HiiT ...Your Premium Training Partner | World Class IT Services since 1996

Certified Ethical Hacker (CEH)

Course Curriculum *www.hiit.ng*

Course Overview: ***This course gives hands-on classroom/online training to scan, hack, test and secure systems and applications***

The extensive course on Ethical Hacking of the most current and practical approach to the present major security systems. This training program prepares candidates to pass EC-Council Certified Ethical Hacker exam 312-50. The training program provides a good start for understanding web and mobile application security and increasing the present knowledge of identifying threats and liabilities.

WEEK	MODULE	TOPIC	HOURS	OBJECTIVES
WEEK 1	1. Introduction To Ethical Hacking	1. Introduction to Ethical Hacking. 2.The CIA Triad 3.Important Security Terminologies. 4. Penetration Testing	1.5	This module Introduces you to the world of information security. At the end of this module, you will have a better understanding of how professionals Practice Ethical Hacking Legally as well as approach's/methodologies being used.
WEEK 1	2. Introduction to Kali Linux	1. Introduction to Kali Linus. 2. Linux file Structure. 3. The Terminal. 4. Linux CLI Commands	3.0	This module will make you love Linux operating system as almost 90% of security tools are compatible with this operating system. At the end of this module, using the terminal for all your operations won't be an issue.
WEEK 1	3. Anonymity	1. Introduction to Anonymity 2. Downloading, Installing and Configuring Proxychains. 3.Downloading, Installing and Configuring Macchanger.	2.0	The main goal of a Hacker is to be undetectable. This module helps you in achieving that. At the end of this module, you will be able to hide your identity over the internet.
WEEk 2	4. Reconnaissance	1. Introduction to Reconnaissance 2. Web Server Reconnaissance 3. DNS Server Reconnaissance 4. Mail Server Reconnaissance 5. Sub Domain Reconnaissance 6. Email Server Reconnaissance 7. Load Balancer Reconnaissance	3.0	Hackers uses different techniques to get information from their targets. This modules shows you the techniques, tools for gathering valuable Information's.
WEEk 2	5. Sniffing	1. TCP Flags 2. TCP Three(3) Way Handshake 3. Introduction to Wireshark 4. Analyzing Packets with Wireshark 5. Important Wireshark Filters	2.0	This module teaches you how you can secure network infrastructures using Wireshark to monitor and analyze traffics to and fro your network.

WEEK	MODULE	TOPIC	HOURS	OBJECTIVES
WEEk 2	6. Port Scanning & Enumeration	1. Introduction to Port Scanning & Enumeration. 2. Packet Crafting. 3. Port Scanning & Enumeration with Nmap.	4.0	Port scanning and enumeration is technique security professional uses to audit servers to make sure unnecessary ports or services are not exposed. This module equips you with technique. At the end of this module you will be know different types of scans as well as crafting techniques to bypass firewall rules.
WEEk 2	7. Vulnerability Assessment/Analysis	1. Introduction to Vulnerabiliy Assessment 2. Need for Vulnerability Assessment. 3. Ways of discovering vulnerabilities. 4. Tools for Vulnerability Assessment	3.0	The sole of a penetration tester is to look for loopholes within an infrastructure. At the end of his module you will be able to conduct a vulnerability test, identify vulnerabilities, create a report and finally patch these vulnerability.
WEEK 2	8. Password Hacking	1. ntoduction to Password Hacking. 2. Types of Password Attacks. 3. Tools for Password Hacking. 4. Tools for Generating Customs Wordlist. 5. Mitigatings	3.0	At the end of this module, you will be familiar with different hash algorithms, where to locate hashes in operating Systems and finally retrieve the plain text values from the hash.
WEEk 3	9. Server Hacking	1. Server Hacking via Brute-Force Method (Hydra). 2.Server Hacking via Known Exploits 3. Mitigations	5.0	This module show you different approach toward gaining access to web servers remotely.
WEEk 3	10. System Hacking	1. Intriduction to Metasploit. 2. Hacking Windows 10. 3. hacking Linux Operating System. 4. Hacking Android O.S. 5. Mitigation's	6.0	At the end of this module, you will be learn the techniques used to gain unauthorized access to Windows, Linux and android operating system
WEEk 3	11. Hacking Wireless Network	1. Cracking WPA/WPA2 PSK Passwords. 2. Setting Up Rogue Access Point. 3. Man-In-The-Middle Attack. 4. DNS Spoofing Attach. 5. Mitigation's.	6.0	This module teaches you the art of cracking WIFI password, creating a fake access point, perform man-in-the-middle attack over the internet.
WEEk 4	12. Denial Of Service	1. Introduction To Dos & DDOS. 2. SYN Flood Attack. 3. SMURF Attack. 4. FRAGGLE Attack. 5. LAND Attack. 6. Mitigations	4.0	This module will teach you how to test if a server is vulnerable to DOS/DDOS attack by flooding the server aswell as how you can mitigate this type of attack.

WEEK	MODULE	TOPIC	HOURS	OBJECTIVES
WEEk 4	13. Social Engineering	1.Introduction to Social Engineering 2. Social Engineering With Blackeye. 3. Mitigations	3.0	This module shows you the techniques hackers uses to steal login credentials as well as how you can prevent it.
WEEk 4	14. Cryptography & Steganography	1. Introduction to Cryptography. 2. Tools for Cryptography. 3. Introduction to Steganography. 4. Tools for Steganography.	4.0	At the end of this module, you will be able to conceal files, encrypt files or hard disk.
WEEk 4	15. Web Application Hacking	1. Introduction to OWASP. 2. OWASP TOP 10. 3. Tools For Web Application Testing	8.0	This module teaches you methods used to find vulnerabilities in web application, exploiting them and mitigating them.
		TOTAL	58	