

WIRELESS AND MOBILE HACKING AND SNIFFING TECHNIQUES



DR. HIDAIA MAHMOOD ALASSOULI

Wireless and Mobile Hacking and Sniffing Techniques

By

**Dr. Hidaia Mahmood Alassouli
Hidaia_lassouli@hotmail.com**

While every precaution has been taken in the preparation of this book, the publisher assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.

Wireless and Mobile Hacking and Sniffing Techniques

Copyright © 2021 Dr. Hidaia Mahmood Alassouli.

Written by Dr. Hidaia Mahmood Alassouli.

1. Introduction

Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of “tapping phone wires” and get to know about the conversation. It is also called wiretapping applied to the computer networks.

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

There are several ways how hackers can gain access to a public WiFi network and infiltrate connected devices to steal data. The most common practice that hackers use is called sniffing. This method allows hackers to hijack any packet of data that is being transmitted between a device and a router.

The mobile device has become an inseparable part of life today. The attackers are easily able to compromise the mobile network because of various vulnerabilities, the majority of the attacks are because of the untrusted apps. SMS is another way the attackers are gaining access to the mobile devices by sending phishing messages/spam messages to user

This report covers the main Wireless and Mobile Hacking and Sniffing Techniques. The report contains the following parts:

- Part A: Setup Lab

- Part B: Sniffer and Phishing Hacking
- Part C: Wireless Hacking Networks in Linux
- Part D: Mobile Platforms Hacking

You can download all hacking tools and materials from the following websites

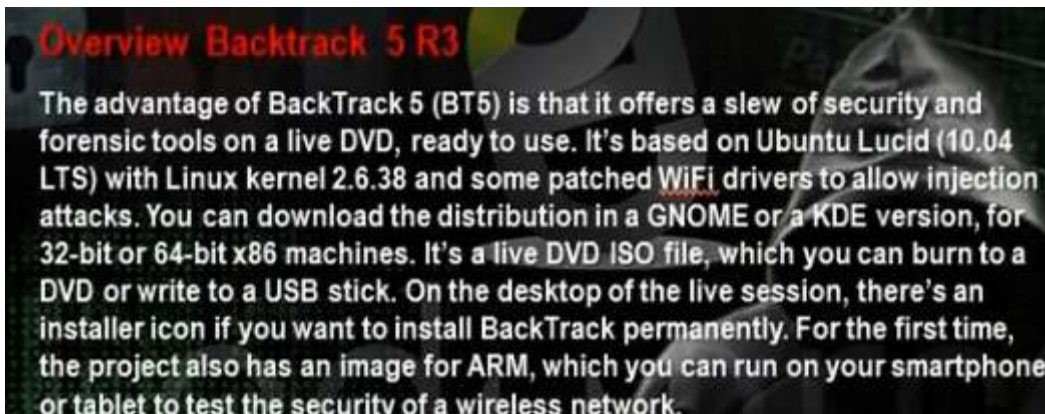
<http://www.hax4rall.com/2016/02/13/ceh-v9-pdf-certified-ethical-hacker-v9-courseeducatonal-materials-tools/>

www.mediafire.com%2Ffolder%2Fad5szsted5end%2FEduors_Professional_Ethical_Hacker&h=gAQGad5Hf

2. Part A: Setup Lab

a) Setup lab

- From the virtualization technology with software VMware or virtual box we can do more than one virtual machines, one linux and other windows 2007 or windows Xp
- Download vmware and install it
- Create folder edurs-vm in non-windows partition. Create a folder for each operating system
- Install any windows operating system.
- Download backtrack



- To install backtrack on usb, download unebootin. We need also to use the tool to support booting from flash memory in vmware.

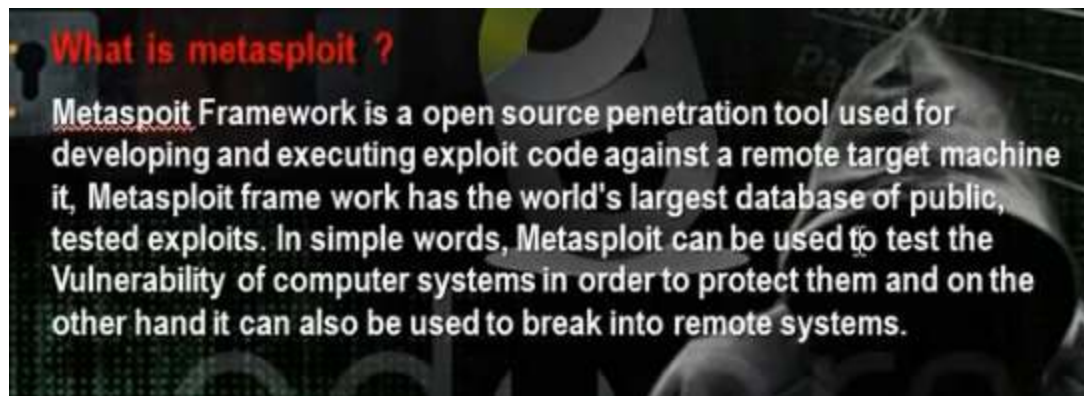


- Download and install kali linux

A slide titled "Overview Kali Linux" with a background image of a person in a hoodie. The slide contains a bulleted list of information about Kali Linux.

- **Overview Kali Linux**
- Kali Linux is an advanced Penetration Testing and Security Auditing Linux distribution.
- **Kali Linux Features**
- Kali is a complete re-build of BackTrack Linux, adhering completely to Debian development standards. All-new infrastructure has been put in place, all tools were reviewed and packaged, and we use Git for our VCS.
- More than 300 penetration testing tools:
- Free and always will be
- Open source Git tree:
- **Download**
- <http://www.kali.org/downloads/>

- Download and install metasploit.

A slide titled "What is metasploit ?" with a background image of a person in a hoodie. The slide contains a paragraph describing the Metasploit Framework.

What is metasploit ?

Metasploit Framework is a open source penetration tool used for developing and executing exploit code against a remote target machine it, Metasploit frame work has the world's largest database of public, tested exploits. In simple words, Metasploit can be used to test the Vulnerability of computer systems in order to protect them and on the other hand it can also be used to break into remote systems.

Metasploit is big project that contains a lot of modules or programs. These modules or programs can utilize the holes in windows machines or linux machines operating systems. For any hole that occur in the operating systems, we can develop the program that can utilize this hole. We can work on it through command line or graphical interface. The programs that use graphical interface are armitage and Koblet Strike . In linux we can update the metasploite using command msfupdate.