Ethical Hacking Syllabus

ROOMAN
INNOVATE INTEGRATE EMPOWER

Rooman Technologies Pvt Ltd
#30, 12th Main, 1st Stage Rajajinagar,
Bangalore – 560010

E-mail: info@rooman.net
Phone: 7022020000

Module 1: Principles of Hacking & Legal Parameters

Ethical Hacking Overviews

- Hacking concept, what is hacking?
- Terms we use in hacking.
- Need of Ethical hacking.
- Cases of Hacking in India & across the globe

Principles of Ethical hacking

- Basic Principle
- Commandments of Ethical Hacking

Hacking Methodologies

- Types of Hacking.
- Building the foundation for Ethical hacking
- Hacking Phases

Role of Ethical Hacker

- Types of Hackers
- Roles and Responsibilities

Scope & limitations of hacking.

- Advantages & scope for hacking
- Drawbacks & Limitation of hacking

Cyber Threats and Attacks Vectors

- Threats & categories
- Attack Vectors and Exploitation

Hacking tools and techniques

- Common Hacking Tools
- Hacking Techniques & Approaches

Policies and Controls

Information Security policies

- Risk Management & Incident Management
- Information Security controls
- Data Management

Overview of PT / VA.

- Concept of Penetration testing
- Types of Penetration testing
- Phases of Penetration testing
- Vulnerability Assessment by Penetration testing

Module 2 : Viruses, Trojans, Malwares, and OS Level Attacks and Counter Measures. Malware Analysis.

Malware Overviews

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

Virus Worm & Trojan Concepts

- Introduction to Viruses, Worms & Trojan
- Types of Virus, Worms &Trojan
- Fake Antiviruses
- How Did Antivirus Works.

Malware Analysis

- Introduction to Malware Analysis
- Malware Analysis Procedure
- Malware Detection Method.

Module 3 : Foot printing , Enumeration, Scanning, Sniffing, Social Engineering

Footprinting through Search Engines, Web Services,

- Information Gathering Using Google Advanced Search and Image Search.
- VoIP and VPN Footprinting through Google Hacking Database

Footprinting through Web Services

- Finding Company's Top-level Domains (TLDs) and Sub-domains
- Finding Location, People search, Professional search.

Enumeration

- Techniques for Enumeration, Services and Ports to Enumerate
- NetBIOS, SNMP, LDAP Enumeration
- Information Gathering Using Groups, Forums, and Blogs.

Scanning targets

- Network Scanning Concepts.
- Scanning Tools and Techniques
- Scanning Pen Testing
- Port Scanning & Countermeasures

Sniffing Network

- Sniffing Concepts & Techniques
- WireShark installing & concept
- Sniffing Detection Techniques

Social Engineering

- Social Engineering Concepts
- Social Engineering Techniques
- Insider Threat / Insider Attack.
- Social Engineering Countermeasures

Module 4: SQL Injection, DOS Attacks, Session hijacking and System hacking

SQL Injection

- Basics to the SQL queries
- How Injection Can be done
- Cross Site Scripting Attacks

DOS Attacks

- DoS/DDoS Attack Techniques.
- DDoS Case Study
- DoS/DDoS Attack Tools

Session Hijacking

- Session Hijacking Concepts,
- Network Level Session Hijacking
- Client side Hijacking.

System Hacking

- System Hacking Concepts
- Cracking Passwords
- Escalating Privileges
- Hiding Files and Covering tracks

Module 5: Web Applications and Web Servers attacking methodology and Counter measures.

Basics to Web application & threats

- Basics of Web Application and Technology stack.
- OWASP Top 10 Application Security Risks – 2017

OWASP Top 10 Application Security Risks – 2017

- Injection Flaws
- File Injection Attack
- Broken Authentication
- Sensitive Data Exposure
- XML External Entity (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS) Attacks
- Insecure Deserialization
- Using Components with Known Vulnerabilities

Web Hacking methodology and tools

- Web App Hacking Methodology and its foot printing.
- Password Attacks:
- Password Functionality Exploits
- Password Guessing and Brute-forcing

Introduction to Web Server

- Web Server Concepts
- Web server attacks
- Web Server Attack Methodology
- Web Server Attack Tools

Counter measures

- Detecting Web Server Hacking Attempts
- Patch Management
- Web Server Security Tools

Module 6: IoT and Cloud Attacks and Defense Mechanisms

IOT Concept and Attacks

- Basic of IOT, Architecture, Technology and Protocols
- Challenges, Opportunity in IOT
- OWASP Top 10 IOT Vulnerabilities and Obstacles
- Hacking IOT Devices
    - DDos Attack
    - Jamming Attack
    - Botnets
    - Man In middle concept
    - Data & Identity Theft

Cloud Computing Overview

- Introduction to Cloud & Virtualization
- Cloud Deployment and responsibilities

Threats and attack in Cloud

- Topic 1 : Service Hijacking
    - Social Engineering
    - Network sniff
    - XSS attack
- DNS (Domain Name system attack)

Cloud Security and tools

- Control Layers and Responsibilities
- Cloud Computing Security Consideration

Module 7: **Mobile & Wireless Networks Hacking and Counter measures**

Mobile Hacking

- Introduction to the Mobile architecture
- Working principle for mobile OS
- Security of the application used in Mobiles
- Hacking Methodology for mobile with Metasploit

Wireless Overview

- Introduction to Terminology, Networks, Standards
- Types of Wireless Authentication and Encryption
    - WEP (Wired Equivalent Privacy) Encryption
    - WPA (Wi-Fi Protected Access) Encryption
- WPA2 (Wi-Fi Protected Access 2) Encryption

Wireless Hacking Methodology

- Wi-Fi Discovery
- GPS Mapping
- Traffic canalizing
- Launch Wireless attacks
- Crack Wi-Fi Encryption

Module 8 : Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures

Basics of Firewalls, IDS, Honeypots

- What is Firewall & Examples
- What is IDS & examples
- What is Honeypots & examples
- Case study of Bypassing Firewall ,IDS, Firewall

IDS/Firewall/Honeypot Evasion Techniques

- Packet Fragmentation and Source Routing
- Working with SNORT [Detection Tool]
- IP address Decoy and Spoofing
  - IP Spoofing Detection Techniques: Direct TTL Probes
  - IP Spoofing Detection Techniques: IP Identification Number
  - IP Spoofing Detection Techniques: TCP Flow Control Method
  - IP Spoofing Countermeasures

Module 9 : Cryptology, Vulnerability Analysis, Logging and Audit.

Introduction to Cryptography Concepts

- Types of Cryptography
- Government Access to Keys (GAK)

Encryption Algorithms

- Ciphers
- Data Encryption Standard
- Advanced Encryption Standard
- RC4, RC5, and RC6 Algorithms

Email, Disk Encryption and Cryptanalysis

- Digital Signature, SSL, TLS
- Cryptography Toolkit & Disk Encryption
- Cryptography Attacks
  - Brute-Force Attack
  - Meet-in-the-Middle Attack on Digital Signature Schemes
  - Side Channel Attack
  - Hash Collision Attack
  - DUHK Attack
  - Rainbow Table Attack

Vulnerability Analysis

- Vulnerability Assessment Concept & Solutions
- Vulnerability Assessment Tools & Reports
- Comparing Security Audit, Vulnerability Assessment, and Penetration Testing

Module 10 : Capture the flag [CTF] .

Bandit Overthewire [WarGame]

- Understanding of Kali Linux commands.
- Using commands situation based.

Natas Overthewire [WarGame]

- Understanding of web application.
- Web application tricks to get data.
- Doing pentesting Situation based.

Mr. Robot

- Installing and working on Kali Linux.
- Vulnerability Assessment Concept & Solutions.
- Vulnerability Assessment Tools & Reports.