ETHICAL HACKING & CYBER SECURITY

Dear Student,
Based upon your enquiry we are pleased to send you the course curriculum for Ethical Hacking & Cyber Security. Given below is the brief description for the course you are looking for:

Introduction to Ethical Hacking

- Technology Brief & Objectives of Information Security Attacks
- Top Information Security Attack Vectors
- Types of Attacks on a System
- Ethical Hacking Introduction
- Phases of Ethical Hacking
- Information Security Controls
- Threat Modeling
- Information Security Policies
- Physical Security
- Incident Management Process
- Responsibilities of Incident Response Team
- Vulnerability Assessment and its type
- Penetration Testing
- Important for Penetration testing
- Types and Phases of Penetration Testing
- Security Testing Methodology
- Information Security Laws and Standards (PCI-DSS, ISO-27001, HIPPA, SOX)

Footprinting & Reconnaissance

- Pseudonymous Footprinting
- Internet Footprinting
- Footprinting Methodology
- Footprinting through Search Engines
- Footprinting using Advanced Google Hacking Techniques
- Footprinting through Social Networking Sites
- Website/Email/WHOIS/DNS/Network Footprinting
- Footprinting through Social Engineering
- Footprinting Tools
- Maltego Tool Overview
- Recon-ng Overview
- Countermeasures of Footprinting

Gathering information using Windows Command Line Utilities
Downloading a Website using Website Copier tool (HTTrack)
Gathering information using Metasploit

Scanning Networks

TCP Communication
Creating Custom Packet Using TCP Flags
Scanning Methodology
Checking for Live Systems
Check for Open Ports
Hping Commands
Xmas Scanning
Scanning Beyond IDS
OS Fingerprinting & Banner Grabbing
Draw Network Diagrams
Creating Network Topology Map using Tool
Prepare Proxies

Enumeration

Enumeration and its Techniques
Services and Ports to Enumerate
Services Enumeration using Nmap
NetBIOS Enumeration Tool
Enumeration using SuperScan Tool
Enumerating Shared Resources Using Net View
Enumeration using SoftPerfect Network Scanner Tool
SNMP Enumeration
SNMP Enumeration
Simple Network Management Protocol
LDAP Enumeration
Lightweight Directory Access Protocol (LDAP)
LDAP Enumeration Tool:
NTP Enumeration
Network Time Protocol (NTP)
SMTP Enumeration
Simple Mail Transfer Protocol (SMTP)
SMTP Enumeration Technique

DNS Zone Transfer Enumeration Using NSLookup
Enumeration Countermeasures

Vulnerability Analysis

Vulnerability Assessment and its Life-Cycle
Vulnerability Assessment Solutions
Vulnerability Scoring Systems
Vulnerability Scanning
Vulnerability Scanning using Nessus Vulnerability Scanning Tool

System Hacking

System Hacking Methodology
Password Cracking
Online tool for default passwords
Rainbow Table using Winrtgen toolLab 6-3: Password Cracking using Pwdump7 and Ophcrack tool.
Escalating Privileges
Executing Applications
Hiding Files
NTFS Stream Manipulation
Steganography
Image Steganography
Covering Tracks
Clearing Audit Policies on Windows
Clearing Logs on Windows
Clearing logs on Linux

Malware Threats

Malware
Trojan Concept
Virus and Worms Concepts
Virus Analysis and Detection Methods
Malware Reverse Engineering
Sheep Dipping
Malware Analysis
HTTP RAT Trojan
Monitoring TCP/IP connection using CurrPort tool

Sniffing

- Introduction to Sniffing
- Types of Sniffing
- Hardware Protocol Analyzer
- SPAN Port
- Wiretapping
- MAC Attacks
- MAC Address Table / CAM TableMAC Flooding
- Switch Port Stealing
- Defend against MAC Attacks
- DHCP Attacks
- Dynamic Host Configuration Protocol (DHCP) Operation
- DHCP Starvation Attack
- Rogue DHCP Server Attack
- Defending Against DHCP Starvation and Rogue Server Attack
- ARP Poisoning
- Address Resolution Protocol (ARP)
- ARP Spoofing Attack
- Defending ARP Poisoning
- Spoofing Attack
- MAC Spoofing/Duplicating
- Configuring locally administered MAC address
- DNS Poisoning
- DNS Poisoning Techniques
- How to Defend Against DNS Spoofing
- Sniffing Tools
- Wireshark
- Introduction to Wireshark
- Countermeasures
- Defending Against Sniffing
- Sniffing Detection Techniques
- Promiscuous Detection Tool

Social Engineering

- Social Engineering Concepts
- Phases of a Social Engineering Attack
- Social Engineering Techniques

Types of Social Engineering
Insider Attack
Impersonation on Social Networking Sites
Risks of Social Networking in a Corporate Networks
Identify Theft Overview
The process of Identity theft
Social Engineering Countermeasures
Social Engineering using Kali Linux

Denial-of-Services

DoS/DDoS Concepts
How Distributed Denial of Service Attacks Work
DoS/DDoS Attack Techniques
Basic Categories of DoS/DDoS Attacks
Botnets
Botnet Setup
Propagation of Malicious Codes
Botnet Trojan
DoS/DDoS Attack Tools
Pandora DDoS Bot Toolkit
Other DDoS Attack tools
DoS and DDoS Attack Tool for Mobile
SYN Flooding Attack using Metasploit
SYN Flooding Attack using Hping3
Counter-measures
Detection Techniques
DoS/DDoS Countermeasure Strategies
Techniques to Defend against Botnets
Enabling TCP Intercept on Cisco IOS Software

Chapter Session Hijackin

Session Hijacking Techniques, its type and Process
Session Hijacking in OSI Model
Spoofing vs. Hijacking
Application Level Session Hijacking
Compromising Session IDs Using Man-in-the-Middle Attack, Man-in-the-Browser Attack & Client-side Attacks

Session Replay Attack
Session Fixation
Network-level Session Hijacking
The 3-Way Handshake
TCP/IP Hijacking
Source Routing
RST Hijacking
Blind Hijacking
Forged ICMP and ARP Spoofing
UDP Hijacking
Countermeasures
Session Hijacking Countermeasures
IPSec

Evading IDS, Firewall and Honeypots

IDS, Firewall and Honeypot Concepts
Intrusion Detection Systems (IDS)
Firewall
Honeypot
IDS, Firewall and Honeypot System
Intrusion Detection Tools
Evading IDS
Insertion Attack
Evasion
Denial-of-Service Attack (DoS)
Obfuscating False Positive Generation
Session Splicing
Unicode Evasion Technique
Evading Firewalls
Firewall Identification
IP Address Spoofing
Source Routing
By passing Techniques
Bypassing through SSH Tunneling Method
Bypassing Firewall through External Systems
IDS/Firewall Evasion Counter-measures
Configuring Honeypot on Windows Server 2016

Hacking Web Servers

Web server Concepts & Security Issue
Open Source Web server Architecture
IIS Web Server Architecture
Web server Attacks
DoS/DDoS Attacks
DNS Server Hijacking
DNS Amplification Attack
Directory Traversal Attacks
Man-in-the-Middle/Sniffing Attack
Phishing Attacks
Website Defacement
Web server Misconfiguration
HTTP Response Splitting Attack
Web Cache Poisoning Attack
SSH Brute-force Attack
Web Application Attacks
Attack Methodology
Information Gathering
Web server Footprinting
Web Server Footprinting using ToolMirroring a Website
Vulnerability Scanning
Session Hijacking
Hacking Web Passwords
Countermeasures
Countermeasures
Patch Management
Patches and Hotfixes
Patch Management
Microsoft Baseline Security Analyzer (MBSA)
Web server Security Tool

Hacking Web Applications

Web Application Concepts
Server Administrator
Application Administrator
Client

Web App Threats
Web App Hacking Methodology
Analyze Web Applications
Attack Authentication Mechanism
Authorization Attack Schemes
Session Management Attack
Perform Injection Attacks
Attack Data Connectivity
Countermeasures
Encoding Schemes

SQL Injection

SQL Injection Concepts and its type
How SQL Query worksSQL Injection Tools
In-Band SQL Injection
Inferential SQL Injection (Blind Injection)
Out-of-band SQL Injection
SQL Injection Methodology
Information Gathering and SQL Injection Vulnerability Detection
Launch SQL Injection Attacks
Advanced SQL Injection
Evasion Techniques
Evading IDS
Types of Signature Evasion Techniques
Counter-measures
Using IBM Security AppScan Standard

Hacking Wireless Networks

Wireless Concepts
Wireless Networks
Wi-Fi Technology
Types of Wireless Antenna
Wireless Encryption
WEP Encryption
WPA Encryption
WPA2 Encryption
Wireless Threats

Access Control Attacks
Integrity and Confidentiality Attacks
Availability Attacks & Authentication Attacks
Rogue Access Point Attack
Client Mis-association
Misconfigured Access Point Attack
Unauthorized Association
Ad Hoc Connection Attack
Jamming Signal AttackWireless Hacking Methodology
Wi-Fi Discovery & GPS Mapping
Wireless Traffic Analysis
Launch Wireless Attacks
Bluetooth Hacking & Bluetooth Attacks & Bluetooth Countermeasures
Wireless Security Tools
Wireless Intrusion Prevention Systems
Wi-Fi Security Auditing Tool
Hacking Wi-Fi Protected Access Network using Aircrack-ng
Countermeasures

Hacking Mobile Platforms

Mobile Platform Attack Vectors
OWASP Top 10 Mobile Threats
Mobile Attack Vector
Hacking Android OS
Introduction to Android Operating System
Hacking iOS
iPhone Operating System & Jailbreaking iOS
Hacking Windows Phone OS
Windows Phone
Hacking BlackBerry
BlackBerry Attack Vectors
Mobile Device Management (MDM)
Mobile Device Management Concept
Bring Your Own Device (BYOD)
BYOD Architecture Framework
Mobile Security Guidelines

IoT Hacking

- Technology Brief Internet of Things (IoT) Concept
- How does the Internet of Things works?
- IoT Communication Models
- Understanding IoT Attacks
- Challenges to IoT
- OWASP Top 10 IoT Vulnerabilities
- IoT Attack Areas
- IoT Attacks
- IoT Hacking Methodology
- Information Gathering
- Vulnerability Scanning
- Launch Attack
- Gain Access
- Maintain Attack
- Countermeasures:

Cloud Computing

- Introduction to Cloud Computing
- Types of Cloud Computing Services
- Cloud Deployment Models
- NIST Cloud Computing Reference Architecture
- Cloud Computing Benefits
- Understanding Virtualization
- Cloud Computing Threats
- Data Loss/Breach
- Abusing Cloud Services
- Insecure Interface and APIs
- Cloud Computing Attacks
- Service Hijacking using Social Engineering Attacks
- Service Hijacking using Network Sniffing
- Session Hijacking using XSS Attack
- Session Hijacking using Session Riding
- Domain Name System (DNS) Attacks
- Side Channel Attacks or Cross-guest VM Breaches
- Cloud Security
- Cloud Security Control LayersResponsibilities in Cloud Security

Cloud Computing Security Considerations
Cloud Security Tools
Core CloudInspect
CloudPassage Halo

Cryptography

Cryptography Concepts
Types of Cryptography
Government Access to Keys (GAK)
Encryption Algorithms
Ciphers
Data Encryption Standard (DES)
Advanced Encryption Standard (AES)
RC4, RC5, RC6 Algorithms
The DSA and Related Signature Schemes
RSA (Rivest Shamir Adleman)
Example of RSA Algorithm
Message Digest (One-way Hash) Functions
Secure Hashing Algorithm (SHA)
SSH (Secure Shell)
Cryptography Tools
MD5 Hash Calculators
Calculating MD5 using Tool
Hash Calculators for Mobile:
Cryptography Tool
Advanced Encryption Package 2014
Public Key Infrastructure(PKI)
Certification Authorities (CA)
Signed Certificate Vs. Self Signed Certificate
Email Encryption
Digital Signature
SSL (Secure Sockets Layer)
SSL and TLS for Secure CommunicationPretty Good Privacy (PGP)
Disk Encryption
Cryptography Attacks
Code Breaking Methodologies

Course Duration	20 to 25 Hours
Fees	Call 9015041412 to know
Slots	Weekends

Available Discounts

(Any two discounts are applicable for single student)

- **Flat 10% Discount** on **onetime payment**.
- **Flat 10% Discount** if joining on the **same day** of **demo or enquiry**.
- **Special discount** for group joining(minimum 5 students)
- Got someone's reference??, get **flat ₹ 500 Discount.** .
- **Flat 10% Discount for our old students.**.

Trainer Profile

Piyush Tyagi

Certification: - Certified Ethical Hacker

Education: - B.Tech in Cyber Security and Forensics

Achievements:-

1. Won National Level Cyber Security Hackathon
2. Won Ethical Hacking Task at Hughes Systique Corporation, Gurgaon
3. Won many other Cyber Security and Hacking Related events.

Counselling