C)VA™ Certified Vulnerability Assessor

mile2® CYBER SECURITY CERTIFICATIONS

Certified Vulnerability Assessor

Course Title: Certified Vulnerability Assessor

Duration: 3Day

Language: English

Class Format Options:

Instructor-led classroom
Live Online Training

Prerequisites:

- Basic networking understanding

Student Materials:

- Student Workbook
- Student Prep Guide

CPEs: 24

WHO SHOULD ATTEND?

- Information System Owners
- Analysts
- Ethical Hackers
- ISSO's
- Cyber Security Managers
- IT Engineer

COURSE BENEFITS

The vendor neutral Certified Vulnerability Assessorcertification course helps students understand the importance of vulnerability assessments byproviding intricate knowledge and skills in the Vulnerability Assessmentarena. 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.

Pen Testing Hacking Career

C)VA™ Certified Vulnerability Assessor *

C)PEH™ CERTIFIED PROFESSIONAL ETHICAL HACKER

C)PTE™ CERTIFIED PENETRATION TESTING ENGINEER

C)PTC™ CERTIFIED PENETRATION TESTING CONSULTANT

All combos Include:

- Online Video
- Electronic Book (Workbook/Lab guide*)

  *in all technical classes only
- Exam Prep Questions
- Exam

ias™ INFORMATION ASSURANCE SERVICES · pt™ PENETRATION TESTING · dr™ DISASTER RECOVERY · gs™ GENERAL SECURITY · sc™ SECURE CODING · vbp™ VIRTUALIZATION BEST PRACTICES · ws™ WIRELESS SECURITY · cf™ COMPUTER FORENSICS

ACCREDITATIONS

is **ACCREDITED** by the **NSA CNSS 4011-4016**
Is **MAPPED** to NIST/Homeland Security NICCS's Cyber Security Workforce Framework
is **APPROVED** on the **FBI Cyber Security Certification Requirement list (Tier 1-3)**

UPON COMPLETION

Upon completion, the **Certified Vulnerability Assessor**candidate willnot only be able to competently take the CVA exam but will also be able to understand and implement a basic vulnerability assessment.

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 $400 USD and must be purchased from Mile2.com.

OUTLINE

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 of the Trade
Module 7 – Output Analysis

DETAILED OUTLINE

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 Some Vulnerabilities that Are
Not Always 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

Module3 - 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
Identifying and 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