for digital forensics
- 80 Complex Labs during the course
- 6 months access to EC-Council virtual lab environment for CND

Course Overview

thinQtank® Learning is offering a unique five-day training camp comprised of five days of instructor-led learning for Certified Network Defender. As with all our Cisco Training Experiences – exams are delivered in the classroom.

Learn about hackers and cyber defense strategies required in today's critical infrastructure. EC-Council has reviewed the entire CND space as designated by the Department of Defense as IAT I, II, III and IAM I, II, III as well as the NICE Framework KSA's as they relate to cyber defense and day-to-day cyber operations. With each of these considered, they built their exam blueprint, overall training scope, and got to work building the next certification we believe will be a game changer for cyber security professionals – Certified Network Defender.

The class is a professional level introduction to the cyber defense strategies needed in today's critical infrastructure. Certified Network Defender v2 has been designed by industry experts to help IT Professionals play an active role in the Protection of digital business assets and Detection and Response to Cyber Threats, while leveraging Threat Intelligence to Predict them before they happen. CND is a network security course designed to help organizations create and deploy the most comprehensive network defense system.

Course Objectives

This course will help students learn:

- Network security management
- Network security policies and procedures
- Windows and Linux security administration
- Mobile and IoT device security
- Data security techniques
- Virtualization technology security
- Cloud and wireless security
- Risk assessment tools
- Basics of first response and forensics
- Indicators of Compromise, Attack, and Exposures (IoC, IoA, IoE)
- Threat intelligence capabilities
- Log management
- Endpoint security
- Firewall solutions
- IDS/IPS technologies
- Network Authentication, Authorization, Accounting (AAA)

thinQtank® LEARNING

Does it Benefit You?

According to LinkedIn's 2020 Emerging Jobs Report, Network Defender jobs are in high demand. Globally, Network Administrators and Engineers are adding significant value to their jobs and salary by learning critical network security and network defense skills.

The following individuals can consider EC-Council's Network Security Certifications as the next move in their career:

- Cisco or Microsoft Certified Network Administrator/Engineers
- Wireshark Certified Network Analyst
- SolarWinds Certified Professional
- Juniper Certified Network Professional
- Professionals with Comptia's Network+/Security+ Certification
- University professors who are teaching cybersecurity courses
- IT professionals planning a career transition
- Learners who wish to start a career in cybersecurity

Individuals who complete the CND v2 cybersecurity course qualify for the following entry-level job roles:

- Entry-level Network Administrators
- Entry-level Network Security Administrators
- Data Security Analyst
- Junior Network Security Engineer
- Junior Network Defense Technician
- Security Analyst
- Security Operator

The end goal of Certified Network Defender (CND v2) is to help Blue Teams defend and win the war against network breaches. The program is the ideal cyber defense course for organizations and individuals for the following reasons:

- Based on Common Job Role frameworks recognized by organizations around the world.
- ANSI/ISO/IEC 17024 accredited Certification Program.
- Mapped to the NICE 2.0 framework.
- Focuses on latest technologies including Cloud, IoT, Virtualization and Remote Worker Threats, Attack Surface Analysis, Threat Intelligence, Software Defined Networks (SDN), and Network Function Virtualization (NFV), as well as docker, Kubernetes, and container security.
- Covers the latest tools, techniques, and methodologies used by top cybersecurity experts around the world.

Build Your Career

YOUR PATHWAY TO A CAREER IN A BLUE TEAM

- The Protect, Detect, Respond, and Predict approach defines the job roles for a Blue Team Security Professional. One can continue their career as a Network Defender or later transition into a niche job profile as CND v2 covers a base understanding of Blue Teams.

MOBILE & IOT SECURITY DEFENSE

- The first certification program to offer device and enterprise level security for its students. Career changers planning a move into cybersecurity will also benefit from this.

TACTICAL DEFENSE OF CLOUD SERVICES

- Learn different ways to ensure security across various cloud platforms — Amazon Web Services, Microsoft Azure Cloud, and Google Cloud Platform.

LEARNING BEYOND TECHNICAL ASPECTS

- CND v2 is the only certification program that offers a chance to learn beyond the technological aspects of network security. The module has a strong focus on the strategical domain with special attention to adaptive & defense in depth security, framing network policies, achieving compliance, and the operational domain to learn the implementation of the above decisions.

BUILDING PERIMETER DEFENSE SKILLS

- CND v2 puts the spotlight on perimeter defense as the latest technologies have made networks too complex for everyone. Perimeter defense can help with modern security requirements.

80 COMPLEX LABS

- The only program that gives a chance to students to learn under simulated threat environments and gain real-world skills before they start their professional career.

Course Modules and Labs

- Module 01: Network Attacks and Defense Strategies
- Module 02: Administrative Network Security
- Module 03: Technical Network Security
- Module 04: Network Perimeter Security
- Module 05: Endpoint Security-Windows Systems
- Module 06: Endpoint Security-Linux Systems
- Module 07: Endpoint Security- Mobile Devices
- Module 08: Endpoint Security-IoT Devices
- Module 09: 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

- Exercise 1-1: Understanding the Workings of SQL Injection Attacks
- Exercise 1-2: Understanding the Workings of XSS Attacks
- Exercise 1-3: Understanding the Workings of Network Scanning Attacks
- Exercise 1-4: Understanding the Workings of Brute-Force Attacks
- Exercise 2-1: Implementing Password Policies Using Windows Group Policy
- Exercise 2-2: Implementing Password Policies in Linux
- Exercise 2-3: Monitoring Activities on a Remote User System
- Exercise 3-1: Implementing Just Enough Administration to Secure Privileged Access
- Exercise 3-2: Implementing Role-Based Access Control using Windows Admin Center
- Exercise 4-1: Implementing Network-Based Firewall Functionality: Blocking Unwanted Website access using pfSense Firewall
- Exercise 4-2: Implementing Network-Based Firewall Functionality: Blocking Insecure Ports using pfSense Firewall
- Exercise 4-3: Implementing Network-Based Firewall Functionality: Blocking Internal FTP Server Access Using Smoothwall Firewall
- Exercise 4-4: Implementing Host-ba sed Firewall Functionality Using Windows Firewall
- Exercise 4-5: Implementing Host-based Firewall Protection with iptables
- Exercise 4-6: Implementing Network-based IDS Functionality Using Suricata IDS
- Exercise 4-7: Implementing Host-based IDS functionality using Wazuh HIDS
- Exercise 5-1: Basic Network Administration and Troubleshooting Using Windows Command-Line Utilities
- Exercise 5-2: Securing Windows File Share in Active Directory
- Exercise 5-3: Analyzing Security Configuration Baseline Using Microsoft Security Compliance Toolkit in Windows
- Exercise 5-4: Remote Patch Management using BatchPatch
- Exercise 5-5: Remote Patch Management using ManageEngine Patch Manager Plus
- Exercise 5-6: Delegating Admin Permission to User Using Delegation of Control Wizard
- Exercise 5-7: Securing Local Administrator Password using LAPS
- Exercise 6-1: Implementing Linux Security Best Practices
- Exercise 7-1: Implementing Enterprise Mobile Security Using Miradore MDM Solution
- Exercise 8-1: Securing IoT Device Communication Using TLS/SSL
- Exercise 9-1: Implementing Application Whitelisting Using AppLocker
- Exercise 10-1: Encrypting Data at Rest Using VeraCrypt
- Exercise 10-2: Implementing Encryption on SQL Server Database using Transparent Database Encryption Method
- Exercise 10-3: Implementing Always Encrypted in SQL Server
- Exercise 10-4: Encrypting Data in Transit Using SSL
- Exercise 10-5: Ensuring Secure Email Communication using PGP
- Exercise 10-6: Performing Data Backup Using AOMEI Backupper Standard
- Exercise 10-7: File Recovery Using EaseUS Data Recovery Wizard
- Exercise 10-8: File Recovery Using Kernel for Windows Data Recovery Tool
- Exercise 10-9: Partition Recovery Using MiniTool Power Data Recovery Tool

Course Labs Continued

- Exercise 11-1: Auditing Docker Host Security Using Docker-Bench-Security Tool
- Exercise 11-2: Securing SDN Communication Between Switch and SDN Controller Using SSL
- Exercise 12-1: Implementing Amazon Web Services Identity and Access Management
- Exercise 12-2: Implementing Key Management Services in Amazon Web Services
- Exercise 12-3: Securing Amazon Web Services Storage
- Exercise 13-1: Configuring Security on a Wireless Router
- Exercise 14-1: Capturing Network Traffic using Wireshark
- Exercise 14-2: Analyzing and Examining Various Network Packet Headers using Wireshark
- Exercise 14-3: Analyzing and Examining Various Network Packet Headers in Linux using tcpdump
- Exercise 14-4: Applying Various Filters in Wireshark
- Exercise 14-5: Detecting Clear-Text Traffic using Wireshark
- Exercise 14-6: Monitoring and Detecting Network Reconnaissance Attempts
- Exercise 14-7: Detecting Brute-Force Attempt Using Wireshark
- Exercise 14-8: Detecting SQL Attack using Wireshark
- Exercise 14-9: Network Traffic Monitoring using PRTG
- Exercise 14-10: Network Traffic Analysis Using Capsa
- Exercise 14-11: Network Traffic Bandwidth Monitoring - NTOP in pfSense
- Exercise 15-1: Configuring, Viewing, and Analyzing Windows Event Logs
- Exercise 15-2: Configuring, Viewing, and Analyzing IIS Logs
- Exercise 15-3: Configuring, Viewing, and Analyzing Logs in a Centralized Location Using Splunk
- Exercise 15-4: Identifying Suspicious Activities Using Log Monitoring and Analysis
- Exercise 16-1: Working with Incident Tickets in OSSIM
- Exercise 17-1: Implementing Business Continuity and Disaster Recovery Using NLB
- Exercise 18-1: Vulnerability Management using OSSIM
- Exercise 18-2: Vulnerability Analysis Using the Nessus
- Exercise 18-3: Network Vulnerabilities Scanning Using GFI LanGuard
- Exercise 18-4: Auditing the Network Security with Nsauditor
- Exercise 18-5: Application Vulnerability Scanning using OWASP ZAP
- Exercise 19-1: System Attack Surface Analysis using Windows Attack Surface Analyzer
- Exercise 19-2: Analyzing Web Application Attack Surface using OWASP Attack Surface Detector (ZAP Plugin)
- Exercise 19-3: Attack Surface Mapping and Visualizing using Amass
- Exercise 20-1: Integrating OTX Threat Feeds in OSSIM

THINQTANK® LEARNING

EC-COUNCIL CERTIFIED NETWORK DEFENDER v2.0

Exam 312-38

thinQtank® Global, Inc. dba thinQtank® Learning P.O. Box 803215, Valencia, CA 91380 USA
Tel 855-TO-THINQ Fax 208-979-0668 www.thinqtanklearning.com

thinQtank Global, Inc. warrants that it will perform these training services in a reasonable manner using generally accepted industry standards and practices. THE EXPRESS WARRANTY SET FORTH IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICES AND DELIVERABLES PROVIDED BY THINQTANK GLOBAL, INC., OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM. THINQTANK GLOBAL, INC. WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO CUSTOMER. All materials provided in this training are copyrighted by thinQtank Global, Inc. ("Learning Materials"). thinQtank Global, Inc. grants the customer of this learning a license to use Learning Materials strictly for the purpose of facilitating such company's internal understanding, utilization and operation of the technology covered herein. Except as set forth expressly in the sentence above, there is no transfer of any intellectual property rights or any other license granted under the terms of this training.