DIGI SAMURAI

Academics & Consulting

Devoted to providing the best service possible at a competitive price to bridge the quality gap in the industry

Ethical Hacking

About Course

One of the most challenging and developing topics in the industry is ethical hacking. By enrolling in this course, you will be trained by seasoned industry experts who will bring industry experience to your bowl. The course is designed with the ideal blend of gaining real-world experience and solid background knowledge.

Learn

Discover the tools & techniques used by any professional hackers in the industry

Implement

Put into action the knowledge gained in real-life simulated labs to hone your skills

Adapt

Get acquainted with newly acquired skills & perspective and transform yourself

WARNING – Course contains real world simulation of hacking. Trainer or Institute is not responsible for misuse of the gained knowledge

Course Duration – 60 Hours

COURSE OVERVIEW

1. Welcome to Cyber World

1. Introduction to Information Security
   1.1. What is Information Security?
   1.2. How is it different than Cyber Security?
2. The Pillar of Cyber Security – CIA Triad
3. DAD – Disclosure, Alteration & Destruction
4. Organisation's Security – People, Process & Technology
5. Threat, Vulnerability & Risk

2. Introduction to Ethical Hacking

1. What is Hacking?
2. How hacking can be ethical?
3. Different Types of Hackers
4. Common Hacking Terminologies
5. Steps of Hacking
6. Different Standards & Methodologies

3. Feasibility Study, Scoping & Engagement Methodology

1. Feasibility Study of the Engagement
   1.1. Operational Feasibility
   1.2. Financial Feasibility
   1.3. Technical Feasibility
2. Scoping of the Engagement
   2.1. Scoping of Network Security Testing
   2.2. Scoping of Web Application Security Testing
   2.3. Scoping of Mobile Application Security Testing
3. Determining the Methodology for Testing
   3.1. Selecting the Standards to Conduct the Test
   3.2. Customizing the Standard based on Clients' Requirement

4. Configuring Lab for Practice

1. Choosing Virtual Machine (VM)
2. Downloading & Installing VMs
   2.1. Playing with VM Configurations
   2.2. VM Snapshot – Your Saviour
3. Configuring the Environment to Hack
   3.1. Installing Kali Linux – Hackers System
   3.2. Installing Victim Systems

3.2.1. Installing Windows Operating System
3.2.2. Installing Linux Operating System
3.2.3. Installing Metasploitable

5. Network Security Vulnerability Assessment

1. OSINT/Foot Printing
   1.1. What is Footprinting?
   1.2. Footprinting Objectives
   1.3. Footprinting Methodologies
      1.3.1. Footprinting through Search Engines
      1.3.2. Footprinting through Advance Google Hacking Techniques
      1.3.3. Footprinting through Social Networking Sites
      1.3.4. Website Footprinting
      1.3.5. WHOIS Footprinting
      1.3.6. DNS Footprinting
      1.3.7. Network Footprinting
      1.3.8. Using Spiderfoot
      1.3.9. Using OSINT Framework
2. Scanning
   2.1. Scanning IPs using Nmap
   2.2. Basic scanning techniques
   2.3. Discovery Options
   2.4. Firewall Evasion Techniques
   2.5. Version Detection
   2.6. Output Options
   2.7. Automating Nmap Scripting
3. Enumeration
   3.1. Executes Individual Scripts
   3.2. Executes Multiple Scripts
   3.3. Executes Scripts by Category
   3.4. Executes Multiple Scripts Categories
   3.5. Troubleshoot Scripts
   3.6. Update the Scripts Database
   3.7. Scripts Categories
      3.7.1. All
      3.7.2. Auth
      3.7.3. Default
      3.7.4. Discovery
      3.7.5. External
      3.7.6. Intrusive
      3.7.7. Malware
      3.7.8. Safe
      3.7.9. Vuln

4. Vulnerability Identification & Analysis
   4.1. Analysing Vulnerabilities using Automated Vulnerability Scanners
5. Exploiting the Detected Vulnerability with Metasploit
6. Identifying and Installing Patches to fix Vulnerabilities

6. Email Security

1. How Email Works?
2. Pillars of Email Authentication – SPF, DKIM & DMARC
3. Checking Emails Security Configurations
4. Testing the Email Security with Spoofing

7. Social Engineering

1. What is Social Engineering?
2. URL Re-directions to sabotage victims
3. Harvesting Facebook Credentials using Kali Linux
4. Compromising 2FA of Gmail using Social Engineering
5. Notorious IDN Homograph Attacks
6. How to Identify Phishing Mail?
7. Using spoofing to leverage the social engineering attacks

8. Web Application Security Testing

1. Web Application Working Analogy
2. Static vs Dynamic Web Application
3. Web Application Security Risks
   3.1. Understanding OWASP Top 10 Web Application
4. Web Applications Security Testing
   4.1. Authenticated vs Unauthenticated Security Scanning
   4.2. Scanning with Automated Web Security Vulnerability Scanner
   4.3. Eliminating False Positives with Manual Testing
5. Manual Testing with Burp Suite
   5.1. Introducing to Burp Suite
   5.2. Configuring the Proxy
   5.3. Understanding Burp Suite
6. Web Application Security Standards

9. Mobile Application Security Testing

1. Overview of Mobile Application Architecture
2. Understanding the Risk of Mobile Breach
3. OWASP Top 10 for Mobile Application Security
4. Conducting Static Mobile Application Security Testing using MobSF

10. Wireless Security

1. How wireless transmission works?
2. Understanding the different types of Wireless Security IEEE Standards
3. Understanding Wireless Adaptors
4. Testing Wi-Fi with Automated Wireless Security Scanners

11. Malware

1. What is a Malware?
2. Understanding Different Types of Malwares
   - 2.1. Ransomware
   - 2.2. Spyware
   - 2.3. Adware
   - 2.4. Trojans
   - 2.5. Worms
   - 2.6. Rootkits
   - 2.7. Keyloggers
   - 2.8. Mobile Malware
   - 2.9. Wiper Malware

12. Cloud Security

1. Overview of Cloud Architecture
   - 1.1. Cloud Consumer
   - 1.2. Cloud Provider
   - 1.3. Cloud Carrier
   - 1.4. Cloud Auditor
   - 1.5. Cloud Broker
2. Different types of Cloud Deployment Models
   - 2.1. Private Cloud
   - 2.2. Public Cloud
   - 2.3. Community Cloud
   - 2.4. Hybrid Cloud
   - 2.5. Multi Cloud
3. Types of Cloud Computing Services
   - 3.1. Infrastructure-as-a-Service (IaaS)
   - 3.2. Platform-as-a-Service (PaaS)
   - 3.3. Software-as-a-Service (SaaS)
   - 3.4. Identity-as-a-Service (IDaaS)
   - 3.5. Security-as-a-Service (SECaaS)
   - 3.6. Container-as-a-Service (CaaS)
   - 3.7. Function-as-a-Service (FaaS)
4. Risks of Cloud Computing
5. OWASP Top 10 Cloud Security Risks

13. IoT Security

1. What is Internet of Things (IoT)?
2. Understanding IoT Eco-system
3. Threat Modelling IoT Eco-system
4. OWASP Top 10 for IoT
5. Different IoT Standards

14. Cryptography

1. What is Cryptography?
2. Plain Text vs Cipher Text
3. Encoding
4. Encryption
5. Hashing & Salting

15. Sniffing

1. Sniffing with Wireshark
   1.1. Capturing Live Network Data
   1.2. Analysing the Captured Packets
2. Experience the Difference between HTTP and HTTPS

16. Writing a Security Report

1. How to write a professional security report
2. Do's & Don't of a security report

Course Pre-requisite

Basic working knowledge of Computer, Internet & Network

Course Duration

60 Hours to Master Hacking from ZERO to HERO

OTHER COURSES OFFERED

Foundation Courses

- Networking for Hackers
- Linux for Hackers
- Python for Hackers
- Java Script for Hackers
- Cryptography for Hackers

Offensive Security Courses

- OSINT
- Network Pentesting & Config Review
- Web Security Testing & GIGW
- Mobile Application Security Testing
- API Security Testing
- IoT Pentesting
- Wireless Hacking
- Vulnerability Management
- Cloud Security Testing

Defensive Security Courses

- Cyber Crime & Digital Forensic
- SOC
- IAM & System Admin
- Threat Intelligence & Threat Hunting

Compliance Courses

- ISO 27001 (ISMS)
- ISO 27701 (PIMS)
- ISO 22301 (BCMS)
- ISO 31000 (RM)
- ISO 9001 (QM)
- ITGC
- PCI DSS
- WFH Assessment

Special Program: 15 Months Post Graduation Diploma for Information Security

CONTACT US

www.digisamurai.co.in

+91 8910632224

+91 7595887833