5 Days Training Module
CDAC-MOHALI

Network, Web & Wireless Security

Introduction

- ✓ Introduction to Information Security
- ✓ What is Hacking and why learn it?
- ✓ Building your Hacking environment
- ✓ Basic overview of Linux – Terminal and Linux Commands
- ✓ Browser Security, Privacy and Tracking
- ✓ Introduction to Browser Fingerprinting
- ✓ Email Forgery/Hacking/Tracing/Tracking/Spoofing
- ✓ The Zero Trust Model
- ✓ Threat Modelling and Risk Assessments
- ✓ Hackers, Crackers and Cyber Criminals
- ✓ Cyber Law - IT Act 2000 and ITA 2008 Introduction
- ✓ Defence against Online Attacks
- ✓ Hidden Secret Messages behind Images – Steganography
- ✓ Building and Writing the Trojans

Wireless and Wi-Fi Security

- ✓ Introduction to Wireless Attacks and Threats
- ✓ Types of Wireless Protocols
- ✓ Wi-Fi Weaknesses – WEP
- ✓ Wi-Fi Weaknesses – WPA, WPA2, TKIP and CCMP
- ✓ Wi-Fi Weaknesses – WPS, Evil Twin and Rouge AP
- ✓ Wireless Security – Secure Configuration and Network Isolation
- ✓ Who is on my Wi-Fi Network?
- ✓ Targeted Packet Sniffing using Airodump-ng
- ✓ WEP Cracking – Theory Behind Cracking WEP Encryption (Practical Demo)
- ✓ Fake Authentication and ARP Request Replay Attacks
- ✓ Exploiting WPS Security – WPA Cracking
- ✓ Capturing the Wireless Handshake with/without Deauthentication
- ✓ WPA/WPA2-PSK Cracking With Evil Twin (MITM)
- ✓ WPA/WPA2-PSK Cracking with Fluxion (Wireless Phishing)
- ✓ Cracking Wireless Key using a Wordlist – Dictionary Attack
- ✓ Generating Fake Dictionary Lists with Crunch
- ✓ Discovering Hidden Wireless Networks with Aireplay-ng Tool
- ✓ Bypassing MAC Filtering
- ✓ Performing Denial of Service on Wireless Networks

Network Penetration Testing

- ✓ Introduction to Network PT
- ✓ Network Basics & Information Gathering
- ✓ Gathering More information using Autoscan and Zenmap
- ✓ MITM - ARP Spoofing using Arpspoof and MITMf
- ✓ Detecting ARP Poisoning Attacks
- ✓ Bypassing HSTS and Session Hijacking
- ✓ Injecting & Spreading JS Malware
- ✓ Packet Sniffing – HTTP and HTTPS

- ✓ HTTPS Data Sniffing with SSLSTRIP and DSNIFF
- ✓ URL and Mail Sniffing with URLSNARF and MAILSNARF
- ✓ Basics of Wireless – A Packet Analyzer Tool
- ✓ Analysing HTTP Traffic with Wireshark
- ✓ Detecting Suspicious Activities with Wireshark
- ✓ Nmap Introduction and Basics
- ✓ Version and Operating System Detection with Nmap
- ✓ Nessus Installation and Scanning
- ✓ SSH Remote/Local Port Forwarding
- ✓ SSH Hardening And Configuration
- ✓ Network Monitoring with TCPDUMP, Wireshark, Tshark and Iptables
- ✓ Finding Malware and Hackers with Wireshark Tool
- ✓ Hacking with Netcat – Listening and Exploitation (On both Windows/Linux)
- ✓ Overview of SETOOLKIT – Social Engineering Toolkit
- ✓ Cracking Windows/Linux Passwords – OnLogin

Post Exploitation Attacks

- ✓ Introduction to Post Exploitation Attack
- ✓ Basic Information Gathering and Exploitation
- ✓ Introduction to Metasploit Framework
- ✓ Installation and Configuration of Metasploitable2
- ✓ Exploiting a Code Execution Vulnerability
- ✓ Targeted Scanning with Metasploit Framework
- ✓ Overview of Armitage Tool
- ✓ Nexpose – Installation and Configuration
- ✓ Veil Overview and Payload Basics – Malware Kit
- ✓ Generating an Undetectable Backdoor using Veil and Weevely
- ✓ BeEF Overview and Basics Exploitation with JS Hooking
- ✓ Stealing Credentials/Passwords using Fake Login Prompt
- ✓ BeEF – Gaining Full Control over Windows Target
- ✓ Detecting Trojans using a Sandbox/Manually
- ✓ Meterpreter Basics – Post Exploitation Module
- ✓ Maintaining Access – Using FUD Backdoors
- ✓ Exploiting Devices on the same Network
- ✓ How Passwords are Cracked using Hashcat and John the Ripper
- ✓ Creating & Gaining Access with Reverse Shell
- ✓ Persistent Backdooring with MSFVENOM
- ✓ Metasploit Attacks over WAN with/without Port Forwarding
- ✓ Hacking Windows (XP/7/8/8.1/10) with Metasploit Framework
- ✓ Hacking Windows (XP/7/8/8.1/10) with CHAOS Framework
- ✓ Android Hacking over LAN/WAN
- ✓ Fake APK Generation and Persistence Phone Backdooring
- ✓ MITM – Man in the Middle Attacks using Ettercap and Driftnet

Website Penetration Testing

- ✓ Introduction – What is a Website?
- ✓ Overview of HTTP Status/Versions
- ✓ Scanning HTTP Methods – HEAD/TRACE/OPTIONS/GET/POST/DEBUG/PUT/DELETE
- ✓ Information Gathering using HTTP Headers
- ✓ Introduction to OWASP Top 10 Attacks

5 Days Training Module
CDAC-MOHALI

- ✓ Discovering Technologies Used on the Website
- ✓ Gathering Comprehensive DNS Information
- ✓ Sub-domain Brute forcing with Dirbuster
- ✓ Basic Input Validation Attacks – Breaking into Databases
- ✓ SQL Injection – Threats and Exploitation – Practical Demo
- ✓ Dangers of SQL Injection Vulnerabilities – String/Boolean/Blind/Time
- ✓ Discovering SQL Injections and Extracting Data using SQLMAP
- ✓ Right Way to Prevent SQL Injection
- ✓ Discovering and Exploiting File Upload Vulnerabilities
- ✓ Local and Remote File Inclusion Attacks
- ✓ Cross Site Scripting – Attacks and Types
- ✓ Exploiting XSS – Hooking Vulnerable Page Visitors to BeEF
- ✓ Preventing XSS Vulnerabilities
- ✓ Exploiting Whole Server with HTTP PUT Method
- ✓ SSL – Introduction, Types and Configuration
- ✓ Session Mismanagement – Hijacking/Replay Attacks
- ✓ WordPress and Joomla CMS Exploitation
- ✓ Complete Website Security Testing with Burp Suite/Acunetix and IBM Appscan
- ✓ Best Practices on Secure Coding