Certified Network Defense Architect (CNDA)

Course Overview

The Certified Network Defense Architect (CNDA) Program, also called the Certified Ethical Hacker (CEH) Program, certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. A Certified Network Defense Architect is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems, and uses the same knowledge and tools as a malicious hacker.

Course Specifications

Course number: ECCEH41
Course length: 5 days

Target Student

This certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

Prerequisites

A Certified Network Defense Architect candidate should have at least two years of information technology security experience, a strong working knowledge of TCP/IP, and a basic familiarity with Linux.

Delivery Method

Instructor-led, group-paced, classroom-delivery learning model with structured minds-on and hands-on activities.

Benefits

This class will immerse students into an interactive environment where they will be shown how to scan, test, and secure their own systems. The lab-intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems.

Students will begin by understanding how perimeter defenses work and then be led into scanning and attacking their own networks. Students then learn how intruders escalate privileges, and examine what steps can be taken to secure a system. Students will also learn about intrusion detection, policy creation, social engineering, open source intelligence, incident handling, and log interpretation.

Course Objectives

- Developing the hacker's mind
- Network surveying
- Port scanning
- System identification/OS fingerprinting
- Vulnerability research and verification
- Service identification
- Internet application testing
- Document grinding
- Recognizing security issues within an organization
- Performing legal assessments on remote/foreign networks
- Examining an organization for weaknesses as through the eyes of an industrial spy or a competitor
- Implementing the right tools for each task of the Methodology
- Competitive Intelligence
- Exploiting vulnerabilities remotely
- Examining appropriate countermeasures to thwart malicious hacking

503.520.0555
www.KineticOregon.com

9225 SW Nimbus Avenue
Beaverton OR 97008

1001 SW Fifth Avenue, Suite 305
Portland, OR 97204

Course Outline

Day 1
- Module 1: Ethics and Legal Issues
- Module 2: Footprinting
- Module 3: Scanning

Day 2
- Module 4: Enumeration
- Module 5: System Hacking

Day 3
- Module 6: Trojans and Backdoors
- Module 7: Sniffers
- Module 8: Denial-of-Service
- Module 9: Social Engineering

Day 4
- Module 10: Session Hijacking
- Module 11: Hacking Web Servers
- Module 12: Web Application Vulnerabilities
- Module 13: Web-Based Password Cracking Techniques
- Module 14: SQL Injection

Day 5
- Module 15: Hacking Wireless Networks
- Module 16: Viruses and Worms
- Module 17: Physical Security
- Module 18: Hacking Linux
- Module 19: IDS, Firewalls and Honeypots,
- Module 20: Buffer Overflows
- Module 21: Cryptography
- Module 22: Penetration Testing Methodologies (Self-Study)

Conduct the CEH exam (312-50) on the last day of class (Friday).

503.520.0555
www.KineticOregon.com

9225 SW Nimbus Avenue
Beaverton OR 97008

1001 SW Fifth Avenue, Suite 305
Portland, OR 97204