KPMG Learning Academy

Penetration Testing Training: Tools and Techniques Course Outline

Introduction to Ethical Hacking –

- Defining a penetration testing methodology
- Creating a security testing plan

Footprinting and Intelligence Gathering –

Acquiring target information

- Locating useful and relevant information
- Scavenging published data
- Mining archive sites

Scanning and enumerating resources

- Identifying authentication methods
- Harvesting e–mail information
- Interrogating network services
- Scanning from the inside out with HTML and egress busting

Identifying Vulnerabilities –

Correlating weaknesses and exploits

- Researching databases
- Determining target configuration
- Evaluating vulnerability assessment tools

Leveraging opportunities for attack

- Discovering exploit resources
- Attacking with Metasploit

KPMG Learning Academy

Attacking Servers and Devices to Build Better Defences –

Bypassing router Access Control Lists (ACLs)

- Discovering filtered ports
- Manipulating ports to gain access
- Connecting to blocked services

Compromising operating systems

- Examining Windows protection modes
- Analysing Linux/UNIX processes

Subverting web applications

- Injecting SQL and HTML code
- Hijacking web sessions by prediction and Cross–Site Scripting (XSS)
- Bypassing authentication mechanisms

Manipulating Clients to Uncover Internal Threats –

Baiting and snaring inside users

- Executing client–side attacks
- Gaining control of browsers

Manipulating internal clients

- Harvesting client information
- Enumerating internal data

Deploying the social engineering toolkit

- Cloning a legitimate site
- Diverting clients by poisoning DNS

Exploiting Targets to Increase Security –

Initiating remote shells

- Selecting reverse or bind shells
- Leveraging the Metasploit Meterpreter

KPMG Learning Academy

Pivoting and island–hopping

- Deploying portable media attacks
- Routing through compromised clients

Pilfering target information

- Stealing password hashes
- Extracting infrastructure routing, DNS and NetBIOS data

Uploading and executing payloads

- Controlling memory processes
- Utilising the remote file system

Testing Antivirus and IDS Security –

Masquerading network traffic

- Obfuscating vectors and payloads
- Side–stepping perimeter defences

Evading antivirus systems

- Discovering stealth techniques to inject malware
- Uncovering the gaps in antivirus protection

Mitigating Risks and Next Steps –

- Reporting results and creating an action plan
- Managing patches and configuration
- Recommending cyber security countermeasures

LEARNING TREE INTERNATIONAL