KPMG Learning Academy

Certified Ethical Hacker (CEH v11) Training Course Outline

Ethical Hacking Fundamentals –

Considering the effects of hacking

- Reviewing the elements of information security
- The security, functionality and usability triangle

Outlining the methods of hackers

- Reconnaissance
- Scanning
- Gaining access
- Maintaining access
- Covering tracks
- Identifying attack types: operating system, application level, shrink–wrap code and misconfiguration

Functions of an ethical hacker

- Conducting vulnerability research
- Identifying elements of information warfare

Applying Covert Techniques to Scan and Attack a Network –

Foot printing and reconnaissance

- Objectives and methods of foot printing
- Searching for information with Google Hacking
- Employing foot printing countermeasures

Scanning networks

- Adopting multiple scanning techniques
- Identifying IDS–evasion and IP–fragmentation tools
- Leveraging vulnerability scanning tools
- Applying IP spoofing detection

Examining enumeration techniques

- Enumerating user accounts using default passwords
- Simple Network Management Protocol (SNMP) enumeration

Analysing System Risks and Weaknesses to Apply Countermeasures –

System hacking

- CEH Hacking Methodology (CHM)
- Cracking passwords and escalating privileges
- Defending against password cracking and keyloggers
- Hiding information with steganography

Uncovering Trojans and backdoors

- Injecting a Trojan into a host
- Analysing Trojan activity

Dissecting viruses, worms and sniffers

- Distributing malware on the web
- Recognising key indicators of a virus attack
- Analysing worms and malware

Social engineering and Denial–of–Service (DoS)

- Targets, intrusion tactics and strategies for prevention
- Mitigating the risks of social networking to networks
- Recognising symptoms and techniques of a DoS attack
- Implementing tools to defend against DoS attacks

Assessing and Preventing Gaps in a Network Infrastructure –

Hacking web applications and wireless networks

- Cross–Site Scripting (XSS) and web application DoS attacks
- Defending against SQL injection
- Implementing a man–in–the–middle attack

Hijacking sessions and web servers

- Spoofing a site to steal credentials
- Preventing hijacking by implementing countermeasures
- Leveraging Metasploit in an attack

Evading IDS, firewalls and honeypots

- Assessing various types of Intrusion Detection Systems (IDS) and tools
- Bypassing firewalls and accessing blocked sites

Buffer overflow and cryptography

- Exploiting input validation failures
- Defending against memory corruption attacks

Performing Penetration Testing –

- Performing security and vulnerability assessments
- Determining testing points and locations
- Announced vs. unannounced testing