Section 1 – Introduction

Course Introduction

Basics of Information Security

Ethical Hacking Basics

Home Lab Setup

Hacking Lab Walkthrough

Section 2 – Understanding the Cyber Kill Chain

Introduction

Footprinting & Reconnaissance

Weaponization

Delivery

Exploitation and Installation

Command and Control

Actions on Objectives

Section 3 - Virtual Lab Environment

Creating a Virtual Install of Kali Linux Using VMWare

Creating a Virtual Install of Kali Linux Using VirtualBox

Anonymity – Remaining Anonymous While Hacking Online

Remaining Anonymous Online Using TOR and Proxychains

Setup Free VPN Using Kali Linux

Using Anonsurf on Kali Linux to Stay Anonyms

Section 4 - Gathering Information

Information Gathering Using Maltego

Information Gathering Using Metagoofil

Gathering Information using whois Lookup

Section 5 - Code Execution Vulnerabilities

What are they? & How to Discover & Exploit Basic Code Execution Vulnerabilites

Exploting Advanced Code Execution

Security – Fixing Code Execution vulnerabilities

Section 6 - Local File Inclusion Vulnerabilities (LFI)

What are they? And How to Discover & Exploit Them

Gaining Shell Access From LFI Vulnerabilities

Section 7 - Remote File Inclusion Vulnerabilities (RFI)

Configuring PHP Settings

Discovery & Exploitation

Exploiting Advanced Remote File Inclusion Vulnerabilities

Section 8 - NMap

Introduction to Nmap

Nmap Scripting Engine(NSE)

Scanning for WannaCry Ransomware

Section 9 - Scanning for Vulnerabilities Using NESSUS

Installing NESSUS Using DOCKER

Scanning for Vulnerabilities Using Nessus

Using your Nessus Scan Results

Section 10 - Scanning for Vulnerabilities Using OpenVAS

Installing OpenVAS Using Docker

Scanning for Vulnerabilities Using OpenVAS

Section 11 - Exploiting Windows XP

Using Metasploit to Launch DOS Attack Against Windows XP

Establishing A VNC Shell Using Meterpreter

Using Meterpreter to backdoor Windows XP

Exploiting Vulnerable Applications on Windows XP SP2

Hacking Windows XP via MS11-006 Windows Shell Graphics Processing

Section 12 - NetCat

Using Netcat to Exploit Server 2008

Section 13 - Exploiting Linux

Installing Metasploitable2 Using Virtual Box

Installing Metasploitable2 Using VMWare

LAB - This is SPARTA!

Learning to Hack Linux Using Metaspoitable2

Exploring Endpoint Attack

Exploit Using Social Engineering Toolkit(SET)

Section 14 - BASH Scripting for pentesters

Introduction to BASH Scripting

Creating a BASH Script for Scanning Vulnerable Ports

Lab – Linux BASH Shell Scripting – Task Scheduling

Section 15 - Password Cracking

Password Cracking Using Medusa

Passwords Cracking Using Mimikatz

Section 16 - Introduction

WIFI Hacking Introduction

Wireless Introduction

Introduction to Wi-Fi Technology

Overview of Aircrack-Ng Suite for Wi-Fi Hacking Tools

Airodump-ng Tool and Capture WPS/WPA2 Handshake

Generate Possible Password List by crunch Tool

Section 17 - WiFi Password Cracking

Crack WPA2 PSK Passwords Using Aircrack Ng Tool

How Wi-Fi password Cracked by using Cowpatty Tool

How to Make your own HASH and Crack WPA Password Using Cowpatty

Wifi password Cracked by using Hashcat Tool

How to crack wifi password by Fern Wifi Cracker Tool

Crack Wifi Password Usinf gerix Tool

Hostpad-WpE Wifi Password Craker Tool

How Wifite Tool Used to crack Wifi Password

Convert CAP file to HCCAP format Decrypt WiFi CAP file using john the Ripper Tool

Crack WiFi Password by Using Aircrack and Crunch in Airgeddon tool

Hack WPA/WPA2/WPS with Reaver

Section 18 - Wireless Deauthentication

Kickout the connected Wifi Devices Using Netattack2 Tool

Beacon Flooding by using MDK3

Section 19 - Install WAMP

Install WAMP,the Apache, PHP and MYSQL stack for hosting the demo web server

Section 20 - Install Mutilidae

Install Mutlidae II, a free, open Source, deliberately vulnerable web-app

Section 21 - Install Burp Suite

Section 22 - An integrated platform for security testing of websites

Troubleshooting Burp: Cannot Load HTTPS Websites

Section 23 - SQL Injection – Attack and Defenses

Hacking Techniques and Defenses

Section 24 - OS Command Injection- Attack and Defenses

Hacking Techniques and Defenses

Section 25 - JSON Injection

JSON Injection Attack using Reflected XSS Technique and Defense Measures

Section 26 - Cookie Manipulation

Cookie Manipulation Attack and Defense

Section 27 - Username Enumeration Attack and Defenses

Section 28 - Brute Force Attack Technique and Defenses

Section 29 - Cross Site Scripting

Cross Site Scripting (Reflected XXS using HTML Context)

Cross Site Scripting (Reflected XSS using JavaScript

Section 30 - Storage Cross Site Scripting Attack – XSS Defenses

Section 31 - Insecure Direct Object Reference

IDOR and Defense Using File Tokens

IDOR and Defense Using URL Tokens

Section 32 - Directory Browsing/Travel Threat Demonstration

Section 33 - XXE – XML External Entity Attack

Section 34 - User Agent Manipulation or Spoofing Attack

Section 35 - Security miss-configuration Attack Defenses(DIR Browsing,XXE, User Agent)

Section 36 - Sensitive Data Exposure Vulnerability(HTML/CSS/JS Comments)

Hidden/Secret URL Vulnerability and Defenses

Section 37 - HTML 5 Web Storage Vulnerability and Defense

Section 38 - Role Based Access Vulnerability and Defense

Section 39 - CSRF – Cross Site Request Forgery Attack

Section 40 - Entropy Analysis for CSRF Token

Section 41 - CVSS- Common Vulnerability Scoring System

Section 42 - Unvalidated URL Redirect Attack and Prevention code sample

Section 43 - Weaponizing

Preparing your Android Device

NetHunter Preview and Lab Overview

Section 44 - Information Gathering

Discovering Wireless Networks-Wardriving

Preparing Your Device to crack Wifi Keys/Password – WEP/WPA/WPA2

Network Mapping – Discovering Devices Connected to the Network

Discovering open ports

Discovering installed Services

Section 45 - Spying

Introduction

MITM(Man in the Middle) Methods

Section 46 - Spying MITM Method 1 – Bad USB Attack

What is the Bad USB Attack & How to Launch it

Sniffing Data & Capturing Passwords

Bypassing HTTPS
DNS Spoofing

Section 47 - Spying MITM Method 2 – ARP Poisoning

What is ARP Poisoning

ARP Poisoning and Sniffing Data Using arpspoof

ARP Poisoning & Sniffing Data ZAnti2

Intercepting Downloaded Files

Replace Images & Injecting JavaScript Code

Section 48 - Spying MITM Method 3 – Fake Access Point (Honey Pot)

Fake Access Point Theory

Configuring Access Point settings

Launching The Fake Access Point

Sniffing data Sent over the access Point

Section 49 - Detection & Protection

Detecting ARP Poisoning Attacks

Detecting Suspicious Activity in the Network & Solutions to ARP Poisoning

Practice Modules

CTF – Easy Beginner Level – Basic Pentest

Basic Pentest Walkthrough

Capture the Flag - Basic Pentesting

Capture the Flag - Basic Pentesting II

CTF – Beginner to Intermediate Level – DeRPnStiNK

LAB – DeRPnStiNK Walkthrough

Capture the Flag – DeRPnStiNK

Capture the Flag – DeRPnStiNK II

CTF – Beginner to Intermediate Level – Stapler

LAB – Stapler Walkthrough

Capture the Flag – Stapler
Capture the Flag – Stapler II

Capture the Flag – Stapler III

CTF – Intermediate Level – Mr.Robot

LAB-Mr.Robot Walkthrough

Capture the Flag Mr. Robot Part I

Capture the Flag Mr. Robot Part II

Capture the Flag Mr. Robot Part III

Capture the Flag Walkthrough – Toppo

Capture the flag Walkthrough – Toppo

Lab Preparation

Recon, Enumeration, Gaining Acsess, Post Exploitation

Capture the Flag Walkthrough – Lampiao

Capture the flag Walkthrough – Lampiao

Lab Preparation

Recon, Enumeration, Gaining Acsess,

Exploitation, Privilege, Elevation

Capture the Flag Walkthrough – DC-1

Capture the flag Walkthrough – DC-1

Lab Preparation

Recon, Enumeration, Gaining Acsess

Exploitation, Privilege, Elevation

Capture the Flag Walkthrough – SickOS1.1

Capture the flag Walkthrough – SickOS 1.1

Lab Preparation

Recon, Enumeration, Gaining Acsess, Post Exploitation