C)VA

Duration: *3 Day(s)*

Course Overview

The vendor neutral Certified Vulnerability Assessor certification course helps students understand the importance of vulnerability assessments by providing intricateknowledge and skills in the Vulnerability Assessment arena. The CVA course provides foundational knowledge of general VA tools as well as popular exploits an IT engineer should be familiar with. The CVA is a fundamental cyber security certification course that focuses on vulnerability assessments. The CVA course focuses on foundational information such as the importance of a Vulnerability Assessment and how it can help an engineer prevent serious break-ins to your organization. In the CVA course, the student will be versed with basic malware and viruses and how they can infiltrate an organizations network. The student will also learn how to assess a company's security posture and perform a basic vulnerability test to help secure the organization's networking infrastructure. **Mile2 Accreditations:**

1. Accredited by the **NSA CNSS 4011-4016**
2. Is approved and has been placed on Homeland Security's National Initiative for Cyber Security Careers and Studies (**NICCS) training providers** and maps to the **National Cybersecurity Workforce Framework**
3. Preferred cyber certification for the **FBI**

Review this course online at https://www.alta3.com/courses/C)VA

Objectives

- Understand the fundamentals and importance of vulnerability assessments.
- Implement and conduct basic vulnerability tests to secure network infrastructures.
- Recognize and analyze different types of vulnerabilities and exploits.
- Utilize core vulnerability assessment tools effectively.

Who Should Attend

- Information System Owners
- Analysts
- Ethical Hackers
- Cyber Security Managers
- IT Engineers

Prerequisites

Basic networking understanding

Course Outline

Module 1 - Why Vulnerability Assessment?

1. Overview of Vulnerability Assessment
2. Vulnerability Assessment Methodology
3. Risk Management
4. Policy Review Methods

Module 2 - Vulnerability Types

5. Critical Vulnerability Types
6. Information Leaks and Disclosures
7. Denial of Service
8. Best Practices

Module 3 - Assessing the Network

9. Network Security Assessment
10. Footprinting Tools and Techniques
11. NMAP Scans and Analysis

Module 4 - Assessing Web Servers

12. Web Server Fingerprinting
13. SQL Injection and Web Vulnerabilities
14. Cross-Site Scripting (XSS)

Module 5 - Assessing Remote VPN Services

15. Remote Information Services
16. VPN Protocols and Services
17. Assessing Remote Maintenance Services

Module 6 - Vulnerability Tools of the Trade

18. Vulnerability Scanners and Tools
19. Patch Management Options

Module 7 – Output Analysis

20. Security Alerts and Research
21. Reporting and Results Analysis