

# Ethical Hacking

## Introduction to Ethical Hacking

### Lesson - Hacking Concepts

- 1.What is Hacking
- 2.Who is a Hacker?
- 3.Hacker Classes
- 4.Hacking Phases

### Lesson - Ethical Hacking Concepts

- 1.What is Ethical Hacking?
- 2.Why Ethical Hacking is Necessary
- 3.Scope and Limitations of Ethical Hacking
- 4.Skills of an Ethical Hacker

## Module - Footprinting and Reconnaissance

### Lesson - Footprinting Concepts

- 1.What is Footprinting?
- 2.Objectives of Footprinting

### Lesson - Footprinting through Search Engines

- 1.Footprinting through Search Engines
- 2.Footprinting using Advanced Google Hacking Techniques
- 3.Information Gathering Using Google Advanced Search and Image Search
- 4.Google Hacking Database

### Lesson - Footprinting through Web Services

- 1.Finding Company's Top-level Domains (TLDs) and Sub-domains
- 2.Finding the Geographical Location of the Target
- 3.People Search on Social Networking Sites and People Search Services
- 4.Gathering Information from LinkedIn
- 5.Gather Information from Financial Services
- 6.Footprinting through Job Sites
- 7.Monitoring Target Using Alerts
- 8.Information Gathering Using Groups, Forums, and Blogs
- 9.Determining the Operating System

### Lesson - Footprinting through Social Networking Sites

- 1.Collecting Information through Social Engineering on Social Networking Sites

### Lesson - Website Footprinting

- 1.Website Footprinting
- 2.Website Footprinting using Web Spiders
- 3.Mirroring Entire Website
- 4.Extracting Website Information
- 5.Extracting Metadata of Public Documents
- 6.Monitoring Web Pages for Updates and Changes

## Lesson - Email Footprinting

- 1.Tracking Email Communications
- 2.Collecting Information from Email Header
- 3.Email Tracking Tools

## Lesson - Whois Footprinting

- 1.Whois Lookup
- 2.Whois Lookup Result Analysis
- 3.Whois Lookup Tools
- 4.Finding IP Geolocation Information

## Lesson - DNS Footprinting

- 1.Extracting DNS Information
- 2.DNS Interrogation Tools

## Lesson - Network Footprinting

- 1.Locate the Network Range
- 2.Traceroute
- 3.Traceroute
- 4.Traceroute Tools

## Lesson - Footprinting through Social Engineering

- 1.Footprinting through Social Engineering
- 2.Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving

## Lesson - Countermeasures

- 1.Footprinting Countermeasures

## Module - Scanning Networks

### Lesson - Network Scanning Concepts

- 1.Overview of Network Scanning
- 2.TCP Communication Flags
- 3.TCP/IP Communication
- 4.Creating Custom Packet Using TCP Flags
- 5.Scanning in IPv6 Networks

### Lesson - Scanning Tools

- 1.Nmap
- 2.Hping2 / Hping3
- 3.Scanning Tools

### Lesson - Scanning Techniques

- 1.Scanning Technique
- 2.Port Scanning Countermeasures

### Lesson - Banner Grabbing

- 1.Banner Grabbing
- 2.How to Identify Target System OS
- 3.Banner Grabbing Countermeasures

### Lesson - Draw Network Diagrams

- 1.Draw Network Diagrams

- 2.Network Discovery and Mapping Tools
- 3.Network Discovery Tools for Mobile

## Module - System Hacking

### Lesson - System Hacking Concepts

#### Lesson - Cracking Passwords

- 1.Password Cracking
- 2.Types of Password Attacks
- 3.Password Recovery Tools
- 4.Password Cracking Tools
- 5.How to Defend against Password Cracking

#### Lesson - Executing Applications

- 1.Executing Applications
- 2.Keylogger
- 3.Spyware
- 4.How to Defend Against Keyloggers
- 5.How to Defend Against Spyware

## Module - Malware Threats

### Lesson - Malware Concepts

- 1.Introduction to Malware
- 2.Different Ways a Malware can Get into a System
- 3.Common Techniques Attackers Use to Distribute Malware on the Web
- 4.Components of Malware

### Lesson - Trojan Concepts

- 1.What is a Trojan?
- 2.How Hackers Use Trojans
- 3.Common Ports used by Trojans
- 4.How to Infect Systems Using a Trojan
- 5.How Attackers Deploy a Trojan
- 6.Exploit Kits
- 7.Evading Anti-Virus Techniques
- 8.Types of Trojans

### Lesson - Virus and Worm Concepts

- 1.Introduction to Viruses
- 2.Stages of Virus Life
- 3.Working of Viruses
- 4.Indications of Virus Attack
- 5.How does a Computer Get Infected by Viruses
- 6.Fake Antiviruses
- 7.Ransomware
- 8.Types of Viruses

9.Creating Virus

10.Computer Worms

Lesson - Countermeasures

1.Trojan Countermeasures

2.Backdoor Countermeasures

3.Virus and Worms Countermeasures

Lesson - Anti-Malware Software

1.Anti-Trojan Software

2.Antivirus Software

Module - Sniffing

Lesson - Sniffing Concepts

1.Network Sniffing

2.Types of Sniffing

3.How an Attacker Hacks the Network Using Sniffers

4.Protocols Vulnerable to Sniffing

5.Wiretapping

Lesson - Sniffing Technique: DHCP Attacks

1.How DHCP Works

2.DHCP Request/Reply Messages

3.DHCP Starvation Attack

Lesson - Sniffing Technique: ARP Poisoning

1.What Is Address Resolution Protocol (ARP)?

2.ARP Spoofing Attack

3.Threats of ARP Poisoning

4.ARP Poisoning Tools

5.How to Defend Against ARP Poisoning

6.ARP Spoofing Detection Tools

Lesson - Sniffing Technique: Spoofing Attacks

1.MAC Spoofing/Duplicating

2.MAC Spoofing Technique: Windows

3.MAC Spoofing Tools

4.IRDP Spoofing

5.How to Defend Against MAC Spoofing

Lesson - Sniffing Tools

1.Sniffing Tool: Wireshark

2.Sniffing Tools

3.Packet Sniffing Tools for Mobile

Module - Social Engineering

Lesson - Social Engineering Concepts

1.What is Social Engineering?

2.Phases of a Social Engineering Attack

Lesson - Social Engineering Techniques

- 1.Types of Social Engineering
- 2.Human-based Social Engineering
- 3.Computer-based Social Engineering
- 4.Mobile-based Social Engineering

#### Lesson - Impersonation on Social Networking Sites

- 1.Social Engineering Through Impersonation on Social Networking Sites
- 2.Impersonation on Facebook
- 3.Risks of Social Networking Threats to Corporate Networks

#### Lesson - Countermeasures

- 1.Social Engineering Countermeasures
- 2.Insider Threats Countermeasures
- 3.Identity Theft Countermeasures
- 4.How to Detect Phishing Emails

#### Lesson - Social Engineering Penetration Testing

- 1.Social Engineering Pen Testing
- 2.Social Engineering Pen Testing Tools

#### Lesson - Insider Threats

- 1.Insider Threat / Insider Attack
- 2.Type of Insider Threats

#### Module - Denial-of-Service

##### Lesson - DoS/DDoS Concepts

- 1.What is Denial of Service Attack?
- 2.What is Distributed Denial of Service Attack?

##### Lesson - DoS/DDoS Attack Techniques

- 1.Basic Categories of DoS/DDoS Attack Vectors
- 2.UDP Flood Attack
- 3.ICMP Flood Attack
- 4.Ping of Death and Smurf Attack
- 5.SYN Flood Attack
- 6.Multi-Vector Attack
- 7.Peer-to-Peer Attacks

##### Lesson - DDoS Case Study

- 1.DDoS Attack
- 2.Hackers Advertise Links to Download Botnet
- 3.Use of Mobile Devices as Botnets for Launching DDoS Attacks
- 4.DDoS Case Study: Dyn DDoS Attack

##### Lesson - DoS/DDoS Attack Tools

- 1.DoS and DDoS Attack Tool

##### Lesson - Countermeasures

- 1.Detection Techniques
- 2.DoS/DDoS Countermeasure Strategies
- 3.DDoS Attack Countermeasures

##### Lesson - DoS/DDoS Protection Tools

- 1.Advanced DDoS Protection Appliances

## 2.DoS/DDoS Protection Tools

### Module - Session Hijacking

#### Lesson - Session Hijacking Concepts

- 1.What is Session Hijacking?
- 2.Why Session Hijacking is Successful?
- 3.Session Hijacking Process
- 4.Packet Analysis of a Local Session Hijack
- 5.Types of Session Hijacking

#### Lesson - Network Level Session Hijacking

- 1.TCP/IP Hijacking
- 2.IP Spoofing: Source Routed Packets
- 3.MiTM Attack Using Forged ICMP and ARP Spoofing

### Module - Evading IDS, Firewalls

#### Lesson - IDS, Firewall Concepts

- 1.Intrusion Detection System (IDS)
- 2.Firewall

#### Lesson - IDS, Firewall

- 1.Intrusion Detection Tool
- 2.Firewalls

#### Lesson - Web Server Attack Tools

- 1.Metasploit
- 2.Web Server Attack Tools

### Module - Hacking Web Applications

#### Lesson - Web App Threats

- 1.OWASP Top 10 Application Security Risks – 2017
- 2.Other Web Application Threats

#### Lesson - Web Application Hacking Tools

- 1.Web Application Hacking Tools

#### Lesson - Web App Security Testing Tools

- 1.Web Application Security Testing Tools
- 2.Web Application Firewall

### Module - SQL Injection

#### Lesson - SQL Injection Concepts

- 1.What is SQL Injection?
- 2.SQL Injection
- 3.Understanding HTTP POST Request
- 4.Understanding Normal SQL Query
- 5.Understanding an SQL Injection Query
- 6.Understanding an SQL Injection Query – Code Analysis
- 8.Example of a Web App Vulnerable to SQL Injection
- 9.Example of a Web Application Vulnerable to SQL Injection: Attack Analysis

## 10.Example of SQL Injection

### Lesson - Types of SQL Injection

#### 1.Types of SQL Injection

### Lesson - SQL Injection Methodology

#### 1.SQL Injection Methodology

### Lesson - SQL Injection Tools

#### 1.SQL Injection Tools

### Lesson - Countermeasures

#### 1.How to Defend Against SQL Injection Attacks?

#### 2.SQL Injection Detection Tools

#### 3.SQL Injection Detection Tools

## Module - Hacking Wireless Networks

### Lesson - Wireless Concepts

#### 1.Wireless Terminologies

#### 2.Wireless Networks

#### 3.Wireless Standards

#### 4.Service Set Identifier (SSID)

#### 5.Wi-Fi Authentication Modes

### Lesson - Wireless Encryption

#### 1.Types of Wireless Encryption

#### 2.WEP vs. WPA vs. WPA2

#### 3.WEP Issues

### Lesson - Wireless Threats

#### 1.Wireless Threats

### Lesson - Wireless Hacking Methodology

#### 1.Wireless Hacking Methodology

### Lesson - Wireless Hacking Tools

#### 1.WEP/WPA Cracking Tools

#### 2.WEP/WPA Cracking Tool for Mobile

#### 3.Wi-Fi Sniffer

#### 4.Wi-Fi Traffic Analyzer Tools

#### 5.Other Wireless Hacking Tools

## Module - Hacking Mobile Platforms

### Lesson - Mobile Platform Attack Vectors

#### 1.Anatomy of a Mobile Attack

#### 2.Mobile Spam

#### 3.SMS Phishing Attack (SMiShing) (Targeted Attack Scan)

#### 4.Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections

### Lesson - Hacking Android OS

#### 1.Android OS

#### 2.Android Rooting

#### 3.Launching DoS Attack using Low Orbit Ion Cannon (LOIC)

4. Securing Android Devices
5. Android Security Tool: Find My Device
6. Android Security Tools
7. Android Vulnerability Scanner
8. Android Device Tracking Tools

#### Lesson - Mobile Spyware

1. Mobile Spyware
2. Mobile Spyware: mSpy
3. Mobile Spywares

#### Lesson - Mobile Device Management

1. Mobile Device Management (MDM)
2. Mobile Device Management Solutions
3. Bring Your Own Device (BYOD)

#### Module - Cryptography

##### Lesson - Basic Cryptography Concepts

1. Cryptography

##### Lesson - Cryptography Tools

1. MD5 Hash Calculators
2. Hash Calculators for Mobile
3. Cryptography Tools
4. Cryptography Tools for Mobile

##### Lesson - Email Encryption

1. Digital Signature

##### Lesson - Disk Encryption

1. Disk Encryption
2. Disk Encryption Tools