Certified Vulnerability Assessor (CVA)

Modality: Virtual Classroom

Duration: 3 Days

About this course:

The course of Certified Vulnerability Assessor assists understudies with understanding the significance of weakness evaluations by giving unpredictable information and abilities in the Vulnerability Assessment field. The CVA course gives essential information on general VA instruments and also famous endeavors an IT specialist ought to be comfortable with.

The certification course of CVA is a fundamental cybersecurity course that targets on weakness assessments. The course of CVA aims around primary knowledge, for example, the significance of a Vulnerability Assessment and how it can enable a specialist to forestall genuine break-ins to your association. In the course of CVA, the understudy will be versed with basic viruses and malware and how they can penetrate a network of an association. Also, the learner will figure out how to asses the security posture of an organization and play out a fundamental vulnerability test to help secure the networking infrastructure of the organization.

The normal compensation for Certified Vulnerability Assessor is $63,000 every year.

Course Objective:

With the completion of this course, learners will have a working understanding of:

- Have the information to recognize security vulnerabilities and hazard
- Have information to precisely report their discoveries from assessments
- Be prepared to sit for the CVA Exam
- Benefits of a Vulnerability Assessment
- Security Vulnerability Life Cycle
- Compliance and Project Scoping
- Project Overview Statement
- The Project Overview Statement
- Vulnerabilities in Networks
- Network Vulnerability
- Assessing Current Network Concerns
- Network Vulnerability
- Assessment Methodology
- Assessment Methodology
- Web Application Profiling
- Web Application Technologies Overview
- Active Backend Database Technology Assessment
- HTML Sifting and Analysis
- Remote Information Services
- DNS Zone Transfers

- Retrieving DNS Service Version Information
- Assessing Remote & VPN Services
- Forward DNS Grinding

Audience:

This course is planned for:

The learners who know nothing about security but want to. We prescribe this course for any individual who needs to be secure on the Internet, particularly representatives on duty.

Prerequisites:

Basic Computer Experience

An interest in security

Suggested prerequisites courses:

None

Course 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

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
- 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