Ethical Hacking
By Mr. Abrar & Mr. Vishwanath
(6+ Years Experience)   (6+ Years Experience)

Introduction to Ethical Hacking
- What is Hacking
- Who is a Hacker
- Skills of a Hacker
- Types of Hackers
- Reasons for Hacking
- Who are at the risk of Hacking attacks
- Effects of Computer Hacking on an organization
- Network Security Challenges
- Elements of Information Security: Confidentiality, Integrity & Availability
- The Security, Functionality & Usability Triangle
- What is Ethical Hacking
- Why Ethical Hacking is Necessary
- Scope & Limitations of Ethical Hacking
- What is Penetration Testing
- What is Vulnerability Auditing

Computer and Network Basics:
- Hacking
- Internet protocol
- Types of IP
- Port
- Protocol
- Protocol service
- OS for different hardware platforms
- Vulnerability
- Different Programming languages for different platforms/purposes.
- What are Networks and what is networking
- Network topologies
- How the Networking devices communicate.
- Vulnerable Hacking environments
- Hashing checksums
- Window/Linux commands
- Php code overview
- Assembly language programming overview
- Introduction of kali
- Introduction of backtrack
- Introduction of parrot

Kali Linux
- What is Kali Linux
- How Kali Linux is different from other Linux distributions
- What are the uses of Kali Linux
- What is Metasploit framework.
- Tools for Footprinting, Scanning & Sniffing
- Using Metasploit framework to attack Windows machines

Foot Printing/reconnaissance/Information Gathering
- What is Foot Printing
- Objectives of Foot Printing
- Finding a company's details
- Finding a company's domain name
- Finding a company's Internal URLs
- Finding a company's Public and Restricted URLs
- Finding a company's Server details
- Finding the details of domain registration
- Finding the range of IP Address
- Finding the DNS information
- Finding the services running on the server
- Finding the location of servers
- Traceroute analysis
- Tracking e-mail communications

Scanning
- What is network scanning
- Objectives of network scanning
- Finding the live hosts in a network
- Finding open ports on a server
- Finding the services on a server
- OS fingerprinting
- Server Banner grabbing tools
- What is a Vulnerability Scanning
- Vulnerability Scanner tools
- Finding more details about a vulnerability
- What is a proxy server
- How does proxy server work
- Types of proxy servers
- How to find proxy servers
- Why do hackers use proxy servers
- What is a TOR network
- Why hackers prefer to use TOR network

Enumeration:
- SNMP Enumeration
- SMTP Enumeration
- DNS Enumeration

Vulnerability Analysis (New)
- Perform vulnerability analysis to identify security loopholes in the target organization's network, Communication infrastructure and end systems.

Sniffing and Sniffers
- What is a sniffer
- How sniffer works
- Types of sniffing
- Active sniffing

B-2, 2nd Floor, KVR Enclave, Beside Satyam Theatre, Above Bata Showroom, Ameerpet, Hyd – 16
info@techmarshals.com | www.techmarshals.com | 04040034050 / 9133333875

1

- Passive Sniffing
- What is promiscuous mode
- How to put a PC into promiscuous mode
- What is ARP
- ARP poison attack
- Threats of ARP poison attack
- How MAC spoofing works
- MAC Flooding
- What is a CAM Table
- How to defend against MAC Spoofing attacks
- How to defend against Sniffers in network

System Hacking
- What is system Hacking
- Goals of System Hacking
- Password Cracking
- Password complexity
- Finding the default passwords of network devices and softwares
- Password cracking methods
- Online password cracking
- Man-in-the-middle attack
- Password guessing
- Offline password cracking
- Brute force cracking
- Dictionary based cracking
- Hybrid attack
- USB password stealers
- Elcomsoft Distributed password recovery tools
- Active password changer
- What is a Keylogger
- How to deploy a Keylogger to a remote pc
- How to defend against a Keylogger.

Malware Threats
- What is malware
- Types of malware
- Virus
- What is a virus program
- What are the properties of a virus program
- How does a computer get infected by virus
- Types of virus
- Virus making tools
- How to defend against virus attacks
- Worm
- What is a worm program
- How worms are different from virus
- Trojan
- What is a Trojan horse
- How does a Trojan operate
- Types of Trojans
- Identifying Trojan infections
- How to defend against Trojans
- Spyware
- What is a spyware
- Types of spywares
- How to defend against spyware
- Rootkits
- What is a Rootkit
- Types of Rootkits
- How does Rootkit operate
- How to defend against Rootkits

Phishing and Social engineering
- What is Phishing
- How Phishing website is hosted
- How victims are tricked to access Phishing websites

- How to differentiate a Phishing webpage from the original webpage
- How to defend against Phishing attacks
- SET: Social Engineering Toolkit

DOS : Denial of Service
- What is a DOS attack
- What is a DDOS attack
- Symptoms of a Dos attack
- DoS attack techniques
- What is a Botnet
- Defending DoS attacks

Session Hijacking
- What is session hijacking.
- Dangers of session hijacking attacks
- Session hijacking techniques
- Cross-Site scripting attack
- Session hijacking tools
- How to defend against session hijacking.

Hacking Web Servers & Web Applications
- What is a web server
- Different webserver applications in use
- Why are webservers hacked & its consequences
- Directory traversal attacks
- Website defacement
- Website password brute forcing
- How to defend against web server hacking

SQL Injection
- What is SQL Injection
- Effects of SQL Injection attacks
- Types of SQL Injection attacks
- SQL Injection detection tools

Wireless Network Hacking
- Types of wireless networks
- Wi-Fi usage statistics
- Finding a Wi-Fi network
- Types of Wi-Fi authentications
- Using a centralized authentication server
- Using local authentication
- Types of Wi-Fi encryption methods
- WEP
- WPA
- WPAT
- How does WEP work
- Weakness of WEP encryption
- How does WPA work
- How does WPAT work
- Hardware and software required to crack Wi-Fi networks
- How to crack WEP encryption
- How to crack WPA encryption
- How to crack WPAT encryption
- How to defend against Wi-Fi cracking attacks

Android Hacking
- Android Hacking Online and Offline.
- What is Metasploit framework.
- Using Metasploit framework to attack Android **mobile** devices.

Evading Firewalls, IDS & Honeypots
- What is a Firewall
- What are the functions of a Firewall
- What is an IDS

B-2, 2nd Floor, KVR Enclave, Beside Satyam Theatre, Above Bata Showroom, Ameerpet, Hyd – 16
info@techmarshals.com **|** www.techmarshals.com **|** 04040034050 / 9133333875

2

- How does an IDS work
- SPAN
- IDS tools
- What is a honeypot
- Types of honeypots
- Honeypot tools
- Honeypot detection tools

IoT Hacking (New)
- Different threats to IoT platforms and learn how to defend IoT devices securely.

Cloud Computing
- What is Cloud
- What are the cloud services
- Various cloud computing concepts, threats, attacks, and security techniques and tools (Cloud security).

Stenography
- Stenography

Cryptography
- What is Cryptography
- Types of cryptography
- Cipher algorithms
- Public key infrastructure
- What is a Hash
- Cryptography attacks

Penetration Testing
- What is Penetration Testing
- Types of Penetration Testing
- What is to be tested
- Testing the network devices for misconfiguration
- Testing the servers and hosting applications for misconfiguration
- Testing the servers and hosting applications for vulnerabilities
- Testing wireless networks
- Testing for Denial of Service attack

Counter Measure Techniques for Network level attacks
- Types of Firewall
- Packet Filtering Firewall
- Circuit-Level Gateway Firewall
- Application-Level Firewall

- Stateful Multilayer Inspection Firewall
- Limitations of a Firewall
- IDS / IPS
- What is an IDS
- What is a IPS
- Difference between IDS & IPS
- Placement of IDS in the Network
- Configuring an IDS in the Network
- Placement of IPS in the Network
- Configuring an IPS in the Network
- UTM / Next-Generation Firewall
- What is a UTM
- Features of UTM
- Difference between a Firewall & a UTM
- Placement of UTM in the Network
- Configuring a UTM in the Network
- Monitoring attacks using UTM
- Configuring IPS module in UTM to detect and stop attacks

Counter Measure Techniques for Local Systems
- Identifying the Vulnerabilities of a system
- Understanding the Vulnerabilities of a system
- CVE ID
- Bugtraq ID
- Patch Management
- Identifying the patch for a Vulnerability
- Downloading the Patch
- Testing the patch for stability in test environment
- Deploying the patch to Live Network
- Finding the missing updates in an Operating System
- Microsoft Baseline Security Analyser
- Belarc Advisor

Counter Measure Techniques for Malware Attacks
- Scanning systems for Malware infections
- Types of anti-malwares
- Anti-Virus
- Anti-Worm
- Anti-Trojan
- Anti-Rootkit
- Internet Security Suites
- HIDS
- HIPS

Other Offered Courses:
Bug-Bounty | Dev-Ops | Amazon Web Services | Digital Marketing | Web Designing.

B-2, 2nd Floor, KVR Enclave, Beside Satyam Theatre, Above Bata Showroom, Ameerpet, Hyd – 16
info@techmarshals.com | www.techmarshals.com | 04040034050 / 9133333875

3