Description:



Mile2's Vulnerability Assessor course, C)VA provides an solid understanding of the tools an IT engineer needs to review an Information System. In this course, you will learn the importance of vulnerability assessments and how they are used to prevent serious cyber break-ins. Lessons include understanding malware and viruses and how they can infiltrate an organization's network. After you take this course, you will be able to assess a company's security posture and perform a basic vulnerability test. Plus, you will be able to generate reports to guide new security implementation.

Key Course Information

* Information System Owners
* Analysts
* Ethical Hackers
* ISSOs
* IT Engineers
* Cyber Security Managers

**Live Class Duration:** 3 Days

**CEUs:** 24

**Language:** English

**Class Formats Available:**

Instructor Led

Self-Study

Live Virtual Training

**Suggested Prerequisites:**

* Basic Networking Understanding

**Module 1** -Why Vulnerability Assessment

**Module 2** -Vulnerability Types

**Module 3** -Assessing the Network

**Module 4** -Assessing Web Servers and Applications

**Module 5** -Assessing Remote and VPN Services

**Module 6** - Vulnerability Assessments & Tools of the Trade

**Module 7** -Output Analysis

LABS  
**Lab 1** -Intro to Common Vulnerability Exposures   
**Lab 2** -Drafting Incident Response Procedures  
**Lab 3** -Patch Management Architecture  
**Lab 4** -Operations   
**Lab 5** -Patch Management   
**Lab 6** – Installing Nessus and Conducting a Vulnerability Scan **Lab 7** -Generating Metrics on a Security Report

Modules/Lessons

Who Should Attend







Accreditations

Logo

Description automatically generated

Upon Completion

**Question:** Do I have to purchase a course to buy a certification exam?

Answer: No

**Question:** Do all Mile2 courses map to a role-based career path?

Answer: Yes. You can find the career path and other courses associated with it at [www.mile2.com](http://www.mile2.com).

**Question:** Are all courses available as self-study courses?

Answer: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

**Question:** Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams are not meant to be shared or transferred.

The Certified Vulnerability Assessor exam is taken online through Mile2’s Learning Management System and is accessible on you Mile2.com account.

A minimum grade of 80% is required for certification.

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

1. Pass the most current version of the exam for your respective existing certification
2. Earn and submit 20 CEUs per year in your Mile2 account.

Upon completion, the Certified Vulnerability Assessor candidate will be able to competently take the C)VA exam.

Course FAQ’s

Exam Information

Course and Certification Learning Options





Graphical user interface, application

Description automatically generated

Re-Certification Requirements

DETATILED OUTLINE

1. Why Vulnerability Assessment
2. What is a Vulnerability Assessment?
3. Examination
4. Benefits of a Vulnerability Assessment
5. What are Vulnerabilities?
6. Compliance and Project Scoping
7. The Project Overview Statement
8. Assessing Current Network Concerns
9. Network Vulnerability Assessment Methodology
10. Risk Management
11. What is the Value of an Asset?
12. Types of Policy
13. Vulnerability Types
14. Vulnerability Severity and Critical Vulnerabilities
15. Information Leaks
16. Denial of Service and Best Practices
17. Introduction to Patch Management
18. What is Patch Management?
19. Different Types of Patches
20. Why Patch Management is Necessary
21. Patch Management Process
22. Patch Management Program Challenges
23. Timing, Prioritization, and Testing
24. Patch Management Configuration
25. Alternative Host Architectures
26. Other Challenges
27. Patch Management Technologies
28. Components and Architecture
29. Security Capabilities
30. Management Capabilities
31. Vulnerability Assessment Tools of the Trade
32. Types of Vulnerability Scanners
33. Cyber Vulnerability Assessment Tools
34. Metrics
35. Vulnerability Severity
36. Reportable Vulnerabilities
37. Readability Factor
38. Tool Output and Data Provided
39. Compliance Audits