KPMG Learning Academy

# Vulnerability Assessment Training: Protecting Your Organisation Course Outline

**Fundamentals –**

Introduction

- Defining vulnerability, exploit, threat and risk
- Creating a vulnerability report
- Conducting an initial scan
- Common Vulnerabilities and Exposure (CVE) list

Scanning and exploits

- Vulnerability detection methods
- Types of scanners
- Port scanning and OS fingerprinting
- Enumerating targets to test information leakage
- Types of exploits: worm, spyware, backdoor, rootkits, Denial of Service (DoS)
- Deploying exploit frameworks

**Analysing Vulnerabilities and Exploits –**

Uncovering infrastructure vulnerabilities

- Uncovering switch weaknesses
- Vulnerabilities in infrastructure support servers
- Network management tool attacks

Attacks against analyzers and IDS

- Identifying Snort IDS bypass attacks
- Corrupting memory and causing Denial of Service

KPMG Learning Academy

Exposing server vulnerabilities

- Scanning servers: assessing vulnerabilities on your network
- Uploading rogue scripts and file inclusion
- Catching input validation errors
- Performing buffer overflow attacks
- SQL injection
- Cross–Site Scripting (XSS) and cookie theft

Revealing desktop vulnerabilities

- Scanning for desktop vulnerabilities
- Client buffer overflows
- Silent downloading: spyware and adware
- Identifying design errors

**Configuring Scanners and Generating Reports –**

Implementing scanner operations and configuration

- Choosing credentials, ports and dangerous tests
- Preventing false negatives
- Creating custom vulnerability tests
- Customising Nessus scans
- Handling false positives

Creating and interpreting reports

- Filtering and customising reports
- Interpreting complex reports
- Contrasting the results of different scanners

KPMG Learning Academy

**Assessing Risks in a Changing Environment –**

Researching alert information

- Using the National Vulnerability Database (NVD) to find relevant vulnerability and patch information
- Evaluating and investigating security alerts and advisories
- Employing the Common Vulnerability Scoring System (CVSS)

Identifying factors that affect risk

- Evaluating the impact of a successful attack
- Determining vulnerability frequency
- Calculating vulnerability severity
- Weighing important risk factors
- Performing a risk assessment

**Managing Vulnerabilities –**

The vulnerability management cycle

- Standardising scanning with Open Vulnerability Assessment Language (OVAL)
- Patch and configuration management
- Analysing the vulnerability management process

Vulnerability controversies

- Rewards for vulnerability discovery
- Markets for bugs and exploits
- Challenge programs

LEARNING TREE INTERNATIONAL