KPMG Learning Academy

Penetration Testing Training: Tools and Techniques

Module 1: Introduction to Ethical Hacking

- Choosing a penetration testing framework
- Creating a security testing plan

Module 2: Foot printing 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 email information
- Interrogating network services
- Scanning from the inside out with HTML and egress busting

Module 3: Identifying Vulnerabilities

Correlating weaknesses and exploits

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

Leveraging opportunities for attack

- Crafting malware and undetectable exploits
- Attacking with Metasploit

KPMG Learning Academy

Module 4: 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 firewalls

- Bypassing URL filtering
- Performing Man-in-the-Middle attacks

Subverting web applications

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

Module 5: 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

Module 6: Exploiting Targets to Increase Security

Initiating remote shells

- Selecting reverse or bind shells
- Leveraging the Metasploit Meterpreter

KPMG Learning Academy

Pivoting and island hopping

- Performing lateral movement
- Routing through compromised clients

Pilfering target information

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

Uploading and executing payloads

- Controlling memory processes
- Bypassing User Account Controls

Module 7: Testing Antivirus and IDS Security

Masquerading network traffic

- Obfuscating vectors and payloads
- Sidestepping perimeter defenses

Evading antivirus systems

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

Module 8: Mitigating Risks and Next Steps

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

LEARNING TREE INTERNATIONAL