Content of 6 Weeks Ethical Hacking/Cyber Security Training

Module 1: Introduction

Introduction to Ethical Hacking
Cyber Security and Ethical Hacking Terminologies

Module 2:Networking

IP Address
TCP/IP and OSI Model
VPN and Proxy Servers
Tracing an IP Address
Proxy Chain
Protocols

Module 3: Virtual Lab Setup

Virtual Box Setup
VMware Lab Setup
Setting Windows 7 on Virtual Box (Target Machine)
Setting Kali on Virtual Box (Attack Machine)
Setting Vulnerable Machines on Virtual Box
Setting TAIL in Virtualization Machine

Module 4: Reconnaissance – Art of Information Gathering

Network Reconnaissance
Port Scanning
OS Detection
Recon Concepts
Methodologies of Recon
Recon Tools
Active and Passive Information Gathering
NMAP

Module 5: System Hacking

Introduction
Making USB Pen drive Bootable
Ethical Hacking Window Administrative Password. (All Platforms)
Practical: Hirens_BootCD

Module 6: Google Dorking

Introduction to Google Ethical Hacking
Using Google Dorks on Google Search Engine
Demonstration of leaking of confidential information on vulnerable website
Securing a website from Google Ethical Hacking
Lab – Google Dorking Lab, BigBountyRecon

Module 7: SQL Injection and DDOS

Introduction
SQL Injection
Manual Method and Tool Used
Countermeasures
Denial of Services Attack (DDOS Attack)

Module 8: Important Theft Techniques

Keylogger, Spyware Software
Trojan and Backdoors Attack
Virus, Worm & Trojan
Binders and Cryptor's
Spamming Attacks
Session Hijacking

Module 9: Social Engineering Attack

Hack Anyone without even using a single tool
Physical Security Threats
Identity Theft
Types of Social Engineering Attacks

Module 10: Digital Forensics Science

Recover data from the USB Pen drives, Hard Disk Drive - Forensic way

Module 11: Steganography (Hide data into images)

Introduction
Tools

Module 12: Penetration Testing

Introduction to Penetration Testing
How to do Penetration Testing
Preparing the Report.

Module 13: Web Application Testing Attack vectors

OWASP Top 10
The web application security problem
Web Application Basics
Web Application Security Overview
Installation and setup
Exercise 1. Installing a web application vulnerability testing solution
Preparing for your scan
Configuring your first scan
Exercise 2. Setting up your first scan
Reviewing the result

Module 14: CSRF

Introduction
Why CSRF Using
How to use File Uploading with CSRF

Module 15: CTF's

Pumpkin Garden CTF
Pumpkin Raising CTF
Pumpkin Festival CTF
OWASP Broken Web App
MR Robot
Deathnote
DVWA Lab

Module 16: Spoofing

What is Spoofing
Types of Spoofing
IP Address Spoofing
Mac Address Spoofing

Module 17: Wi-Fi Ethical Hacking & Security

Ethical Hacking on Wi-Fi Passwords on Wi-Fi router with WEP|WPA|WPA2 encryption

Securing Wi-Fi Router from being hacked

Module 18: IOT and OT Hacking

Introduction
Features of IOT
Challenges of IOT
OSWAP Top 10 IOT Vulnerabilities
IOT Threats
Using IOT Hacking Tools

Module 19: Cloud Computing

Introduction
Types of Cloud Based on Services
Types of Cloud According to Development Model
Virtualization
Cloud Computing Attacks

Module 20: Cryptography

Introduction
Algorithms
Key Algorithms
Tools
Hash

Module 21: Mobile Hacking

Introduction
OSWAP TOP 10 Mobile Risk 2016
Vulnerabilities
Guideline for Mobile Security
Tools

Module 22: Wireless Hacking

Introduction
Terminologies
Types of Wireless Hacking
Wifi Technology
Wireless Threats
Wireless Hacking Methodology
Countermeasures

Module 23: DVWA Lab

Brute Force
Command Injection
CSRF
File Injection
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS(Reflected)
XSS(Stored)