Infiniti
Business Solutions

Ethical Hacking Course Outline

Course Description:

The Certified Ethical Hacker Training is the pinnacle of the most desired information security training program any information security professional will ever want to be in. To master the hacking technologies, you will need to become one, but an ethical one! The accredited course provides the advanced hacking tools and techniques used by hackers and information security professionals alike to break into an organization. As we put it, “To beat a hacker, you need to think like a hacker”. This course will immerse you into the Hacker mindset so that you will be able to defend against future attacks. The security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment. This ethical hacking course puts you in the driver’s seat of a hands-on environment with a systematic process. Here, you will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! You will scan, test, hack and secure your own systems. You will be thought the five phases of ethical hacking and thought how you can approach your target and succeed at breaking in every time! The five phases include Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks What Is New in the CEH v11 Course? This is the world’s most advanced ethical hacking course with 18 of the most current security domains any ethical hacker will ever want to know when they are planning to beef up the information security posture of their organization. In 18 comprehensive modules, the course covers 270 attack technologies, commonly used by hackers. EC Council security experts have designed over 140 labs which mimic real time scenarios in the course to help you “live” through an attack as if it were real and provide you with access to over 2200 commonly used hacking tools to immerse you into the hacker world.In short, you walk out the door with advanced hacking skills that are highly in demand, as well as the internationally recognized Certified Ethical Hacker certification! Who Should Attend The Certified Ethical Hacking training course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. Modules Covered Introduction to Ethical Hacking Foot printing and Reconnaissance Scanning Networks Enumeration System Hacking Malware Threats Sniffing Sniffers Social Engineering Denial of Service Session Hijacking Hacking Web Servers Hacking Web Applications SQL Injection Hacking Wireless Networks Hacking Mobile Platforms Evading IDS, Firewalls, and Honeypots Cloud Computing Cryptography Additional Topics Trojans & Backdoors Virus & Worms Buffer Overflow Introductionof Penetration Testing.

Modes of Trainings Available:

Online Training
Class Room Training
Regular Classes Available
Weekend Classes Available

+1 (214) 315 6392
contact@infinitibizsol.com

Infiniti
Business Solutions

Course Outline

Introduction to Ethical Hacking:

Key issues include plaguing the information security world, ethical hacking, information security controls, laws, and standards.

Footprinting and Reconnaissance:

Perform footprinting and reconnaissance using the latest footprinting techniques and tools as a critical pre-attack phase required in ethical hacking.

Scanning Networks:

Network scanning techniques and scanning countermeasures

Enumeration:

Enumeration techniques and enumeration countermeasures.

Vulnerability Analysis:

Vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.

System Hacking:

System hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities

Malware Threats:

Different types of malware (Trojan, Virus, worms, etc.), system auditing for malware attacks, malware analysis, and countermeasures.

Sniffing:

Packet sniffing techniques to discover network vulnerabilities and countermeasures to defend sniffing.

Social Engineering:

Social engineering techniques and how to identify theft attacks to audit human level vulnerabilities and suggest social engineering countermeasures.

Denial of Service:

DoS/DDoS attack techniques and tools to audit a target and DoS/DDoS countermeasures

+1 (214) 315 6392

contact@infinitibizsol.com

Infiniti
Business Solutions

Session Hijacking:

Session hijacking techniques to discover network-level session management, authentication/authorization, cryptographic weaknesses, and countermeasures

Hacking Web Servers:

Web server attacks and a comprehensive attack methodology to audit vulnerabilities in web server infrastructure, and countermeasures.

Hacking Web Applications:

Web application attacks and comprehensive web application hacking methodology to audit vulnerabilities in web applications, and countermeasures.

Evading IDS, Firewalls, and Honeypots:

Firewall, IDS and honeypot evasion techniques, evasion tools and techniques to audit a network perimeter for weaknesses, and countermeasures.

SQL Injection:

SQL injection attack techniques, injection detection tools to detect SQL injection attempts, and countermeasures

Hacking Wireless Networks:

Wireless encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.

IoT and OT Hacking:

Threats to IoT and OT platforms and learn how to defend IoT and OT devices Securely.

Cloud Computing:

Cloud computing concepts (Container technology, serverless computing), various threats/attacks, and security techniques and tools

Cryptography:

Cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.