Cyber Security Training & Consulting

C)VA™ Certified Vulnerability Assessor

# CERTIFIED VULNERABILITY ASSESSOR

## KEY DATA

**Course Title:** C)VA

**Duration:** 2 days

**CPE Credits:** 16

**Class Format Options:**

Instructor-led Classroom
Live Virtual Training

**Who Should Attend:**

IT Professionals

**Prerequisites:**

An Interest In Security

**Provided Materials:**

Student Workbook

**Certification Exam:**

C)VA: Certified Vulnerability Assessor

**Certification Track:**

C)VA: Certified Vulnerability Assessor

C)PTE: Certified Penetration Testing Engineer

C)PTC: Certified Penetration Testing Consultant

## COURSE OVERVIEW

The Certified Vulnerability Assessor course trains students to be proficient in conducting vulnerability assessments by:

1. Teaching the risk associated with information technology and why a vulnerability assessment is crucial to the continuing operations of a business.



2. Preparing students with the tools and knowledge of how to perform a vulnerability assessment.

3. Instructing students on how to summarize and report on their findings from a vulnerability assessment.

This is accomplished by having students perform in-depth labs that focus recognizing prominent threats with industry proven tools, learn our proven methodology by using real world examples, and study what vulnerabilities hackers look for when trying to hack into systems. After completing the course, students will be able to sit for the Certified Vulnerability Assessor exam. Upon passing the exam, students will be able to use the C)VA certification.

## UPON COMPLETION

Students will:

- Have knowledge to detect security vulnerabilities and risk.
- Have knowledge to accurately report on their findings from examinations
- Be ready to sit for the C)VA Exam

## EXAM INFORMATION

The Certified Vulnerability Assessor exam is taken online through Mile2's Assessment and Certification System (MACS), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple choice questions. The cost is $300 USD and must be purchased from the store on Mile2.com.

## COURSE CONTENT

**Module 1:** Why Vulnerability Assessment
**Module 2:** Vulnerability Types
**Module 3:** Assessing the Network
**Module 4:** Assessing Web Servers & Applications
**Module 5:** Assessing Remote & VPN Services
**Module 6:** Vulnerability Assessment Tools
**Module 7:** Output Analysis

## DETAILED MODULE DESCRIPTION

### Module 1 - Why Vulnerability Assessment

Overview
What is a Vulnerability Assessment?
Vulnerability Assessment
Benefits of a Vulnerability Assessment
What are Vulnerabilities?
Security Vulnerability Life Cycle
Compliance and Project Scoping
The Project Overview Statement
Project Overview Statement
Assessing Current Network Concerns
Vulnerabilities in Networks
More Concerns
Network Vulnerability Assessment Methodology
Network Vulnerability Assessment Methodology
Phase I: Data Collection
Phase II: Interviews, Information Reviews, and Hands-On Investigation
Phase III: Analysis
Analysis cont.
Risk Management
Why Is Risk Management Difficult?
Risk Analysis Objectives
Putting Together the Team and Components
What Is the Value of an Asset?
Examples of Vulnerabilities that Are Not Obvious
Categorizing Risks
Some Examples of Types of Losses
Different Approaches to Analysis
Who Uses What?
Qualitative Analysis Steps
Quantitative Analysis
ALE Values Uses
ALE Example
ARO Values and Their Meaning
ALE Calculation
Can a Purely Quantitative Analysis Be Accomplished?
Comparing Cost and Benefit
Countermeasure Criteria
Calculating Cost/Benefit
Cost of a Countermeasure
Can You Get Rid of All Risk?
Management's Response to Identified Risks
Liability of Actions
Policy Review (Top-Down) Methodology
Definitions
Policy Types
Policies with Different Goals
Industry Best Practice Standards
Components that Support the Security Policy
Policy Contents
When critiquing a policy
Technical (Bottom-Up) Methodology
Review

### Module 2 - Vulnerability Types

Overview
Critical Vulnerabilities
Critical Vulnerability Types
Buffer OverFlows
URL Mappings to Web Applications
IIS Directory Traversal
Format String Attacks
Default Passwords
Misconfigurations
Known Backdoors
Information Leaks
Memory Disclosure
Network Information
Version Information
Path Disclosure
User Enumeration
Denial of Service
Best Practices
Review
Lab

### Module 3 - Assessing the Network

Overview
Network Security Assessment Platform
Virtualization Software
Operating Systems
Exploitation Frameworks
Internet Host and Network Enumeration
Querying Web & Newsgroup Search Engines
Footprinting tools
Blogs & Forums
Google Groups/USENET
Google Hacking
Google and Query Operators
Google (cont.)
Domain Name Registration
WHOIS
WHOIS Output
BGP Querying
DNS Databases
Using Nslookup
Dig for Unix / Linux
Web Server Crawling
Automating Enumeration
SMTP Probing
SMTP Probing cont.
NMAP: Is the Host on-line
ICMP Disabled?

NMAP TCP Connect Scan
TCP Connect Port Scan
Nmap (cont.)
Tool Practice : TCP half-open & Ping Scan
Half-open Scan
Firewalled Ports
NMAP Service Version Detection
Additional NMAP Scans
NMAP UDP Scans
UDP Port Scan
Null Sessions
Syntax for a Null Session
SMB Null Sessions & Hardcoded Named Pipes
Windows Networking Services Countermeasures
Review

## Module 4 - Assessing Web Servers

Web Servers
Fingerprinting Accessible Web Servers
Assessing Reverse Proxy Mechanisms
Proxy Mechanisms
Identifying Subsystems and Enabled Components
Basic Web Server Crawling
Web Application Technologies Overview
Web Application Profiling
HTML Sifting and Analysis
Active Backend Database Technology Assessment
Why SQL “Injection”?
Web Application Attack Strategies
Web Application Vulnerabilities
Authentication Issues
Parameter Modification
SQL Injection: Enumeration
SQL Extended Stored Procedures
Shutting Down SQL Server
Direct Attacks
SQL Connection Properties
Attacking Database Servers
Obtaining Sensitive Information
URL Mappings to Web Applications
Query String
Changing URL Login Parameters
URL Login Parameters Cont.
IIS Directory Traversal
Cross-Site Scripting (XSS)
Web Security Checklist
Review

## Module 5 - Assessing Remote VPN Services

Assessing Remote & VPN Services
Remote Information Services
Retrieving DNS Service Version Information
DNS Zone Transfers
Forward DNS Grinding
Finger
Auth
NTP
SNMP
Default Community Strings
LDAP
rwho
RPC rusers
Remote Maintenance Services
FTP
SSH
Telnet
X Windows
Citrix
Microsoft Remote Desktop Protocol
VNC
Assessing IP VPN Services
Microsoft PPTP
SSL VPNs
REVIEW

## Module 6 - Vulnerability Tools of the Trade

Vulnerability Scanners
Nessus
SAINT – Sample Report
Tool: Retina
Qualys Guard
Tool: LANguard
Microsoft Baseline Analyzer
MBSA Scan Report
Dealing with Assessment Results
Patch Management Options
Review

## Module 7 – Output Analysis

Overview
Staying Abreast: Security Alerts
Vulnerability Research Sites
Nessus
SAINT
SAINT Reports
GFI Languard
GFI Reports
MBSA
MBSA Reports
Review