Certified Ethical Hacker (CEH) boot camp

The Certified Ethical Hacker (CEH) Certification Program certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. CEH certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A CEH is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker.

To achieve CEH certification, you must pass the Ethical Hacking and Countermeasures Exam 312-50. This exam is offered at any VUE testing center anywhere around the world.

Venue

Nairobi Kenya
(exact hotel name to be confirmed before course)

Dates

March 31, 2014 — April 4, 2014

Inovatec College

Kenya House, 1st Floor
Koinange Street
P O Box 4290 00100
Nairobi, KENYA

Tel: +254 -717 357 005/
+254 -734 739 893
E-mail:
info@inovateccollege.com

Inovatec
COLLEGE

Ethical hacking is one of the courses that will help you understand the basic principles behind protecting and securing your information, applications, and networks.

Our security instructors are seasoned veterans who have spent considerable time in the industry. When they aren't teaching, our instructors work on real-life consulting projects, ensuring a thorough understanding of their subject matter and applicable real-world experience.

What You'll Learn

- Footprinting and reconnaissance
- Hacking web servers, web applications, and wireless networks
- Cryptography
- Penetration testing
- Social engineering
- Trojans, viruses, and worms
- Evading IDS, firewalls, and honeypots
- Enumeration
- Buffer overflows

Who Needs to Attend

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of their network infrastructure.

Prerequisites

IT security experience and a strong working knowledge of TCP/IP.

Course Outline

1. Introduction to Ethical Hacking

2. Footprinting and Reconnaissance

3. Scanning Networks

4. Enumeration

5. System Hacking

6. Trojans and Backdoors

7. Viruses and Worms

8. Sniffers

9. Social Engineering

10. Denial of Service

11. Session Hijacking

12. Hijacking Web Servers

13. Hacking Web Applications

14. SQL Injection

15. Hacking Wireless Networks

16. Evading IDS, Firewalls, and Honeypots

17. Buffer Overflows

18. Cryptography

19. Penetration Testing

Labs

Lab 1: Footprinting and Reconnaissance

- Discover Network Paths with the Ping Utility
- Query DNS with nslookup Utility
- Search for People Using the AnyWho Online Tool
- Analyze Domain and IP Address Queries Using SmartWhois
- Trace Network Routes Using Path Analyzer Pro
- Trace E-Mail Delivery Routes with the eMailTrackerPro Tool
- Copy a Website with the HTTrack Web Copier Tool
- Extract Web Data with the Web Data Extractor Tool
- Search for Web Vulnerabilities with Search Diggity Tool

Lab 2: Scanning Networks

- Scan System and Network Resources Using Advanced IP Scanner
- Monitor TCP/IP Connections Using the CurrPorts Tool
- Scan for Network Vulnerabilities Using the GFI Languard Network Scanner
- Scan Hosts for Services Using Nmap
- Scan for Vulnerabilities with the Nessus Tool
- Map a Network Using Global Network Inventory Tool
- Create Proxies with Proxy Workbench Tool
- Perform Tunneling with HTTPort/HTTHost Tool
- Create Packets Using Colasoft Packet Builder
- Perform Traffic Analysis with the Dude Sniffer Tool

Lab 3: Enumeration

- Enumerate Services with Zenmap
- Enumerate Hosts Using the SuperScan Tool
- Enumerate Networks with SoftPerfect Network Scanner
- Enumerate a Network with SolarWinds Toolset

Lab 4: System Hacking

- Extracting Administrator Passwords Using LCP
- Hiding Files Using NTFS Streams
- Search for Alternate Data Streams using the ADS Spy Tool
- Hide Content with Stealth Files Steganography
- Extract Passwords with the PWdump7 Tool
- Generate Rainbow Tables with the Winrtgen Tool
- Crack Hashed Passwords using the Rainbowcrack Tool
- Crack Hashed Passwords with the L0phtCrack Tool
- Execute Files Remotely with the RemoteExec Tool
- Hide Content with the Snow Steganography Tool
- Control System Auditing with the Auditpol Utility
- Reset Passwords with the CHNTPW.iso Tool
- Monitor Users with the Spytech SpyAgent Tool
- Hide Content with the QuickStego Tool

Lab 5: Trojans and Backdoors

- Create a Server Using the ProRat Tool
- Create a Trojan with the OneFile EXE Maker Tool
- Create a Server with the Proxy Server Trojan
- Create a Server with the HTTP Trojan
- Create a Server with Atelier Web Remote Commander
- Create a Trojan with Biodox Trojan Creator Tool
- Create a Backdoor with Metasploit

Lab 6: Viruses and Worms

- Create a Virus Using the JPS Virus Maker Tool
- Reverse Engineer Code Using the IDA Pro Analysis Tool
- Scan for Viruses with Kaspersky Anti-Malware
- Generate a Worm Using Internet Worm Maker Thing Tool

Lab 7: Sniffers

Lab 7: Sniffers

- Analyze Packet Captures Using the OmniPeek Network Analyzer
- Spoof MAC Address Using SMAC
- Analyze a Network Using the Colasoft Capsa Network Analyzer
- Sniff Network Traffic with Wireshark
- Perform ARP Poisoning with Cain
- Detect Hosts in Promiscuous Mode with PromqryUI

Lab 8: Social Engineering

- Detect Phishing Using Netcraft
- Create a Rogue Website with Social Engineering Toolkit (SET)

Lab 9: Denial of Service

- Use Hping to Create a Denial of Service Attack
- Use DoSHTTP to Create a Denial of Service Attack

Lab 10: Session Hijacking

- Hijack and Redirect Web Requests with the Zed Attack Proxy (ZAP)

Lab 11: Hacking Webserver

- Footprint Webservers with the HTTP Recon Tool
- Footprint a Webserver Using ID Serve
- Attack Webservers with Metasploit

Lab 12: Hacking Web Applications

- Create a Cross-Site Scripting Attack with JavaScript
- Explore the Vampire Vulnerability Scanner
- Scan a Website for Vulnerabilities Using Acunetix

Lab 13: SQL Injection

- Perform SQL Injection Attacks on MS SQL Database
- Scan an Internet Site with IBM App Scan Vulnerability Scanner
- Scan a WebServer with N-Stalker Vulnerability Scanner

Lab 14: Hacking Wireless Networks

- Analyze WiFi Traffic with AirPcap with Wireshark
- Crack the WEP Key for Captured Traffic with Aircrack-ng
- UnWEP Bulk Captured Traffic with OmniPeek Once Key is Known

Lab 15: Evading IDS and Firewalls

- Configure the Snort Intrusion Detection Tool
- Use the Kiwi Syslog Viewer to Analyze Snort Logs
- Install, Configure, and Attack the KFSensor Honeypot Tool

Lab 16: Buffer Overflow

- Code, Compile, and Execute a Buffer Overflow Attack

Lab 17: Cryptography

- Hash Files and Data Using HashCalc
- Encrypt Data Using the Advanced Encryption Package
- Encrypt File Systems with TrueCrypt
- Encrypt Data with the BCTextEncoder Tool

Cost

The entire course will cost USD2,200 per delegate

Sign up now using form below

Banking details;

Account Name: Securenet Technologies (k) Ltd
Bank Name: Commercial Bank of Africa
Branch: Wabera Street
Account Number: 6510560011
SWIFT CODE: CBAFKENXXXX