Ethical Course Content

Chapter 1 : Introduction To Ethical Hacking

- Technology Brief
- Information Security Threats, Attacks
- CIA Triangle
- Network Security Zone
- Phases of Hacking
- Methodologies
- Scoping and engagement
- Target and strategy
- Penetration Testing
- Information Security Laws
- Incident Management

Real-time Practicals:

- ✓ Will see some CyberAttacks from various domain
- ✓ Know about Various methodologies
- ✓ Data Breaches

Chapter 2: Information Gathering

- Footprinting objectives
- Footprinting through Search Engines
- Email Footprinting
- Monitoring Website Traffic
- OSINT
- Google Hacking Database
- IOT Search Engines
- Domain Reconnaissance
- Social Infrastructure
- Network Infrastucture

Real-time Practicals:

- ✓ Gathering the domain owner details
- ✓ Gathering Subdomains
- ✓ Finding for Breached datas
- ✓ Identify unkown person
- ✓ Compromising unsecured WebCams

Chapter 3: Scanning and enumeration

- Network Scanning TCP/UDP
- Network Topology
- OS fingerprinting
- Service enumeration
- Hping3 and Xmas Scanning
- Firewall Scanning and Evasion
- Nmap script engine
- NETBIOS, FTP, LDAP, SMTP enumeration

Real-time Practicals:

- ✓ Finding ports and services
- ✓ gathering the Network Topology
- ✓ Bypassing the Firewall while scanning

Chapter 4 : Vulnerability Analysis

- Vulnerability Assesment
- Assesment Life-Cycle
- Vulnerability Scanning OpenVas,nessus etc.
- Acunetix, Vega, IBM Appscan
- Microsoft Baseline Security Analyser(MBSA)

Chapter 5 : Social Engineering

- Phishing
- Vishing
- Elicitation
- Shoulder Surfing
- Bad USB
- Motivation Techniques

Real-time Practicals:

- ✓ Creating and hosting a phishing page
- ✓ Compromising facebook,gmail
- ✓ Hacking system with RubberDucky

Chapter 6: Malicious codes

- Virus
- Trojans
- Keylogger
- Botnet
- HTTP/S
- FUD & Crypter

Real-time Practicals:

- ✓ Using Windows and Linux Keyloggers
- ✓ Creating FUD and Obfuscator
- ✓ Building Botnets

Chapter 7: System Hacking

- Name Resolution exploit
- Default Password tools
- Rainbow Table
- Windows Password Cracking
- SMB and FTP exploit
- DoS Attacks
- UAC Bypass
- Windows Hacking
- Mobile Device Hacking

Real-time Practicals:

- Hacking Windows system with SMB, NETBIOS
- Sniffing HTTPS Traffic
- Using Metasploit Hacking Windows, Android, iOS
- Bypassing User Access Control

Chapter 8: Covering Tracks

- Clearing Audit Policies
- Clearing Event logs on windows
- Clearing Event logs on Linux

Chapter 9: Sniffing

- Wiretapping
- MAC and CAM Table
- MAC Flooding
- DHCP Attacks
- ARP Poisioning

Chapter 10: Network Analysing

- Wireshark/tcpdump
- Filters
- Statistics and Analysis
- Playing with Buffers
- Packet analysis

Chapter 11: Bypassing Techniques

- Evading Firewall
- Bypassing IDS, Honeypot
- Obfuscation
- Session Slicing
- Spoofing IP

Chapter 12: Wireless and RF

- Evil Twin (Karma, Downgrade)
- Deauth attacks
- Analysis of RF Signals
- Cracking WEP/WPA/WPA2-PSK
- WiFi IDS
- Wireless Social Engineering
- Bluesnarfing

Real-time Practicals:

- ✓ Hacking WiFi using various types
- ✓ Bluetooth hacking
- ✓ Intercepting RF
- ✓ Wifi Phishing attacks

Chapter 13: Spoofing

- EMail spoofing
- Call, SMS Spoofing
- Identity Spoofing (IP,MAC)

Real-time Practicals:

- ✓ Sending a fake email and sms
- ✓ VoIP calling
- ✓ IP and Mac address changing

Chapter 14: Web Hacking

- Overview of Web
- Understanding web server
- Understanding the status codes
- Mirroring a Website
- Cross Site Scripting
  - ✓ Reflected
  - ✓ Stored
  - ✓ DOM
- HTML Injection
- Directory Traversal
- SQL Injection
  - ✓ Union Based
  - ✓ Time Based
  - ✓ Error Based
  - ✓ Blind SQL Injection
  - ✓ Cookie Based
  - ✓ Bypassing Firewall
  - ✓ Sql to Shell Access
- Session Hijacking
- Bruteforcing credentials
- Redirection Attacks

- Host Header Atttacks
- Parameter Pollution
- Local File Inclusion
  - ✓ Website Defacement
- Remote Code Execution
- Web Application Fuzzing
- Server Side Request Forgery
- XXE Attacks
- API Pentesting
- Covering Tracks

Real-time Practicals:

- ✓ Burpsuite exploration
- ✓ Live XSS, HTMLi, and other vulnerabilities
- ✓ Hacking websites via SQLi, LFI, RCE, Command injection
- ✓ Buying products for free (Read Disclaimer)

Chapter 15: Cloud

- Introduction to Cloud Computing
- Cloud Computing Threats
- Cloud Computing Attacks
- Insecure Interface API
- Cloud Security Tools and Penetration Testing

Real-time Practicals:

- ✓ Active scanning on Cloud

Chapter 16: Crypto

- Cryptography Concepts
- Steganography
- Encryption Algorithms
- Cryptography Tools
- Kerberos Authentication
- PGP, PKI, SET
- Heartbleed, Poodle

Real-time Practicals:

- ✓ Cracking windows passwords
- ✓ Identifying the threats on web

Chapter 17: Reporting

- Standards
- Own Methodologies
- Bug Bounty Reports

Contact Info:

☎ +91 9884412301 | +91 9884312236

✉ info@credosystemz.com

Know more about Ethical Hacking

New # 30, Old # 16A, Third Main Road,
Rajalakshmi Nagar, Velachery, Chennai
(Opp. to MuruganKalyanaMandapam)

BOOK A FREE DEMO