C)VA™
Certified Vulnerability Assessor

Certified Vulnerability Assessor™

DATOS CLAVE

Nombre del curso:

Certified Vulnerability Assessor

Duración:

2 días

Idioma:

Inglés

Formato:

* Aula con instructor

Pre-requisitos:

* Uso de la computadora

Material el estudiante:

* Libro de Ejercicios

BENEFICIOS DEL CURSO

El curso “Certified Vulnerability Assessor” ayuda a los estudiantes a entender la importancia de la evaluación de vulnerabilidades.

1. Brinda habilidades y conocimientos especiales en evaluaciones de vulnerabilidades.
2. Prepara al estudiante para aplicar estos conocimientos, y practicar estas habilidades en el interés de los demás.
3. Ayuda a entender la importancia de la evaluación de vulnerabilidades y como puede ayudar a prevenir importantes intromisiones a su empresa.

ESTO SE LOGRA MEDIANTE:

- Realización de laboratorios especializados escogiendo las mejores herramientas.
- Aprender una metodología usando conceptos reales.
- Dotar de conocimientos con los cuales los hackers intentan infiltrar el sistema.
- Realizar evaluaciones para probar el nivel de seguridad de la empresa, para ayudar a asegurar mejor la infraestructura contra los hackers, virus, etc.

MÓDULOS DEL CURSO

Módulo 1 - Why Vulnerability
AssessmentOverview
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
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

CNSS
gs™ GENERAL SECURITY

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

Módulo 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

Módulo 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, Hacking
Google and Query Operators
Domain Name Registration
WHOIS, WHOIS Output
BGP Querying
DNS Databases
Using Nslookup
Dig for Unix / Linux
Web Server Crawling
Automating Enumeration
SMTP Probing
NMAP: Is the Host on-line
ICMP Disabled?
NMAP TCP Connect Scan
TCP Connect Port Scan
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

Módulo 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

Módulo 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

Módulo 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

Módulo 7 – Output Analysis

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