Ethical Hacking MasterClass - A to Z of Hacking

Simpliv LLC

Course Specifications

Mode of Study : Online study mode

Location : Nairobi

Duration : 410 days 58 weeks 13 months 1 year

Intake : April

Course Summary

About this Course
Welcome to Ethical Hacking Course ! In this course, you will start as a beginner and leave the course with an expert . The course purely focused on Practicals.

Course is divided in 2 parts: -

1. Network Pentesting
2. Web Pentesting

The course is structured in a way that will take you through the basics of computer systems, networks and how devices communicate with each other. We will start by talking about how we can exploit these systems to carry out a number of powerful attacks. This course will take you from a beginner to a more advanced level - by the time you finish, you will have knowledge about most penetration testing fields.

Network Penetration Testing - In this section you will learn major and minor attacks on networks .it can be divided in 3 sections : -

Pre-connection: in this section, we still don't know much about penetration testing - all we have is a computer with a wireless card. You will learn how gather information about the networks and computers around you and launch a number of attacks without a password, such as controlling the connections around you (ie: deny/allow any device from connecting to any network). You will also learn how to create a fake access point, attract users to connect to it and capture any important information they enter

Gaining Access: Now that you have gathered information about the networks around you and found your target, you will learn how to crack the key and gain access to your target network. In this section you will learn a number of methods to crack WEP/WPA/WPA2 encryption
Post Connection: Now you have the key to your target network and you can connect to it. In this section, you will learn a number of powerful attacks that can be launched against the network and connected clients. These attacks will allow you to gain access to any account accessed by any device connected to your network and read all the traffic used by these devices (images, videos, audio, passwords ...etc)
Gaining Access - In this section you will learn how to gain full control over any computer system
Server Side Attacks: In this approach, you will learn how to gain full access to systems without the need for user interaction. You will learn how to gather information about a target computer system such as its operating system, open ports, installed services and discover weaknesses and vulnerabilities. You will

also learn how to exploit these weaknesses to gain full control over the target. Finally, you will learn how to generate different types of reports for your discoveries

Client-Side Attacks - If the target system does not contain any weaknesses then the only way to gain access to it is by interacting with the user. In this approach, you will learn how to launch a number of powerful attacks to fool the target user and get them to install a backdoor on their device. This is done by creating fake updates and serving them to the user or by backdooring downloaded files on the fly. You will also learn how to gather information about the target person and use social engineering to deliver a backdoor to them as an image or any other file type. Post Exploitation - In this section you will learn how to interact with the systems you compromised so far. You'll learn how to access the file system (read/write/upload/execute), maintain your access, spy on the target and even use the target computer as a pivot to hack other computer systems
Web Application Penetration Testing - In this section, you will learn how websites actually work. you will learn various web application attacks like SQL injection attack , XSS attack, csrf attack , shell upload attack, buffer overflow attack, local file inclusion attack, etc . we have covered all major attacks on web applications.

Summary

In this course, you will perform a test to carry out and exploit a hidden vulnerability within your network and systems, not only you will be exposing those but you will also provide ways and methods to fix and secure and hardening your system security preventing it from any other attacks. You will learn how to test your network against various types of attacks & develop a network-testing environment that can be used to test scanning tools and techniques. Employ the methods used by real hackers effectively, to ensure the most effective penetration testing of your network, select and configure the most effective tools from Kali Linux to test network security, employ stealth to avoid detection in the network being tested, recognize when stealthy attacks are being used against your network. Exploit networks and data systems using wired and wireless networks as well as web services. Identify and download valuable data from target systems & learn to maintain access to compromised systems. Use social engineering to compromise the weakest part of the network—the end-users. Port scanning for UDP scanning, stealth scanning, connect & zombie scanning using pen-testing tools. You will learn how to utilize the arsenal of tools available in Kali Linux to conquer any network environment. By the end of this course, you will become a pro with the tools that Kali Linux offers to perform some advanced penetration testing, how to exploit the vulnerable systems and how to patch them.

NOTE: This course is created for educational purposes only.

NOTE: This course is a product of Sunil Gupta and no other organization is associated with it or a certification exam. Although, you will receive a Course Completion Certification from Simpliv.

Basic Requirements

- Computer Basics
- Wireless Adapter (for wifi cracking) - Details inside course
- No need of Programming /code
- Windows Operating System as main OS in PC/Laptop

Course Outline

Introduction

Lab setup and Softwares

Network Pentesting Overview

Network Pentesting - Wireless (Wifi) Hacking Preparation

Network Pentesting - Wireless (Wifi) Hacking - WEP/WPA/WPA2 Hack

Network Pentesting - MITM Attack

Network Pentesting - Server Side Attacks

Network Pentesting - Client-side attack - Social Engineering

Network Pentesting - Client-side attack - Bypass Antivirus in Windows7

Lab Setup - Windows10 machine

Network Pentesting - Client-side attack - Bypass Antivirus in Windows10 machine

Website Pentesting - Lab Setup

Website Pentesting - SQL Injection Attack on Websites

Website Pentesting - XSS Attack on web application

Website Pentesting - CSRF (cross-site request forgery) attack

Website Pentesting - Other Attacks

Contact:

BrighterMonday

+254703026000, +254703026123

bmlearning@brightermonday.co.ke