Ethical Hacking v12

24 Hours

Course Description

StormWind's Ethical Hacking v12 online training course will immerse students into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. Students will gain an understanding of how to leverage a multitude of tools at the disposal of today's hackers. Ethical hackers use many of the same tools as malicious hackers including, footprinting, sniffing, trojans, and more! When a student completes this online training course they will have knowledge and experience working as penetration testers on their organization's Red Team. Students completing all activities in this training will have the knowledge to pass the CEH exam (312-50).

Skills Learned

After completing this online training course, students will be able to:
- Key issues plaguing the information security world, information security controls, penetration testing, and information security laws and standards
- Different types of footprinting, footprinting tools, and countermeasures
- Network scanning techniques and scanning countermeasures
- Enumeration techniques and enumeration countermeasures
- Different types of vulnerability assessment and vulnerability assessment tools
- System hacking methodology
- Different types of malware, malware analysis procedure, and malware countermeasures
- Various packet sniffing techniques and sniffing countermeasures
- Social engineering techniques, insider threats, identity theft, and countermeasures
- DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures
- Session hijacking techniques and countermeasures
- Firewall, IDS, and honeypot evasion techniques, evasion tools, and countermeasures
- Different types of web server and web application attacks, hacking methodology, and countermeasures
- SQL injection attacks, evasion techniques, and SQL injection countermeasure
- Different types of wireless encryption, wireless threats, wireless hacking methodology, wireless hacking tools, Wi-Fi security tools, and countermeasures
- Mobile platform attack vector, andriod and iOS hacking, mobile device management, mobile security guidelines, and security tools
- Different IoT attacks, IoT hacking methodology, IoT hacking tools, and countermeasures
- Various cloud computing threats, attacks, and security techniques and tools
- Different types of encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools

Prerequisites

A working knowledge of TCP/IP, a background in either security or information systems as well as at least a year of experience working with networking technologies is strongly recommende

Who Should Attend

Ethical Hacking v12 will significantly benefit security officers, auditors, security professionals, site administrators, anyone who is concerned about the integrity of their network infrastructure, and those looking to become CEH (312-50) certified will be prepared by this class.

Course Outline

1. Hack, Hacker, Hacking
    Hack
    Hacker
    Hacking

2. Hacking Process
    Basics of Hacking
    Reconnaissance
    Scanning, Uptime Chart
    Gaining Access and Clearing Tracks

3. What is Hacking
    What Exactly is Ethical Hacking

4. Organizational Infrastructure
    Network Infrastructure, OSI Model, Network Devices
    Understanding IP, DNS, DHCP, Subnetting
    Understanding IPv4 Addresses, Address Classes
    Subnet Masks
    CIDR
    DHCP
    Domain Name Systems
    Dual Homed Host, APT's
    Intrusion Detection Software

5. Physical Security Techniques
    Securing the Perimeter

6. Organizational Protocols
Security Based Organizational Protocols

7. Organizational Policies
Confidentiality, AAA, Non-Repudiation

8. Governmental Policies
Mandatory and Non-Mandatory Compliance Frameworks

9. Keys
Keys, Digital Certificates

10. Threat Level Midnight
Attack Steps, Wireless Attacks
Internet of Things (IoT)

11. Malware
Viruses, Worms, Trojans
Stealth Viruses, Steganography
Ransomware, Spyware, Adware, Scareware

12. Spamalot
Spam Emails and Mitigation Techniques

13. Exploitable Bugs
Bug Types and Attack Vectors

14. Password Cracking
Honeypots and Password Attacks

15. Exploiting Web Applications
Website Vulnerabilities

16. Risk Management
Understanding Risk and Liability