C|EH
EC-Council's Certified Ethical Hacker has become the fastest growing certification in the security industry.
C|EH
Master
The Core Technologies Of
Ethical Hacking

Certified Ethical Hacking Certification

- A candidate with CEH certification and relevant experience is certainly favored in the IT Security industry today.
- CEH is the course to go for someone wanting to move into the security domain in any organization and CEH certification provides a good start for learning Web applications security and understanding the finer nuances of vulnerabilities and exploits.
- EC-Council certification training first teaches you how to "be" a cyber criminal, because understanding the motivations, tricks and techniques of attackers is the first step in making you the ultimate weapon against attack. EC-Council certifications measure your skills in the latest information security tools, technologies, prevention methods and countermeasures.
- A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.
- The CEH certification helps in understanding the risks & vulnerabilities holistically and complete exploit life-cycle. This enables security professionals look at security holes objectively and determine possible attack vectors, rather than merely responding to attacks.

What You'll Learn

Footprinting, and Objectives of Footprinting, Footprinting Methodology, Footprinting through Search Engine, Finding Company's Public and Restricted Websites, Determining the Operating Systems, Collecting Location Information, People Search: Social Networking Sites/People Search Services, Peoples Search Online Services, and Gather Information from Financial Services, Collecting Information through Social Engineering on Social Networking Sites, Information Available on Social Networking Sites, Website Footprinting

Scanning Networks, TCP Connection Flags, TCP/IP Communication, and Creating customs Packets using TCP Flags. ICMP Scanning, Ping sweep, Scanning Techniques, Scanning Tools: Nmap, Hping2 / Hping3, Hping TCP Connect / Full Open Scan, Stealth Scan (Half-open Scan), Inverse TCP Flag Scanning, Xmas Scan, ACK Flag Probe Scanning, and IDLE/IPID Header Scan, Banner Grabbing, Port Scanning, Firewall and IDS Evasion Techniques, Countermeasures.

Enumeration Concept & Techniques , Services and Ports Enumerate, NetBIOS Enumeration and SNMP Enumeration, NetBIOS Enumeration Tool: SuperScan, Hyena, Winfingureprint, NetBIOS Enumerator and Nsauditor Network Security Auditor, Enumerating User Accounts, Enumerating shared Resources Using NetView, LDAP Enumeration, NTP Enumeration, SMTP/DNS Enumeration, Enumeration Pen Testing, Enumeration Countermeasures

System Hacking and Methodology, System Hacking Steps, Password Cracking, and Types of Password Attacks, Password Cracking: Active Online Attacks: Trojan/Spyware/ Keylogger, using Wire Sniffing, Man-in-the-Middle/Replay Attacks, and Man-in-the-Middle and Replay Attacks, How hash Passwords Are Stored in Windows SAM, NTLM Authentication Process, Kerberos Authentication, Password Salting, Password Cracking Tools: L0phtCrack, Ophcrack, Cain & Abel, RainbowCrack, Defend against Password Cracking, Privilege Escalation Tool, Covering Tracks

Introduction to malware, different ways malware can get into a system, common techniques attackers use to distribute malware on the web, Trojan concepts, financial loss due to Trojans and how hackers use Trojans, how to infect systems using a Trojan, evading anti-virus techniques, how a computer get infected with viruses, malware detection, how to detect Trojans and viruses, pen testing for Trojans and backdoors, Trojan and virus countermeasures

Sniffing concepts, how a sniffer works and types of network sniffing- Active and Passive sniffing, MAC address attacks, DHCP starvation attack, rogue DHCP server attack, ARP spoofing and ARP poisoning attack, how to defend against DHCP attacks, DNS spoofing, DNS poisoning DNS cache poisoning and how to defend against DNS poisoning, Sniffing Tools- Wireshark and Tcpdump/Windump, Sniffing Pen Testing and Sniffing Detection Techniques

Social Engineering Concepts & Social Engineering Techniques, Human-based Social Engineering: Impersonation, Computer-based Social Engineering, Social Engineering through Impersonation on social Networking sites & Identity theft, Social Engineering Penetration Testing, Social Engineering Countermeasures

Hacking Webservers, Web Server Security Issue, Why Web Servers are Compromised, Impact of Webserver Attacks and DNS Server Hijacking, Webserver Password Cracking, Webserver Footprinting Tools, Enumerating Webserver Information Using Nmap, Mirroring a website, Vulnerability Scanning, Session Hijacking, and Hacking Web Passwords, Detecting Web Server Hacking Attempts and How to Defend against Web Server Attacks

Understanding Web Application Security, OWASP and the Top 10 Web Application Security Risks, Understanding Untrusted Data, Parameter Tampering, Hidden Field Tampering, Cookie Poisoning, Insecure Direct Object References, Persistent and Reflected Cross Site Scripting (XSS), Insufficient Transport Layer Security, Cross Site Request Forgery (CSRF), Unvalidated Redirects and Forwards, Session Management and Hijacking

Threats from Wireless, Types of Wireless Attacks- Attack on the AP and Attack on the Client, The Methodology of Hacking Wireless, Wi-Fi Discovery, Wireless Traffic Analysis, Extracting WEP and network passwords, Harvesting connections from rogue wireless access points, Encryption in Wireless - WEP Encryption and WPA & WPA2 Encryption, Breaking Encryption, Defending Against Cracking passwords

Hacking Mobile Platforms , Understanding the Android and iOS Devices & Understanding the Architecture, Rooting and Jailbreaking, Android and iOS Malware, Various Attacks, Hacking Android & iOS, Locking Down Android and iOS, MDM: Mobile Device Management, Guidelines, and Tools,

About IDS, Firewalls, and Honeypots, Firewall Architectures, Types of Firewall, Identifying the Firewall and Firewall Evasion Techniques & Tools, IDS Overview, Signature-based and Statistical Anomaly-based IDS, Network Based and Host Based IDS, IDS Evasion by Obfuscation, Fragmentation and Other Evasion Techniques, Honeypot Overview, Types of Honeypot, Detecting Honeypots

Cloud Computing Concepts, Understanding IaaS, PaaS, and SaaS, Cloud Deployment Models, The NIST Cloud Computing Reference Architecture, Cloud Computing Risks, Service Hijacking via Social Engineering, Economic Denial of Sustainability (EDoS), Hypervisor Breakouts, Malicious Cloud Uses and Other Potential Risks, Hardening the Cloud, Securing the Administration Portal and Securing the Transport Layer

Cryptography, Types of Cryptography- Symmetric and Asymmetric Cryptography, Asymmetric key and Symmetric Algorithms, Applications of Cryptography Understanding Hashing and One-Way Functions and Hashing Algorithms, Attacks Against One-Way Hash Functions, Digital Signatures and Public Key Infrastructure, Issues with Cryptography and Cryptography Attacks, Countermeasures