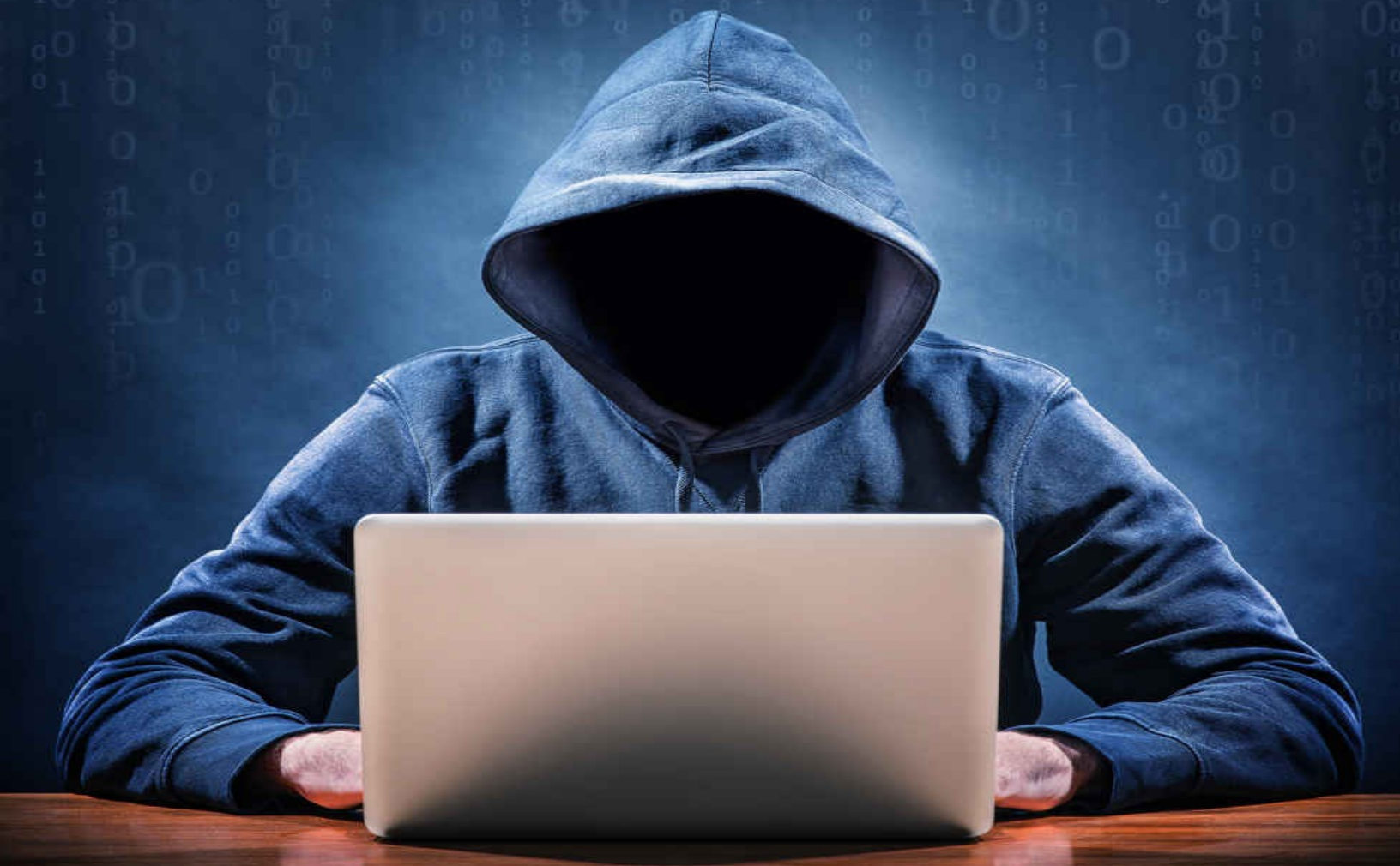
HACKING

A BEGINNERS' GUIDE TO COMPUTER HACKING, BASIC SECURITY AND PENETRATION TESTING



JOHN SLAVIO

hacking

A Beginner's Guide to Computer Hacking, Basic Security, and Penetration Testing

Author: John Slavio

TABLE OF CONTENTS

WHAT IS HACKING AND COMPUTER SECURITY?
VARIOUS TYPES OF HACKING
TYPES OF ATTACKS
HACKING TOOLS
COMMON ATTACKS AND THREATS
HIDING IP ADDRESS
HACKING AN EMAIL ADDRESS
SPOOFING TECHNIQUES
MOBILE HACKING
OTHER COMPLEX HACKING TECHNIQUES
PENETRATION TESTING
ETHICAL HACKING
CONCLUSION

DISCLAIMER

While the author has taken the utmost effort to ensure the accuracy of the written content, all readers are advised to follow information mentioned herein at their own risk. The author cannot be held responsible for any personal or commercial damage caused by information. All readers are encouraged to seek professional advice when needed.

ABOUT THE AUTHOR

John Slavio is a programmer who is passionate about the reach of the internet and the interaction of the internet with daily devices. He has automated several home devices to make them 'smart' and connect them to high speed internet. His passions involve computer security, iOT, hardware programming and blogging. Below is a list of his books:

John Slavio Special

WHAT IS HACKING AND COMPUTER SECURITY?

What is hacking? The dictionary definition of hacking is the following: the practice of modifying the features of a system to accomplish a goal outside of the designer's purpose. "Hacker" refers to a person who practices hacking in more than a sporadic fashion. Hacking has a negative connotation, which means that people generally connect it with a negative experience. When you think of hacking, you probably think of someone in a dark room breaking into someone else's computer and sending them some picture of a skull before their computer shuts down. However, there is more to hacking than this.

History of Hacking

MIT, an organization in the 1960s, had a group of computer geniuses who worked with some of the most difficult programming languages. They were not doing anything illegal or unethical. They were using their intelligence to create new programs and change current programs and understand even the most difficult programing languages. True hackers are those who are pioneers in searching for new ways to do things. They love to learn new information and can remember the most intricate details.

Further down the road, in the late 1960s, UNIX was invented. UNIX is a widely used, multiuser operating system with a pre-programmed operating

language that makes it easier for non-computer geniuses to understand. In 1970, the computer programming language, known as C, was invented to be used with UNIX. These two tools together work to help everyone be able to hack. ARPANET was then created to connect government offices and computers. Their system and way of doing things was later what evolved into the internet as we know it.

In the beginning, being known as a hacker was a complement. It simply meant that you knew how to push a computer to its programming limits. You were an intelligent being who could get around the rules.

In the 1990s, hackers began to take a turn. They realized that they could use their knowledge to get around systems and into places they should not be able to access. Kevin Mitnick was the first hacker arrested in 1995. He was charged with wire fraud and illegal possession of computer files that were not meant for him to see. He reportedly stole corporate secrets and broke into the nation's defense system. He pled guilty and now tours and even speaks at keynotes.

Computer Security

What is computer security? It is the attempt to prevent theft of computer files and the safety and privacy of users. Sometimes, safety comes in physically prohibiting access of hardware to certain individuals. Other times,

this includes protecting your computer against viruses when it is online. Programs can be purchased to warn your computer when it reaches a dangerous website. These programs also conduct periodic scans that can alert you if there is malware on your computer.

Today's Idea of Hackers

Not all hackers are like Kevin Mitnick. Many hackers are constantly seeking the weaknesses in the constantly improving computer safety, as was discussed above. Hackers regulate the electronic communication that is becoming such a pertinent part of our society. Hackers not only find the problems but also propose solutions which can then be incorporated into computer security. Many times, hackers can give our computer developers help when it comes to improving your computer's safety.

However, there are hackers who fit the stereotype. They will use their knowledge to steal files. Educating yourself on their methods will help you be more prepared to fight them off, should someone try to enter your computer system and steal your information.

Last of all, you may be aware of some illegal software known as warez. Those who distribute this software are not necessarily hackers, though they can be. You should stay away from this software. While there are some hackers who can cause destruction like you might have seen in a movie, many

of them are actually helpful and are trying to improve the electronic world. To learn more about the different types of hacking, continue on to chapter two.

VARIOUS TYPES OF HACKING

Hacking can be broken down into three main categories, but we are going to break them down into six categories to be even more specific. After we talk about the types of hacking, you will learn a little bit about a few different motivations or reasons why people might hack.

Black Hat

There are three different hat types to describe three of the types of hacking. Black hat is the stereotype hacker. These types of hackers have negative intentions and are also known as crackers. Sometimes, black hats have someone behind them paying them to do something; other times, black hats simply break into the system for their own gain. Black hats are usually professionals who have extensive knowledge in programming areas such as computer networking, network protocols, and systems and programming. They understand a majority of the operating systems and are able to read the programming languages and script them.

Additionally, black hats are well versed in the hacker tools that you will learn about in chapter four. A black hats reasons are far from ethical as stated above, and he does not care about leaving the software or computer in an untouched state. These hackers are very good at leaving little trail as to

where they came from. Spy hackers would fall into the black hat category as spy hackers are generally entering a computer to steal information from it.

White Hats

White hats are the "good" guys. They aren't breaking into computers for unethical reasons or to steal data. A white hat usually has just as much knowledge as a black hat when it comes to the computer world including computer networking, network protocols, and systems and programming. They also understand programming languages, can write programs, alter programs, and destroy programs.

The only difference between a white hat and a black hat are the intentions. Black hats do it for money or for themselves. White hats are usually working with an organization to protect the organization against black hats. White hats are often employed to conduct periodic assessments of the security of the company's system. They also conduct penetration tests. When they find weaknesses, they work to strengthen the network so that the company's files will be safe from black hats.

Grey Hats

Just as the name implies, grey hats are somewhere in the middle. They are really acting maliciously, yet neither are they trying to help an organization. Grey hats normally have a typical job and hack in their spare time. They have

expansive knowledge in the area of computer programming, though the level of knowledge ranges, depending on the length of experience a grey hat has. Grey hats typically break into computer systems that they should not enter, but they do not do so to destroy the system. They just break in for the fun of it.

Technically, they are not hurting anyone. Sometimes, they even expose the weaknesses of the system to the company, and the company can protect themselves against a more malicious break-in. Some of these hackers may shut down the computer system, once again, just for the fun of it, but most are not harmful. These hackers are ones who might leave a fun note on the computer or in the system just to let the company know that they could enter, but they generally don't cause any harm, making them fall in a grey area of ethical behavior.

Script Kiddie

This type of hacker is an amateur. They are not typically versed in programming and use downloaded or bought tools to break into systems. Their success ranges depending on their experience. The intentions of these hackers can range from ethical to unethical. Think of script kiddies as children who aren't done cooking yet. You're not quite sure yet how they will turn out.

Hacktivist

Hacktivist don't necessary have an unethical end result in mind. They

are simply going about their goal in the wrong way. Hacktivists want to bring attention to political matters or figures. They use their hacking skills to post persistent ads or information in a system. They may be working with the political figure or cause, or they might be working individually.

Phreaker

Last of all, you have the phreaker. Phreakers don't work with computers; they hack into telephone systems. Once in, they make multiple telephone calls without having to pay for them. This type of hacker is obviously acting illegally, and they have been used sporadically by business or organizations that need to make multiple phone calls but do not want to pay for the bill.

Motivations

As we discussed, being a hacker can be a completely ethical position where you go to work every day or it can be a hidden, black-market job where everything you do it illegal. Obviously, black hats cannot be condoned for what they do, and I could never recommend you use any programming knowledge you have to that end. However, it is good to be aware of the different types of hackers.

Being a white hat is a noble profession, and you can use the information in this book to learn more about hacking and the tools you need to

understand in order to become successful in the profession. Continue reading in chapter three to learn about the types of attacks that hackers may attempt to use on your computer or at your business.

TYPES OF ATTACKS

There are three main types of attacks that hackers use to enter a specific computer or a network system. The three categories are malware attacks, password attacks, and denial of service attacks. Sometimes, a hacker will use multiple types of attacks linked together to completely infiltrate a system. Being aware of these types of attacks will prepare you for avoiding them. In chapter five, we will go over the most common types of attacks, how to recognize them, and what to do if you come across one.

Malware Attacks

Malware shares the same base as software, because it is essentially the same thing but with different intentions. Software contains a program for your computer that will teach your computer to perform certain tasks. Some software may contain programs for you to use. Malware performs tasks and sets up programs on your computer, but they are programs you do not want. Malware programs typically serve a third party's interests.

They can range from relatively harmless (only putting pop-up ads on your computer) to disastrous. Some malware programs can range throughout your computer and steal passwords, track your keystrokes, and gather data before sending it off to the third party who invaded your computer. Pop-up

advertisements can be obvious, but sometimes, the malware program is so discreet that you don't even know it is on your computer until you are trying to figure out who stole your credit card information.

Before we talk about a few specific types of malware, let's discuss how malware gets on to your computer. After all, if you're going to stop it, then you need to know how it is succeeding. Malware, at least the first time, is downloaded onto your computer by the direct choice of a user. Malware cannot sneak into your computer without you having done something to put it there. Downloading free music from an untrustworthy site is a great way to get malware. You may have the free music, but it is also packaged with malware. This is called the "Trojan horse" method. Once malware is on your computer, it can be programmed to download other malware, slowly making the problem more and more overwhelming.

Your computer can also become infected through file sharing. Any sort of download should be regarded as hiding possible malware unless it is from a reputable site. Also, emails that have links to click or attachments to open could contain malware that is damaging to your computer. Some websites can contain malware, but once again, you have to click something to let it have access to your computer. If a website insists that you need a certain software to view its contents, then you should always click no. Yes would allow the malware to download. If you see multiple errors menus appear or the website

does not want to let you go back to the site you were on before, then those are red flags that they are trying to install malware on your computer.

Malware that changes the operating system (as much normal software does when it is installed) is even more difficult to remove. Some malware even comes with no uninstall button. There are five basic types of malware that we are going to discuss today.

- Virus- Viruses for a computer work the same way that viruses in a person work. Once they invade, they begin multiplying by themselves and attacking healthy "cells" to survive. Viruses will make you unable to access certain files on your computer or even delete them altogether. Viruses are one of the oldest and most well-known types of malware attacks; however, that does not mean that their procedures have become outdated. They have become craftier along the years and can be very difficult to destroy.
- Spyware- This type of malware spies on you and your activities. In most cases, spyware is almost undetectable. It usually gathers information and sends the information to a third party. While most individuals should not have to worry about being infected with spyware, you should be even more aware of the procedures if you own a business or work with sensitive information. Spyware can view the websites you visit, your IP

address, and even keystrokes. Because it can record your keystrokes, even when your password is not visible on your screen, your password will be known by the other party. This is why changing your password frequently is so important. Sometimes, spyware is only used to understand the customer base for a business and know how to advertise their products; other times, it can be used to steal your identify and information.

- Adware- This type of malware sometimes monitors the websites you visit. It then customizes the ads to reach you. Either the presenter is trying to sell the product advertised or they are being paid to sell the product. Pop-up ads will appear when you are online, even if you not visiting dangerous websites. These will not usually cause lasting harm to your computer, but they can be annoying. Some adware has even been discovered imbedded in the software of low-cost phones made in other countries.
- Worms- Worms are like viruses, because they can replicate themselves. Worms can survive all by themselves, unlike viruses that need to be connected with another file. Worms are much more dangerous than viruses because they can replicate and worm their way into various computers on the same network. That means that if you are connected to a network, you don’t have to download a

worm for it to be on your computer.

- Browser Hijacking- This type of malware is easy to identify, because it does not work silently. You will see your browser modified and shortcuts created without your doing anything. Usually, you are being directed to websites that advertise a certain product. This type of malware is meant to generate sales.

Password Attacks

Password attacks are when a person uses software to identify your username and password combination to gain access to an account or information they should not see. Obviously, this can never be simply a grey hat operation. There are three main types of password attacks that you should recognize.

First of all, there are passive online attacks. These attacks to gain your password are done quietly and smoothly so that you don't even realize the attack is being done. The hacker generally needs some sort of software to perform one of these attacks. In this sort of attack, the hacker intercepts your password between when you type it and when the authentication server receives it. This can be called a "man in the middle" attack. Sometimes, the hacker will even capture the authentication packets along with the password for authentication later. This way, they don't even really need to learn the password. They just submit the captured information along with the

authentication packets, and they are able to gain access.

Secondly, there are Brute-Force attacks. Brute-force attacks are a last resort sort of attack as this takes such a long time. There are programs that are available to help with this sort of attack such as Zip Password Cracker Pro. Basically, the program sorts through all possible possibilities- letters, symbols, numbers, and capitals. There are, many times, other weaknesses in the system that are much easier to try than this sort of attack. If the hacker does not have this sort of program, then he must try each password one by one, which can take a very long time. This method does not work well with longer passwords as there are simply too many options.

If you have a longer password, then chances are that a hacker will try their last type of password attack which is the dictionary attack. This method is simple and consists of the hacker using a dictionary to try different words that and combinations of words that are found there. Because this type of attack is a known way that hackers try to enter your account, it is not recommended that you choose a password that could easily be found in the dictionary.

Denial of Service Attacks

This type of attack tries to prevent a legitimate user from accessing information or a service that is usually accessed in a network or online. Hackers can target your computer or your connection and prevent you from

having access to your email or bank account, even if they don't have access to enter the account yet.

Hackers can flood the network with so much clutter that you are not able to enter your account as the network is trying to process all of the clutter. By typing in the name of a website, you are essentially asking for permission to view the site. If the hacker is flooding your network with information, then your server cannot process your request, and you will not be allowed to view the web page. If you open a spam message in your email, then you are opening yourself up to a denial of service attack that will keep you from accessing your email account.

There is no guarantee that you will not be targeted with a denial of service attack, but you can always protect yourself by having anti-virus software. You may want to apply an email filter and put a firewall on your computer. Changing your passwords frequently to passwords that are strong will also help you be able to be protected.

A subcategory of denial of service attacks are distributed denial of service attacks. This means that there is more than one computer involved in hacking into yours. The main attacker farms out parts of the denial of service attacks to various handlers who are then able to flood your server with information and keep you from accessing your accounts. A botnet happens

when a hacker takes control of various computers without their owners' knowledge for the purpose of performing a denial of service attack on a specific computer. The computers in these botnets are called "bots" or "zombies" because they are not able to control themselves.

There are four ways that information can be sent over a network to attack another computer. The teardrop is sending irregularly formed packets of data. A buffer overflow is what we just discussed, when an overwhelming amount of data is sent on a network. A smurf attack is when a computer is tricked into replying to a fake request for its services, opening itself up for attack. A physical denial of services is when a cable is disconnected or there is some physical interruption to the connection.

Conclusion

This is an overview of the three main types of hacker attacks. Chapter five will discuss the most common threats and easiest ones to perform in depth. In the next chapter, we will talk about some hacker tools that you may need to perform your hacking.

HACKING TOOLS

If you are going to begin hacking, you will need the right tools. As you learned in the last chapter, you don't just want to begin downloading whatever says free as it could have malware attached to it. And just because you want to become a scanner, you are not invincible from being attacked yourself. In this chapter, we will discuss some of the most important hacking tools you will need to have along with which ones are recommended.

Network Vulnerability Scanner

A vulnerability scanner focuses on the different steps that hackers can take to break into your system. This tool attempts to follow the same steps that an attacker would follow to see if your system will hold up against some common attacks. The main engine is composed of different parts that each attack a different area in the computer. There are six main steps that a vulnerability scanner will follow as it is checking out your computer.

Firstly, the scanner needs to make sure that the host is up and running. If there is no response from the machine, then there is no use continuing the scan as no information will be available to gather. The TCP and UDP ports are probed. There are usually some default ports that are probed, and you can most likely change those default ports in the control panel. However, if multiple

ports are probed and shown to be awake, then the rest of the scan can continue taking place.

Next, the vulnerability scanner looks for a firewall. If there is a firewall present, it gathers information on what kind, the company who supports it, etc. Next, the TFP and UDP ports that were just probed are now scanned. The ports that are running will indicate which programs are being used on the computer at that time. Fourth, the vulnerability scan needs to determine the operating system of the scan. This is determined by sending various TCP packets of information to various ports.

Using active discovery tests, the scan targets the open ports to see which services are being run at that time. Last, the scanner will detect the vulnerabilities that are specific to that system and the ports that are open. In the end, you will have an assessment form. The vulnerabilities will never be exploited by the program. If you are running one of these programs on your computer, then you will be told how you can strengthen your computer so that malware will not be able to find as many vulnerabilities. If you are running the scan on someone else's computer, then you will be able to detect the weak areas in their computer.

I would recommend two different vulnerability scanners. Both are free, and both have good reputations. First of all, there is OpenVAS (Open

Vulnerability Assessment System). This program has its components licensed under GNU General Public License, meaning that it cannot contain something that is going to harm your computer. This program does not work with Windows machines. Once you have downloaded this program, it will scan your computer daily and give you a report, emphasizing any new vulnerabilities.

The OpenVAS manager controls what is happening and keeps track of what scans have been done and when. On the other hand, the OpenVAS administrator provides user feedback and allows you to have some control over the functions and areas that the program scans. You will need Linux for this program to operate properly. While this program is not one of the easiest to use, it is worth it once you learn how everything functions. You will have more features available than on any other free vulnerability scanner.

Second, you could choose to go with Nexpose Community Edition. This version can scan not only your computer but also a full network, applications, and a virtual environment. You can only use this program for a year before you need to get a new license. This version does work with Windows or any other machine. There is a web port available where you can set your scanning preferences. You can set scans to run at times when you are not using your computers so that you are not slowed up at all.

You will receive a report from this vulnerability scan that will tell you the assets and negatives about websites that were scanned. This version is very easy to use and set up. You will find that it contains many features, but it does have a limit on the network size. This vulnerability scan cannot be used on a network that has a larger IP than thirty-two. Overall, though, you would be happy with the changes that this program makes.

Angry IP Scanner

This is a very popular tool used by hackers. You can look into someone's data through using another tool in combination with knowing their IP address. Sometimes, getting your hand on the IP address can be difficult. Angry IP Scanner can track people and get their information using the IP address that it is able to discover. This tool will help you scan for open ports and IP addresses so that you can get inside the computer. This is a cross-platform software which means that it can be run on more than one system at a time. Network administrators frequently use Angry IP Scanner as it lets you know immediately if there are any openings where someone could enter.

Some hackers were able to tell what ports were open, but they were not able to access them and find their way in until the user was online. This made the hacking more difficult. This tools scans a specific IP range at a time and reports on any open ports. The scan has a parameter to indicate how many

ports it will list and which ones it will search for first. It is easy to understand, and you can use it in conjunction with another tool or without. Last of all, the scan was fast and allows you to continue with your hacking without being held up. This tool is available for Linux, Windows, and Mac.

Ettercap

This type of hacking tool was designed to perform a man in the middle attack, which as described earlier, is meant to steal someone's password. This tool allows you to quickly locate live connections, analyze the host, and dissect both passively and actively. This software is also licensed under GNU General Public License. Ettercap is rather new and does not have a lot of traffic yet, but it looks promising if you are looking to perform one of the password attacks. Ettercap does not work well on computers that use Windows Operating Systems.

John the Ripper

John the Ripper is another tool for completing a password attack. This hacking tool uses the dictionary attack, which was mentioned earlier. This tool can sometimes take a long time to infiltrate the system as the dictionary technique is more reliant on luck than a necessary technique. The success of this tool depends on the strength of the password. Brute-force methods always give a positive result, but it can take a long time to reach that result. This tool

is used by many hackers because of its success rate. Just keep in mind that you may need extra time to crack the password.

Wireshark

Wireshark works to enter systems by probing the firewalls and searching for vulnerabilities. Once the vulnerabilities are found, you can use them to pass into the network and access the files on the computer or the network. This is used by professionals to analyze networks and by hackers to attempt to enter networks. This tool is free and open source. You may recognize the name Ethereal as that was the tool's original name. This tool was designed to run with Windows, Linux, and OS X.

There are many other hacking tools that are beyond the scope of this book; however, the ones above represent a variety of different attacks as were discussed in the last chapter. Feel free to research more hacking tools, but be careful where you download them from. Buying them from a reputable source is usually a safer option.

COMMON ATTACKS AND THREATS

You may think you know which types of attacks are most likely to occur, and so you protect yourself against them. However, you may be surprised what the most common attacks are. In this chapter, you will learn about the most common attacks and threats along with the easiest attacks to perform.

Most Common Attacks

Trojan attacks were briefly mentioned earlier, but let's look into them a bit deeper right now. A Trojan horse is when a virus or an attack is connected to software that you download on your computer. This goes back to when the Greeks were trying to enter the city of Troy to win the battle. They fought hard but could find no way to enter. So, they created a huge wooden horse on wheels and pushed it up to the gates. Those inside thought the horse was a gift, so they readily let it enter. They even threw celebrations for ending the war. But that night, the horse opened, and all the soldiers hiding inside killed everyone in their homes.

Attacks on your computer love to disguise themselves as something you want to download. The surprising thing is that Trojan attacks can often be found on a website that can be normally trusted. Hackers can break into the

website, making the website another victim of their scheme. You think it is a trusted website, so you accept whatever is being offered. That trick of making something look good so that you will accept a virus on your computer is one of the most common attacks.

Another common attack is unpatched software. There are known, unpatched exploits in common software that you would think you could trust. Software can be Java, Adobe Reader, and Adobe Flash. It is well known that if your programs are perfectly patched, then you are less likely to be exploited. However, many people don't actually do anything about it. If you see that your programs, even programs with big names that you can trust, are not patched well, you need to adjust that to protect yourself.

Phishing is another way that you can be targeted. While a lot of spam email goes into the spam folder, some emails can look very legitimate. The email can seem personal, answering your questions, if you responded to an ad. However, these phishing emails usually want a lot of personal information very quickly. Case in point, I was looking for a house to rent. I saw an ad and sent off an email. The person responded with a very long-winded reply about how they were a missionary in Africa and would not be able to show me the property personally. However, I could drive by and inspect it. He said to ignore any for sale signs I might see. Those were just from earlier, when he was trying to sell the house. Now, he's decided to rent it. He told me that he

just need my payment information, and I could move into the house immediately. He wanted my payment information, but I couldn't even look inside the house? That's definitely phishing.

Emails that are from dangerous sources usually do not reply when you respond and don't give them the information they want. If you ask more questions, they might send you the same rote reply or insist you give them the information first. This is a very common way that people are scammed. Their personal information is then used to take money from their account.

Easiest Hacks

If you are interested in hacking but you don't know if you'll be able to do it, let me go ahead and tell you that you can. I read an interesting news story about a seven-year-old who was able to hack into a public wi-fi system and set up a "man in the middle" attack. The news article can be accessed here. The child watched a tutorial on how to hack in and was able to do so in less than eleven minutes. So, if you're worried about starting out on this new venture, I assure you that you should not be.

We will start off by learning how to hack a website which can be done in only four steps. With the right tools, this attack can be done easily. First, you need to locate a vulnerable site. There is something called Google Dork that can help you locate websites with certain vulnerabilities. It works just like any

search engine. You type in the name of a vulnerability, and the search engine will show you websites with that vulnerability. Once you have had a little practice, you can use this to help you locate websites that have the vulnerability you are most versed in.

Let's say you want to break into a website that has files under a password. You might use the following code: "intitle: index of master.passwd." The websites that appear are those that fit your description. You will now need to use a vulnerability scanner to narrow down your list of prospects even further. One tool that is a vulnerability scanner specifically used for websites is Acutenix. This tool was designed for website designers to tests their products and see what else needs to be adjusted to make the website invulnerable. This application does cost money, though you can get a free trial right from the source.

Acutenix does not help you with penetrating the website. You merely put in the URL of the website you are considering, and Acutenix will give you a list of the vulnerabilities associated with the site. If you see a vulnerability that you feel able to attack, then you can move forward to the next step.

SQL is a programming language and has been made into a tool that is easy to use, even for those who do not understand the language. The programming code captures information stored in the website's database and

allows you to have access to the information. With the program Havij, you can use SQL programming language to penetrate the website. You need to pay for the full version of this hacker tool, but there are cracked versions of the tool out there that can be available for free.

Once you have Havij, you just copy and paste the website address you are targeting and start the app. There are various options of what you can search for, and you literally press "get." After a few minutes, you will have retrieved usernames, passwords, and other sensitive information. Websites that contain extremely sensitive information will have stronger protection than this, but even some high-profile websites, Sony being an example, were able to be hacked using this method.

If the website is too strong for the method just suggested, you may try a denial of service attack, but that is a bit more complicated and for more advanced students of hacking.

Now, let's talk about how you can create your own worm virus which can be used on your computer. First, you will need to log into your computer, go to the C files, and create a folder. Name the folder Programs.

In your notepad application, type "@echo off." Starting a new line, write the following words: "Copy C:\Programs\virus.bat C:\Programs". On the third line, write the following: "Start C:\Programs\virus\bat". Save this note in

the folder that you created earlier, and make the file name virus.bat.

You can right click the file you just made and click “create shortcut” to make the worm start whenever you start up the computer. You should right click on the shortcut you have just made and select cut, then right click again and select copy. Right click on your start menu or home screen and select the button that says “Explore.” Go to All Programs and find a file that says “Startup.”

Paste the shortcut onto the startup folder. Right click on the shortcut to access the properties, select “hidden,” then press “Apply.” When you restart your computer, you will see the worm virus beginning to work. When you want to get rid of the virus, you can delete the folder in which the virus is located.

Conclusion

Now, you understand the most common attacks that can occur on your computer. You also know how to create a few basic attacks. Later on, I will show you some more advanced hacker tools that can do even more damage than the tools we discussed earlier.

HIDING IP ADDRESS

When you connect to the internet, your computer is given an IP address. When you visit websites, that IP address is logged, and a trail of your internet activity is created. This makes you lose some of your privacy as websites can track your activity. If you could completely hide the IP address of your computer, I am sure you would choose to do that. Unfortunately, IP addresses cannot be completely hidden and still allow you to have full access to the internet. However, you can hide your IP address most of the time using one of the following methods: virtual private networking or an anonymous proxy server.

The Easy Way

Before we start talking about virtual private networking or an anonymous proxy server, I want to mention one easy way that you can temporarily hide your IP address if you are trying to hide your geographical location or bypass bans or blacklisting of your IP address. If you go to a coffee shop or a restaurant that has free wi-fi, you will find that your IP address doesn't travel with you. Now, an open network is never one you should use to transmit secure information. As was mentioned in last chapter, open networks are easy to hack. However, for a temporary solution, open wi-fi can help you.

When you use an open wi-fi system, you are temporarily using their IP address. You can check your IP address one of two ways. First, you can go to your networks and see where you are connected. If you are connected to a wi-fi or Ethernet port, you will see your IP address under the status. Check your IP address when you are at home, then check your IP address when you are connected to free wi-fi. You should see the change. You could also choose to go to whatismyipaddress.com and check it both at home and out. So, that's the easy way to hide your IP address. However, it is definitely not a permanent solution.

Virtual Private Networking

Virtual private networking is a service that is offered online. There are some free VPN services, but you can also pay for a service. The service you choose determines the safety level you will have. Once you have signed into your VPN account, you will use the IP address assigned you until you sign out. This IP address can originate from another state or even from another country. Providers of VPNs promise not to track their customers' online traffic.

There are quite a few websites that offer VPN services. However, based on security and reviews on performance, there are two that really stand out as working well. Private Internet Access is the name of the first one. It encrypts all information that passes from you to the website so that anyone

trying to plant a “man in the middle” attack would be unsuccessful. This service does not log your traffic or keep any record of where you have been, meaning that you have privacy even within the service. They also don’t discriminate against certain IP addresses. Anyone can use them. They are versatile and able to support multiple operating systems and function well with each one. You can choose to pay $7 a month for this service or up to $40 a year, and you can use the service for up to five devices at a time. PIA even offers a way to connect your router to the service so that you are constantly hiding your IP address.

IPVanish VPN is another service that works hard to protect your privacy. They operate a little differently in that they use shared IP addresses. This does not compromise your security; it simply means that the service itself cannot track your internet use. Because you are sharing an IP address with one or more other users, your activity is mixed, and it would be impossible for the service to realize which websites you specifically are visiting if they stored that type of information. You can get around location restrictions by choosing from what country you want your IP address. This service offers connections for OS X, Windows, and Ubuntu as well as mobile connection for IOS and Android. This option is a little bit more expensive at $10 a month with only two devices allowed to connect at a time.

It is up to you to decide what VPN option will work best for you or if

you prefer to go with a different method altogether. It is important to note that your activity won't be tracked and that you can choose a location for your IP address so that you will be virtually untraceable when using a VPN. This is also a good way to view TV shows and other programs that may be blocked by the local ISP's in your current location.

Anonymous Proxy Server

This type of server acts as a middle man between you and the internet. The server sets up like a computer with its own IP address. When you want to go somewhere, the anonymous proxy server makes the requests to enter the website or obtain the information on your behalf, meaning that the website only sees the IP address of the anonymous proxy server and not of you. Many anonymous proxy servers are available for free on the internet. You simply need to connect to the internet to view your options. Because they are free services, they are sometimes apt to have problems. They have small bandwidth limits, and you may have trouble accessing the information you want in a timely manner. Some proxy servers may disappear from the internet without notice. The servers that charge fees tend to offer a better quality of service. I recommend anonymous proxy servers as more of a temporary solution as you work to permanently hide your IP address or if you are asking for certain information that you don't want associated with your computer.

HACKING AN EMAIL ADDRESS

If you lost the password to your email account, knowing how to hack in can be useful. You can also use the methods taught in this chapter to check your account's security against basic hacking techniques.

Stealing the Password

In order to log into a Gmail account, you need to know the password. If you have taken a few guesses, and you cannot find out what the password is, then you can try using the key logger method. There are some limitations to hacking into email. The two-step verification that includes sending a code to the account's mobile device is difficult to get around unless you have the mobile device in your possession.

You will need a key logger program to track the keystrokes. Actual Keylogger is a great program to help you accomplish this purpose. Actual Keylogger is free program that runs in the background of a computer. It records every keystroke taken, and the name and time on each website. The information is encrypted and stored in a file that only the administrator can see. This file of information contains all the keystrokes taken, money that was transferred online, the time stamp of each website visited, and if any CDs were copied. This program was originally designed for parents worried about their

children's safety and business owners who do not want information about their secure matters leaked onto the internet. One great feature about Actual Keylogger is that you can completely hide its presence from the computer owner. You can hide it to make it invisible and even undetectable by firewall software. You can also hide its shortcuts and startup file.

For this method to work, you would need access to a computer where the email account is accessed. This can be a public computer or a computer that is used by various people in your family. You will install the program and need to adjust the settings. Make sure that anything you don't want monitored is turned off so that you are not overwhelmed with information.

Usually, there is a button called the log viewer within the program on the computer. Other programs may send you an email with the update on activity. By having the time stamps of the pages visited, you should be able to filter when the password was typed and be down to a couple of options. You now have the password, and you can enter the account from anywhere and everywhere. If you enter from a new location, they will most likely get an email notifying them of the new activity.

Here is one more way you can access the target's password if you are not able to use a key logger program. Launch the browser that the target uses on the computer where they use it. Open the password manager. In Chrome, you

will select “settings,” “show advanced settings,” “passwords and forms,” then “manage passwords.” In Internet Explorer, you will press “internet options,” “content,” “settings,” then “manage passwords.”

Use the search bar to search for Google. You should be able to click something that says show or show password to see the password of the account you want to see. Close the password manager and try using the password from a different computer. You should be successful in entering the email account.

SPOOFING TECHNIQUES

A spoofing attack is when a device or person masquerades as another device or person by entering false data. The word spoofing itself means cheating or acting truthful but with false information. Basically, it is an attack that is played by tricking the other party into thinking you are something you are not. In this chapter, we will go over some basic spoofing strategies along with an example of a successful hack using spoofing.

Types of Spoofing

There are six basic types of spoofing that we are going to talk about today.

- IP Spoofing- This is a type of spoofing that is very similar to a "man in the middle" attack. The hacker gains the IP address of another machine and pretends to be the attacked machine by using this new IP address. By inserting itself between the sending machine and the attacked machine, it is able to receive the messages that each machine is sending each other. These two machines can be two computes or a computer and the internet. This attack even allows the hacker to send messages as though they come from the attacked machine.

- URL Spoofing- Phishing is often performed through using URL spoofing. This kind of attack is done by reproducing a genuine website on a server that is controlled by an attacker. Users will think that they are connected to a trusted site, such as a bank site, and type in information such as their usernames and passwords. The attacker is then able to use these usernames and passwords to gain access to the accounts on the actual website. However, you may think this a pretty difficult attack to pull off. After all, the target would see that the URL address is not right. That is where the URL spoofing comes into play. URL spoofing is having a bug in the site that makes the URL appear different than it really is. The target inserts their information then is given an "incorrect password" message and immediately redirected back to the legitimate website. However, the attacker has already gathered the information necessary to enter the account.
- Referrer Spoofing- This process involves sending false referrer information in the form of an HTTP request. This kind of spoofing is similar to what you learned about two chapters ago with VPNs. This kind of spoofing allows a user to masquerade under a different IP address so that their path is not tracked or recorded and their internet activity remains private.

- Caller ID Spoofing- This spoofing technique allows someone to make their name and number appear different on the caller ID mechanism on a phone. Similar to the way you can masquerade under a different IP address. Phones can now appear to be owned by someone different. Telemarketers or political callers could use this to make you more likely to answer the phone. However, hackers could also use this technique to gain information from a person who thinks they are someone else. This form of spoofing usually comes in the form of a card or chip that is inserted in the phone.
- E-mail Address Spoofing- This kind of spoofing is a technique where the email address is altered to make it appear as though it comes from someone else, making a person more likely to open the email if they think it is something personal, not spam. By changing a few areas, this may convince a user to reply to the email with private information. However, then that information can be used to steal the person's identify or bank account information. This is why it is never recommended to send private information over email.
- GPS Spoofing- This type of attack includes broadcasting signals that resemble GPS signals to confuse a device and

broadcast its location as a different location than it really has. At first, the hacker might broadcast false signals synchronized with actual signals, then the false signals are strengthened and start drawing away from the real signals, confusing the device trying to find its location.

Example of a Successful Hack

These spoofing techniques take place all the time. One large-scale example happened in May of 2016. The Milwaukee Bucks were attacked using the email spoofing technique. A hacker was able to either access the team president's email using the email hacking techniques discussed earlier or was able to masquerade under the team president's IP address. He sent an email to all the players on the team asking for their W-2 forms.

Unfortunately, many of the players didn't suspect a thing. They filled out their forms and turned them in, giving this hacker a wealth of information: names, social security numbers, financial information. The IRS and FBI were brought into the matter to investigate and try to protect the victims of this scam. With email spoofing, the hacker normally poses as a high-ranking individual who needs information for some reason.

MOBILE HACKING

In this chapter on mobile hacking, you will learn what you can do to gain access to another person's cellular device. Before you begin doing any hacking, you will need a Bluetooth Hacking application.

Bluetooth Hacking

There are several options of Bluetooth hacking applications, but I recommend Super Bluetooth Hack 1.08. This software allows you to gain access to some of the phone's features over Bluetooth. The downfall of this software is that the phone you want to enter has to have their Bluetooth function turned on. Most people have this function turned off unless they are directly using their phones.

If you choose to hack via this app, you should know that it comes in another language. If you want to change it to English, you need to find "Nastavent" then select "Jazyk" and you should be able to see the English language and change it. This app is one of the most popular Bluetooth hacker apps, and it has worked successfully for many users.

What information does this app allow you to access? You will have

access to the messages on the phone, contacts, call logs, the SIM card information, and the network information. You can play the music and ringtones on the phone, even if the phone you are hacking into is on silent. You can unlock the phone, switch it on and off, restore the phone to its factory settings, and call from that person's phone. This app has a lot of power.

If you want to follow this method, you will need to download the app and change the language to English as was described before. Next, you will unzip the file and send it to your mobile phone. You will need to install the software on your mobile phone. Sometimes, you can download the app right from your phone, but downloading it on a computer or tablet allows you to have access from that device as well. Also, it lets the file take up less space on your phone. The software will allow you to scan for devices in the area. Once you see a device that has its Bluetooth turned on, you will use the code 0000 to connect.

Other Mobile Hacking Tricks

If the person you want to hack does not have their Bluetooth turned on, you can try some of these other tricks. They will not give you as much access as the previous app gives you, but you will still be able to have fun with your friends.

You can call someone from their own number or any number of your

choosing by following these steps. Go to mobivox.com and register for an account. The account is free. There will be a phone number field when you are registering. You will put the phone number of the person you want to call (not your own phone number) during that step. Once you have confirmed your account, you will be able to login.

Then, you will be given three steps. The first step will ask you to enter a number. You will choose your country, and you can enter any number, including your friend's own number. Select your phone will be when you select who you are going to call. You will then call. Imagine what your friend will think when he sees his own number calling him!

Here is one last mobile hacking technique. What do you do if you want to read a message without opening it? Maybe you don't want someone to know that you have seen it, but you are curious to see what it says. This is very simple. You just need to click Options then forward. You will now be prompted to type in a recipient, but you can read the full message without actually having to forward it.

Enjoy using these new tricks to gain access to information you shouldn't be seeing!

OTHER COMPLEX HACKING TECHNIQUES

The hacking techniques that I will discuss in this chapter are not just for using on your friends or to have fun. They can cause real damage and should not be used to harm another person. You will learn about some serious tools and techniques.

Kali Linux

What is Kali Linux? The practical definition is that it is an open source project that was created as part of an internet security training and penetration testing services. It is maintained by Offensive Security.

Kali Linux has over three hundred programs that are meant to test the vulnerability of a computer or network. Some of the programs that come with Kali Linux are Wireshark (which was mentioned earlier), John the Ripper, nmap, Armitage, and Burp Suite. You already know about some of these. Basically, all the programs included are meant to attack computers and websites from different angles, either trying to undo the password or intercept the communication. This whole program was based on Debian testing and is based in that. The application is maintained by a small group of people so that your information will remain private, and the packages of information must

have the permission of the developer before they can be accessed.

Kali Linux has part of its resources dedicated specifically to addressing Android access and compatibility, meaning that the app works especially well with Android devices. Users have reported Kali Linux as being easy and friendly to use, a greatly updated version of BackTrack, if you are aware of the program that was popular previously. Basically, this program can be used to penetrate any website by using the various tools available within the package. You can also use this hacking tool to check on your own website or computer's security.

Evil Twin

This technique sounds like exactly what you think. This is a fraudulent wi-fi access point that is set up to look legitimate. This type of connection is generally used to steal passwords or other secret information. If you are going to create and evil twin access point, you will need the Kali Linux software. As state above, Kali Linux has a lot of possibilities.

Once you are logged into your account, you will need to create a DCHP server. You will do this by opening the terminal and typing the following: "apt-get install dhcp3-server". Once the server is installed, you will need to manage it so that you can make the settings specific to your purpose.

If you want to know the specific steps for preparing an evil twin portal,

follow this link. This website will show you specifically each set of codes that you need to type and how to find the information relative to your computer and the area where you will have the portal.

You have now completed setting up one of the more difficult hacking techniques. If you are having trouble making it work on the first try, go back through and make sure that you typed everything correctly. You should always try getting a few successes on easier techniques first before you try one of the harder techniques such as the evil twin access point.

PENETRATION TESTING

As you have learned before, having a MySQL database can be useful to your hacking needs. Certain hacking codes will need the database to have the codes organized and able to complete their purpose. Penetration testing was discussed a bit before, and it is a proven way that you can identify the security of your computer and the weaknesses that you need to address. This chapter will walk you through how you can complete penetration testing using MySQL.

Many websites use the MySQL database as a platform for the website's functions. If you have MySQL as your platform and do not perform a penetration test using it, then you are opening yourself up to multiple security hazards.

MySQL is regularly updated to perform new functions or to perform the regular functions even better. Because of these constant updates, a security plan that you put into effect four months ago may now not fully cover your device and/or website.

So, what allows many penetration attacks to occur? There are two main reasons that hackers are able to complete penetration attacks: the data was not input correctly or dynamic queries are in use. More complex problems will be

covered a little later on. Finding the way and reason that your website or device is vulnerable is the only way that you can prevent it from being harmed.

You may be experiencing a single quotes issues or multiple queries with a colon issue. A single quotes issue occurs when you use MySQL, it is not necessary for you to use the single quotes function. You can skip the need for that by using a constant string that does not need single quotes. If you want to know the value in a field that is labeled 'username,' you could use either one of the following examples:

- Username like 'A%'
- Username LIKE OX4125

Both of these values equal the same result; however, you can bypass the single quotes by selecting the second option. Next, you may find yourself asking various questions in the same sentence, using only a semicolon to separate them. The MySQL database does not understand this type of command and will therefore not function as you may have thought you wrote it to function when you are using non-homogenous SQL commands. A hacker will easily identify that error and know that your website is easily attacked with a SQL injection attack.

There is another term known as fingerprinting your system. The marks /* */ are used to identify comments. MySQL identifies exclamation marks within

the comment field. When many exclamation points are used, then your website is fingerprinted as a website that is easy to hack. You can prevent this by cleaning out the comments section from comments that have such command marks.

If a hacker identifies your site as its next attack, then it will begin searching to identify the version of MySQL you are using so that it will eventually be able to identify the weaknesses of that particular version.

- Union all select @@version/*
- Union all select version() /*

Those are both ways that a hacker can identify your version of MySQL. MySQL has two different kinds of users, the ones who are connecting to the database and she one who is executing any commands or queries to the system. The two bullet points below show the injection attacks that will be used to identify the user. You should try completing these attacks on your own website to see if it is vulnerable to giving information to hackers.

- Union all select user () */
- User like ‘root%’ or ‘admin%’

You may also need to find the database name. You can find that by using the following command: union all select database() */ By now, you have

probably figured out that this general command can be altered just a little to perform different information finding functions within MySQL.

SCHEMA is a part of the newest version of MySQL, 5.0 and newer. This part of the system contains the information that you just located along with much more information about any databases or tables that you may have stored in MySQL. This allows you as the user to have easy access to your information, but if a hacker could penetrate this area, then he would also have easy access. Performing penetration testing on this area of your computer is one of the most important parts.

While you should periodically perform penetration tests step by step as was described above, you should also have software on your computer that regularly tests your website for any sign of weakness. While the software may not be able to resolve the problem, it will alert you and give you the opportunity to change your programming before a hacker gets the opportunity to gather your website's information.

Metasploit Framework is the world's most-used penetration software. You can download this testing tool for free, and it boasts some of the top protection. This technology regularly works with your computers to upgrade and update your protection and even offers some training tips on how you can educate anyone else who has administrator access to the website so that

nothing is accidentally done that will expose your website. Because hackers are constantly devising new ways to get around security systems, Metasploit is constantly updating itself so that it will be prepared for any potential attacks.

Feel free to look at other software that offers regular scans, updates, and protection. The choice is really up to you, but you must have penetration testing constantly running or you have a higher risk of being invaded.

ETHICAL HACKING

As mentioned at the beginning of this manual, there are three main types of hackers: black hats, grey hats, and white hats. White hats have the same type and level of knowledge as other hackers, but these types of hackers are performing their services typically for ethical reasons. In this chapter, we're going to dive into the following question: are ethical hackers really acting ethically?

Ethical hackers are sometimes employed by large corporations. These corporations pay them to find the weaknesses in the business's security and find a way to protect those areas. However, if someone who is going to perform this kind of work is going to be considered ethical, then they must follow these rules.

- Written permission (a contract) that the hacker has permission to search for security risks and openings in the network. With no contract (verbal contracts do count), then the hacker is acting behind the company's back. The hacker must also have permission from someone who is capable of giving permission. A written contract with Joe down the street to check the bank's security does not count

as ethical hacking. Think of it as this. If Sally wants to borrow her sister's dress, she's not going to ask her brother for permission.

- Respect for the company's privacy. You will be seeing sensitive information if you work as an ethical hacker. You will not be able to share this information with others. If the company were to find out that its information had been shared, you would be seen as the perpetrator.
- Careful procedures must be executed at all times. Knowing what you now know about how easy it is for hackers to enter a computer system via open wi-fi connections, you must choose a secure location to perform penetration testing, etc. You must be connected to wi-fi that is locked and not give anyone the ability to look over your shoulder. You should also always close any browser windows you open regarding the company's safety. This way, even if someone has access to the computer you were using, they will not be able to enter the programs.
- You must report your findings correctly. If you hold back information about a certain vulnerability, then you have lost your white hat title. White hat hackers must be completely honest about any possible hazards to the company's information.

If you follow the above rules carefully, then you will be an ethical

hacker. Ethical hackers are the only kind of hackers who perform their work legally. If you wish to work in the ethical hacking world, you will need to become a certified ethical hacker so that a company will consider you for a position in its protection.

To become certified, you must sit for an exam. You can prepare for the exam through a training course or through self-study at home. You usually need at least two years of ethical work in security to complete the self-study course and be eligible for the exam. If you don't have that background, then you need to take the training course that will give you some of that experience necessary.

The newest version, version eight, has one hundred and twenty-five questions, and it is a pass/fail exam. You need at least 70% to pass. You need to contact the EC-Council or look at your nearest testing center to find the prices both for the examination and the training course.

Fortunately, the job market for ethical hackers is growing. Think about it. Businesses are relying more and more on the virtual marketplace. Every store has a webpage and social media presence. Many stores also use databases to store sensitive information. This also means that the time is ripe for hackers to steal information. More and more businesses are seeing the benefits of hiring someone who can save them from being hacked.

Once you have trained and taken the exam, you need to study the market

in your area. See what prices ethical hackers are charging. There may not be very many in your area, and that gives you even more opportunity to jumpstart your business to make it a success. Here are three quick tips for you as you begin your career as an ethical hacker.

- Have business cards, fliers, and pamphlets. Giving people something to look at will help them remember your business and number.
- Make yourself known. Don't be afraid to visit businesses and offer your services personally. Research which businesses in your area might be interested in your services as an ethical hacker. You may receive a lot of rejections before you get a job.
- Offer some great deals and low prices in the beginning, but don't try to be too economical. Businesses might think you are trying to scam them by offering them a deal too good to be true.

CONCLUSION

You are now prepared to begin your journey towards being an ethical hacker. The programming languages that you are working with will go more in-depth than you did in this book. I recommend that you spend some time playing with the tools recommended here. Get a MySQL database and get to know each function. With use, you will understand the tools better and better.

Remember, if you're not sure about what a business is asking you to do, check back on the quick definition of what makes an ethical hacker ethical. Yes, ethical hackers exist, but even ethical hackers make mistakes sometimes. Make sure that you always have express permission to hack what you are hacking. Having the permission in writing can prevent confusion later. If a business refuses to give you a written contract, then you should know something is strange. Don't accept a position with them simply because they are the only ones offering. Pass up that "deal" and keep looking. You don't want to end up in a legal battle because you thought you were allowed to do something, but you really weren't. Good luck as you begin working with white hat hacking!