CERTIFIED ETHICAL HACKING COURSE OUTLINE

Course overview

The certified Ethical Hacker program is the pinnacle of the most desired information security program anyone looking interested in security will ever want to be in. To master the hacking technologies, you will need to become a hacker, but an ethical one! This course provides the advanced hacking tools and techniques used by hackers and IT security professionals alike to break into an organization. The ethical hacking course will immerse you into the hacking technology so that you will be able to defend against future attacks, and you will be immersed in a hacker's mindset, evaluating not just logical, but physical security.

This course will significantly benefit security officers, auditors,
Security professionals, network administrators, and anyone who is concerned about the integrity of their network infrastructure. To beat a hacker, you need to think like a hacker. Why not take a hands-on course in VoISIP to empower yourself to become a CERTIFIED ETHICAL HACKER.

SOFTWARES USED & AVAILABLE TO STUDENTS IN THE TRAINING

- *Virtual box, Vmware & hyper-V virtualization software*
- *Kali penetration testing & ethical hacking Linux Operating system (contains over 600 hacking tools already installed).*
- *Parrot Security operating system (contains over 600 hacking tools already installed).*
- *Metasploitable Ubuntu intentionally vulnerable virtual machine*
- *Windows 7 & 10 SP2 Operating system ISO file*
- *HP servers with 32GB Ram, 2TB HDD for spinning virtual machines for students without laptops.*

COURSE DURATION

Regular Course: 8 weeks, fast track 6 days

Instructor profile: Mr kelvin Ojanomare

Msc Telecomms, Bsc. Elect/Elect Engr, CCNP Voice, CCNA, MCSA, Linux+, CEH

COURSE OUTLINE

INTRODUCTION TO ETHICAL HACKING & PENETRATION TESTING

- Types of hackers
- Virtualbox download and installation
- Installation & initial Configuration of Kali & parrot Operating System
- Installation of virtualbox guest-additions or VMWARE tools add-ons on Kali & Parrot OS
- Installing Windows 7, windows 10, Windows Server 2012, Metasploitable

INTRODUCTION TO LINUX

- Linux overview
- Using Linux as a hacking environ
- Command Line Skills
- Getting Help
- Working with Files and Directories
- Network Configuration

FOOTPRINTING & RECONAISANCE

- What is foot printing?
- Objectives and tools
- Whois lookup
- DNS foot printing functions and process
- Determining victim operating system
- Introduction to phishing attacks
- Collecting information database (facebook, gmail, youtube,Instagram, etc)
- Introduction to Nmap ZenMap
- The harvester process and functions
- Whois and dnsenum overview
- URLcrazy, DNSdict and DNSrecon
- Recon-ng

SOCIAL ENGINEERING & INFORMATION GATHERING

- Introduction to Social Engineering and information gathering
- SETOOLKIT installation and configuration
- Types of Social Engineering attacks
- Spear phishing attack using SETOOLKIT to gain login details for Facebook, Gmail etc
- Mass Mailer attack

TROJAN & COMPUTER MALWARES

- Introduction to computer malwares
- Types of computer malwares
- Dangerous viruses of all time
- Installing rootkit hunter
- SYSTEM HACKING
- Hacking a windows machine using SETOOLKIT
- Backdoor overview, process & functions
- Gaining access through backdoor
- Maintaining access through backdoor using SETOOLKIT meterpreter
- Introducing command prompt backdoor
- Meterpreter backdoor
- I am root (getting Windows system SYSTEM account status)
- Forensic escaping
- Hacking Windows 8 SAM database
- Using jack the ripper to crack windows hash password
- Advanced meterpreter commands
- PDF embedded Trojan horse
- Introduction to Java Applet Attack method
- Man-In-the-Middle Attack
- ARP poisoning attack

DNS SPOOFING & DNS POISONING

- DNS spoofing Vs DNS poisoning
- Advanced concepts on DNS spoofing
- DHCP spoofing
- Port stealing

ICMP REDIRECTION

- Introduction to ICMP redirection
- ICMP redirection visual chart
- ICMP redirection process & functions

TROJANS, NETWORKS & EVILGRADE

- Killing a network

- Ddosing unauthorized network
- Drifnet
- Introduction to Evilgrade

DENIAL OF SERVICE ATTACK

- Introduction to denial of Service (DOS)
- DoS Vs DDos
- Levels of DDoS attacks
- Preventing DDoS attacks
- Introduction to DDosing windows
- DDoSing Windows 7 methods

PASSWORD CRACKING

- Introduction to password cracking
- Password cracking strategy
- Windows password cracking overview
- Nuts and bolts of windows password cracking strategy
- Introduction to Linux hash cracking
- Linux hash cracking strategy
- Generating wordlist process and functions
- CeWl cracking

WIRELESS HACKING

- WEP & WPA
- 802.1X standard
- Wireless cracking overview
- Wireless cracking via kali Linux or parrot OS.

METERPRETER

- Meterpreter overview
- Activating payloads
- Using Armitage, meterpreter GUI toolkit

METASPLOIT

- Msfconsole overview
- Msfconsole commands
- Exploits
- Payloads
- Generating payloads

WEB APPLICATION PENETRATION TESTING

- Installing testbed for web application testing
- Installing Vega Firefox addons and brute force
- Exploring the Command injection vulnerability
- Reflected and stored XSS i.e cross site scripting
- DOM based XSS and learning resource
- Cross site request forgery vulnerability

HACKING WEB SERVERS (SQL INJECTION)

- Introduction to SQL injection
- SQL injection to google dorks
- SQL mapping via Kali Linux
- Generating password and cracking the hash

CRYTOGRAPHY

- Introduction & basic concepts on cryptography
- Hash function and oracle method
- Birthday theorem digital signature
- Pros and Cons of cryptography

METASPLOIT DATABASE

- Importing & Exporting databases
- Exporting databases shown in practicals.

HACKING MOBILE DEVICES

- Hacking through android
- Hacking android via kali linux or Parrot OS