Ethical Hacking / Cyber Security

Duration: - 35 Hrs **Cost Per Head**: ₹**4,500/-**

Module 01: Introduction to Ethical Hacking

Information Security Overview: Elements of Information Security-Motives-Goals and Objectives of Information Security Attacks, Classification of Attacks-Information Warfare
Hacking Concepts : What is Hacking-Who is a Hacker- Hacker Classes-Hacking Phase: Reconnaissance, Scanning, Gaining Access , Maintaining Access and Clearing Tracks **Ethical Hacking Concepts** : What is Ethical Hacking?-Why Ethical Hacking is Necessary-Scope and Limitations of Ethical Hacking - Skills of an Ethical Hacker
Information Security Controls: Information Assurance (IA), Defence-in-Depth -What is Risk-Risk Management -Cyber Threat Intelligence -Threat Modelling -Incident Management- Incident Handling and Response
Role of AI and ML in Cyber Security: How Do AI and ML Prevent Cyber Attacks?
Information Security Laws and Standards: Payment Card Industry Data Security Standard (PCI DSS) - ISO/IEC 27001:2013-Health Insurance Portability and Accountability Act (HIPAA) · Sarbanes Oxley Act (SOX) -The Digital Millennium Copyright Act (DMCA) - The Federal Information Security Management Act (FISMA) -Cyber Law in Different Countries

Module 02: Foot printing and Reconnaissance

Foot printing Concepts: What is Foot printing-Foot printing through Search Engines? Footprint Using Advanced Google Hacking Techniques · Google Hacking Database
Foot printing through Web Services: Finding a Company's Top-Level Domains (TLDs) and Sub-domains · finding the Geographical Location of the Target –Foot printing through Social Networking Sites -Harvesting Email Lists -Determining the Operating System
Foot printing through SHODAN
Website Foot printing: Website Foot printing -Website Foot printing using Web Spiders – Mirroring Entire Website
Email Foot printing: Tracking Email Communications
Whois Foot printing: Who is Lookup, Finding IP Geolocation Information?
DNS Foot printing: Extracting DNS Information -Reverse DNS Lookup
Network Foot printing: Locate the Network Range - Traceroute
Foot printing through Social Engineering: Foot printing through Social Engineering -Collect Information Using Eavesdropping, Shoulder Surfing, Dumpster Diving,
Foot printing Countermeasures: Foot printing Countermeasures

Module 03: Scanning Networks

Network Scanning Concepts: Overview of Network Scanning -TCP Communication Flags - TCP/IP Communication
Host Discovery -Host Discovery Techniques
Port and Service Discovery -Port Scanning Techniques
OS Discovery (Banner Grabbing/OS Fingerprinting) -OS Discovery/Banner Grabbing
Scanning Beyond IDS and Firewall -IDS/Firewall Evasion Techniques

IP Address Spoofing - Proxy Servers, Proxy Chaining, Anonymizers, Tails
Enumeration Concepts: What is Enumeration, Techniques for Enumeration, Services and Ports? to Enumerate -Enumeration Countermeasures - Enumeration Countermeasures
Vulnerability Analysis: Vulnerability Research, Vulnerability Assessment, Vulnerability-Management Life Cycle ▪ Pre-Assessment Phase -Vulnerability Assessment Phase - Post Assessment Phase -Vulnerability Assessment Reports - Penetration Testing

Module 04: System Hacking

System Hacking Concepts -System hacking Goals -Gaining Access
Cracking Passwords - Types of Password Attacks, Password Salting
Vulnerability Exploitation - Exploitation - Buffer Overflow- Escalating Privileges-Maintaining Access -Key logger - Spyware -Ransomware -Rootkits -Steganography –Clearing Logs, Malware Concepts, Malware Analysis
Countermeasures

Module 05: Sniffing

Sniffing Concepts -Types of Sniffing -How an Attacker Hacks the Network Using Sniffers – Protocols-Vulnerable to Sniffing - Hardware Protocol Analysers - SPAN Port -Wiretapping
Sniffing Technique: MAC Address/CAM Table, How CAM Works, What Happens When a CAM Table Is Full-MAC Flooding -Switch Port Stealing - How to Defend against MAC Attacks
DHCP Attacks -How DHCP Works, DHCP Starvation Attack, Rogue DHCP Server Attack, How to Defend Against DHCP Starvation and Rogue Server Attacks
ARP Poisoning -What Is Address Resolution Protocol (ARP) - ARP Spoofing Attack - Threats of ARP Poisoning, How to Defend Against ARP Poisoning, Configuring DHCP Snooping and Dynamic ARP, Inspection on Cisco Switches
Spoofing Attacks -MAC Spoofing/Duplicating, DNS Poisoning
Sniffing Tools -Sniffing Tool: Wireshark
Countermeasures

Module 06: Social Engineering

Social Engineering Concepts: What is Social Engineering?-Phases of a Social Engineering Attack-Social Engineering Techniques -Types of Social Engineering -Insider Threats – Impersonation on Social Networking Sites- Identity Theft
Countermeasures

Module 07: Denial-of-Service

DoS/DDoS Concepts: What is a DoS Attack- What is a DDoS Attack?-DoS/DDoS Attack Techniques -Distributed Reflection Denial-of-Service (DRDoS) -Attack · Botnets
Countermeasures

Module 08: Session Hijacking

Session Hijacking Concepts: What is Session Hijacking? -Types of Session Hijacking - Spoofing vs. Hijacking
Application Level Session Hijacking -Session Hijacking Using Proxy Servers
Network Level Session Hijacking -TCP/IP Hijacking
Countermeasures

Module 09: Evading IDS, Firewalls, and Honeypots

IDS, IPS, Firewall, and Honeypot Concepts: Intrusion Detection System (IDS) -Types of Intrusion Detection Systems -Intrusion Prevention System (IPS) -Firewall -Demilitarized Zone (DMZ) - Honeypot, HTTP Tunnelling -Evasion Techniques
Countermeasures

Module 10: Hacking Web Servers

Web Server Concepts: Web Server Types
Web Server Attacks: Web Server Foot printing -Website Mirroring, Password Cracking, Server-Side Request Forgery (SSRF) Attack
Vulnerability Scanning: Finding Exploitable Vulnerabilities
Countermeasures

Module 11: Hacking Web Applications

Web Application Concepts: Introduction to Web Applications
Web Application Threats: OWASP Top 10 Application Security Risks – 2017
Web Application Hacking
Methodology SQL Injection Concepts: What is SQL Injection? -Types of SQL Injection
Countermeasures

Module 12: Hacking Wireless Networks

Wireless Concepts: Wireless Terminology - Wireless Networks - Wireless Standards-Service Set Identifier (SSID) -Wi-Fi Authentication Modes -Types of Wireless Antennas
Wireless Encryption: Types of Wireless Encryption
Wireless Threats: Password Attacks -Jamming Signal Attack - Bluetooth Hacking
Countermeasures

Module 13: Hacking Mobile Platforms

Mobile Platform Attack Vectors
Hacking Android OS: Android Exploitation, Android Rooting, Securing Android Devices
Bring Your Own Device (BYOD)
Mobile Security Guidelines and Tools

Module 14: IoT and OT Hacking

IoT Concepts: IoT Hacking -What is the IoT? - How the IoT Works -IoT Architecture -IoT Application Areas and Devices · IoT Technologies and Protocols - IoT Communication Models - Challenges of IoT

IoT Attacks - Identifying and Accessing IoT Devices, DDoS Attack, Rolling Code Attack, Blue Borne Attack, Jamming Attack

OT Concepts: What is OT? - Essential Terminology - IT/OT Convergence (IIOT) - The Purdue Model -Challenges of OT - Introduction to ICS - Components of an ICS

OT Attacks

Countermeasures

Module 15: Cloud Computing

Cloud Computing Concepts: Introduction to Cloud Computing -Types of Cloud Computing Services - Cloud Deployment Models -Virtual Machines -Server less Computing - Server less Vs. Containers

Cloud Computing Threats

Module 16: Cryptography

Cryptography Concepts: Cryptography, Government Access to Keys (GAK)

Encryption Algorithms - Data Encryption Standard (DES) and Advanced Encryption Standard (AES) · RC4, RC5, and RC6 Algorithms **,**Two fish and Three fish**,** DSA -Rivest Shamir Adelman (RSA) -Message Digest (One-Way Hash) Functions -Secure Hashing Algorithm (SHA) -HMAC

Public Key Infrastructure (PKI): Certification Authorities -Signed Certificate (CA) Vs. Self-Signed Certificate - Digital Signature -Secure Sockets Layer (SSL) - Transport Layer Security (TLS) - Pretty Good Privacy (PGP)

Disk Encryption

Cryptanalysis

Cryptography Attacks