Digital Ethical Hacking Course Curriculum

Add - on

Networking

1. Introduction to Networking
2. OSI Model
3. TCP/IP Vs. OSI Model
4. Protocols
5. IP address Vs. MAC address

Objective

- Understanding of basic networking terminologies, topologies, protocols and addressing scheme.

Theory / Practical

Theory

Duration

5 Hours

Model 1

Introduction to Hacking

1. Introduction To Hacking
2. Essential Terminology
3. Confidentiality Integrity Availability (C.I.A)
4. Types of Hacker
5. Types of System Attack
6. Impact of Hacking

Objective

- Understanding of Information Security and essential terminology used in Ethical Hacking.

Theory / Practical

Theory

Duration

2 Hours

Model 2

Information Gathering/ Vulnerability Scanning

1. Footprinting Concepts
2. Footprinting Methodology
3. Footprinting through Social Networking Sites
4. Email Footprinting
5. WHOIS Footprinting
6. Network Scanning
7. Scanning Techniques
8. Scan for Vulnerability
9. Vulnerability Assessment
10. Network Vulnerability Scanning
11. Vulnerability Scanning for Mobile

Objective

- Techniques of Gathering information about potential target. Finding Weak areas of target for exploitation. Scanning and classification of vulnerability found.

Theory / Practical

Practical

Duration

3 Hours

Model 3

Malwares (Virus,Worm,Trojan…)

1. Introduction to Malware
2. Concepts of Virus,Worm,Trojan
3. Types of Trojans
4. Types of Virus and Worms
5. Malware Reverse Engineering
6. Penetration Testing

Objective

- Insight of Malware Learn how to detect and quantify Virus,Worm,Trojan and other types of malware. Reverse engineering of Malware codes

Theory / Practical

Practical

Duration

3 Hours

Model 4

System Hacking

1. System Hacking Goals
2. Methodology
3. Password Cracking
4. Key loggers
5. Spyware
6. Covering Tracks

Objective

- Understanding the process of exploiting vulnerabilities, password cracking, post exploitation and clearing tracks

Theory / Practical

Practical

Duration

3 Hours

Model 5

Sniffing

1. What is Sniffing?
2. Types of Sniffing
3. IP Spoofing
4. MAC Spoofing
5. DHCP Hijacking
6. ARP Poising
7. DNS Poising
8. Network Sniffing
9. Online credential sniffing and countermeasures
10. Sniffing Detection
11. Web Sniffing and patching

Objective

- Understanding of Network sniffing and packet spoofing. Tools used for network stress testing

Theory / Practical

Practical

Duration

3.5 Hours

Model 6

Web Site and Web server Hacking

1. Webserver Attacks
2. Attack Methodology
3. Webserver Footprinting Tools
4. Enumerating Webserver Information
5. Webserver Attack
6. Metasploit
7. Webserver Security
8. Web Server Security Scanner
9. SQL Injection Attacks
10. Cross-Site Scripting (XSS) Attacks
11. Cross-Site Request Forgery (CSRF) Attack
12. Session Fixation Attack
13. Cookie/Session Poisoning
14. Buffer Overflow Attacks
15. CAPTCHA Attacks
16. Improper Error Handling
17. Web Services XML Poisoning
18. Web App Hacking Methodology
19. Attacking Web Servers
20. Analyze Web Applications
21. Attack Authentication Mechanism
22. Authorization Attack Schemes
23. Attack Session Management Mechanism
24. Perform Injection Attacks
25. Web Application Hacking Tools

Objective

- Advanced Web site and Web server attack methods and configuration vulnerability. Advanced XSS and CSRF attack with advanced SQL injection. Identifying weak configuration and quantifying the founded vulnerabilities. Uses of Web Application Pen testing tools.

Theory / Practical

Practical

Duration

3.5 Hours

Model 7

SQL Injection and XSS

1. SQL Injection
2. Types of SQL Injection
3. SQL Injection Attacks
4. Advanced SQL Injection
5. SQL Injection Counter-measures
6. Cross-Site Scripting (XSS) Attacks
7. Cross-Site Scripting Attack Scenario
8. Advanced XSS Attack
9. Cross-Site Request Forgery (CSRF) Attack

Objective

- Web Application hacking with XSS and SQL injection. Advanced tools used for attacking sophisticated security environment on web servers as well as code level attacks on front end of web application or website. Quantifying and applying security practices

Theory / Practical

Practical

Duration

4 Hours

Model 8

Buffer Overflow

1. Buffer Overflows: Attacks and Defences for the Vulnerability of the Decade
2. Basic Integer Overflows
3. Exploiting Format String Vulnerabilities
4. Stack based Buffer overflow
5. Heap Based Buffer Overflow

Objective

- Buffer overflow attack scenario and exploitation for good. And to find possible breach

Theory / Practical

Practical

Duration

3 Hours

Model 9

Cross Platform System Hacking and Wireless Hacking (Linux/Windows/Server)

1. Hacking Methodology
2. Exploiting Bugs in Linux / Windows
3. Stress testing of Operating system
4. Fuzzing
5. Network Hacking
6. Bypassing Authentication
7. Exploiting Operating system level vulnerabilities
8. Exploit identification and Payload Management

Objective

- Cross Platform hacking and exploiting possible vulnerabilities in popular operating system platform. Understanding 802.11 weakness, WEP cracking, de-authentication and its countermeasures.

Theory / Practical

Practical

Duration

4 Hours

Model 10

Mobile Pentesting

1. Hacking Android OS
2. Android Trojan
3. Securing Android Devices
4. Hacking iOS
5. Jailbreaking iOS
6. Securing iOS Devices
7. Mobile Device Management (MDM)
8. Bring Your Own Device (BYOD)
9. Mobile Penetration Testing

Objective

- Mobile penetration testing. Hacking into Android, Windows and iOS platform to find possible vulnerabilities in native code as well as in app based structure

Theory / Practical

Practical

Duration

3 Hours

Model 11

Network DOS and DDOS

1. DoS/DDoS Attack
2. Botnets, Zombies
3. DoS/DDoS Attack Tools
4. Attack Forensics
5. Enabling TCP Intercept
6. DoS/DDoS Protection Tools
7. DoS/DDoS Attack Penetration Testing
8. Mitigate Attacks
9. Deflect Attacks
10. Application Level Flood Attacks

Objective

- Network pentesting and sterss testing with advanced Dos and DDoS attacks.

Theory / Practical

Practical

Duration

4 Hours

Model 12

Cryptography

1. Cryptography
2. Encryption Algorithms
3. Cryptography Advantages
4. Ciphers
5. Data Encryption Standard (DES)
6. Advanced Encryption Standard (AES)
7. RC4, RC5, RC6 Algorithms
8. RSA
9. Public Key Infrastructure(PKI)
10. Disk Encryption

Objective

- Understanding of Cryptography and its data hiding techniques with latest algorithms and possible tools

Theory / Practical

Duration

4 Hours

Model 13

Penetration Testing IDS/IPS and Firewall

1. Penetration Testing Methodology
2. Network Penetration testing
3. Application Penetration Testing
4. Report Generation

Objective

- Penetration Testing methodology and area of deployment as well as a effective Report creation

Theory / Practical

Practical

Duration

3 Hours

Total - 45 Hours