Hacking:

The Ultimate Beginners to Experts Guide to Computer Hacking, Penetration Testing and Basic Security Coding

Contents

Introduction

Hackers are those individuals who use their knowledge of computers to infiltrate and compromise the security of other computer networks. They often target home and office computers that are connected to the Internet. The Internet is a gateway to a computer to connect to the world, which also makes it vulnerable to attacks from hackers across the globe. Hackers can work alone or in groups, and in a lot of cases are self-taught.

Positive Side of Hacking

Supporters argue that despite the inconvenience, hackers can cause benefit to the systems of business, they also provide high security to big companies; it helps to make the Internet safer. Businesses nowadays tend to employ "ethical hackers" whose agenda is to test online security based systems and keep away potential threats.

Ethical hackers test the networks for vulnerabilities. Their aim is to check if these networks are secure enough to get past their security defenses. They ensure their companies are not susceptible in any way to attacks from the black and Grey hat hackers who are the bad hackers.

Thank you for choosing to read this book. I believe it will answer your questions and help you understand hacking more.

Chapter 1 – Ethical Hacking

Does the famous word hacking sound familiar? Does it scare you? Ironically hacking is not that bad as many may think. Illegal hacking is bad, legal hacking on the other hand is doing us good. If this is your first book or reading on hacking then surely you will get some potential insight on hacking after reading this. My article gives a simple overview on ethical hackers.

The term ethical hacker came to surface in the late 1970s when the government of United States of America hired groups of experts called 'red teams' to hack its hardware and software system. Hackers are cyber criminals or online computer criminals that practice illegal hacking. They penetrate into the security system of a computer network to fetch or extract information.

Technology and internet facilitated the birth and growth of network evils like a virus, anti-virus, hacking and ethical hacking. Hacking is a practice of modification of a computer hardware and software system. The illegal breaking of a computer system is a criminal offense. Recently a spurt in the hacking of computer systems has opened up several courses on ethical hacking.

A 'white hat' hacker is a moral hacker who runs penetration testing and intrusion testing. Ethical hacking in the process of legally hacking a computer system, that is hacking with permission and penetrating into the systems' database database. The whole idea behind this is to secure the vulnerabilities and loopholes in the cyber-security system.

Legal hacking experts are usually Certified Ethical Hackers who are hired to prevent any potential threat to the computer security system or network. Courses for ethical hacking have become widely popular, and many are taking it up as a serious profession. Ethical hacking courses have gathered huge responses all over the world.

The moral hacking experts run several programs to secure the network systems of companies.

A moral hacker has legal permission to breach the software system or the database of a company. The company that allows a probe into its security system must give legal consent to the moral hacking school in writing.

Moral hackers only look into the security issues of the company and aim to secure the breaches in the system.

The school of moral hackers runs vulnerability assessment to mend loopholes in the internal computer network. In addition to this, they run security software application programs which are used as the measure to prevent against any form of illegal hacking.

Legal hacking experts are people who are used to detect vulnerabilities in systems which are loopholes for the entry of online cyber criminals. They conduct these tests mainly to check if the hardware and software programs are effective enough to prevent any unauthorized entry.

The moral experts conduct this test by replicating a cyber attack on the network to understand how strong it is against any network intrusion.

The vulnerability test must be done on a regular basis or annually. The company must keep a comprehensive record of the findings and check for further reference in the future.

Chapter 2 – Types of Hackers

Internet hacking is a game for some people. They receive a level of satisfaction from accomplishing the task. For many others, breaking into systems is simply a way of ensuring that their own personal or business' security system is successfully keeping out hackers. When people start getting into illegal hacking, they are breaking the law and therefore may be subject to serious legal consequences if they are caught and convicted of an offense.

Some of the different types of computer hacking are outlined below:

White hat - Legal hacking. Typically used for the benefit for those wanting to know whether or not their systems are secure.

Black hat - Using hacking for personal gain.

Grey hat - This type of computer hacking is a combination of the two kinds listed above. A grey hat hacker uses legal breaking into a computer while using the information for personal gain.

Blue hat - Permission is given to another party to break into a computer security system to test for any bugs or errors.

Elite – This term is used to describe hackers who are extremely talented.

Script kiddie – These are the hackers who often use the tools and advice of other people to hack into the system. Typically these hacker not extremely knowledgeable as far as computers are concerned.

Neophyte - Inexperienced in the field of internet basics.

Hacktivism - Spreads a message about personal beliefs through breaking into computer security systems.

Many of these types of hackers, especially talented ones, break laws. No matter the degree of the crime, those arrested are entitled to a defense attorney to protect them from harsh sentences. Sentences for these charges can be more than 10 years.

Chapter 3 – Hacking Methods and their Prevention

What's a or who is referred to as the Hacker?

"Hacker" is a term that has a different meanings. This is based on who and the context that it is used. Thanks to Hollywood, most people think a hacker is someone who gains access to a network or computer(s) and steals stuff. Also hackers are considered people who break into military networks then they launch missiles for fun.

These days, a hacker doesn't have to be a geek from a top university who breaks into banks and government systems. A hacker can be anyone, even the kid next door.

With an ordinary laptop, anyone can download simple software off the Internet to see everything that goes into and out of a computer on the same network. And the people who do this don't always have the best of intentions.

These days, we are faced with a new type of hacker - your next door neighbor. Every day, thousands of people download simple software tools that allow them to "sniff" wifi connections. Some do this just to eavesdrop on what others are doing online. Others do this to steal personal data in an attempt steal an identity.

The Most Common Attacks

Mass Meshing

Also known as mass SQL injection, this is a technique whereby the hackers poison websites by imbedding illegally a redirection javascript from the code of the legitimate websites previously infected and controlled by the hackers. These javascripts redirect the visitor's computer to servers which contain additional malicious programs that can attack a user's computer.

Common targets are Web Servers and Personal Computers
With the ever growing use of wifi, laptops are becoming one of the most hacked devices. Everything a person visits online can be exposed to a person using software to "sniff" that connection. The website URL, passwords used to log into an online banking account, Facebook pictures, tweets, and an entire instant message conversation can be exposed. It is the easiest form of hacking as it requires little skill.

Tablets and Palm Top devices
Tablets, cell phones, and other mobile-ready devices are just as popular as laptops are in wifi hotspots. A hacker in a public hotspot can see a mobile device, as well as all data going into and out of it, just as easily as he can a laptop.

How You Can Protect Yourself

The simple truth is that anyone connecting to the Internet is vulnerable to being hacked. Thus, there is a need to be proactive when it comes to protecting yourself from such attacks.

Sniffing attacks are the most dangerous, as firewalls and antivirus software cannot help. Only a personal VPN can protect a person from a sniffer. The would-be victim, if connected to a personal VPN, has all their data routed through a secure server, making it impossible for the hacker to sniff. A user who has a secure VPN can surf as if he or she is invisible to hackers. PRIVATE WiFi provides such a VPN service.

Chapter 4 – Knowing the Target and Victim

One of the questions I hear all of the time is "who are these hackers, and why are they targeting me?" Many individuals tend to assume hackers are geeks or also referred to as super-smart kids who are poorly behaved and they get a kick out of manipulating the system and causing mischief.

Today, hacking is no longer kid's stuff, but a multi-billion dollar industry that spans the globe. Some experts believe that as many as 25% of all computers are infected by hacker's software. A big part of what hackers do is to turn your computer into a robot.

The tech name for this is a BOT-network, actually. Suppose you go on the Internet and download something--perhaps a song, some freeware, a game--you will never know that download is infected. When you click download, you not only get your music, but the download will install hidden software deep inside your computer that will turn your computer into a robot. This software is called a virus, a worm, spy ware, malware, or a Trojan horse.

The hackers gather thousands of bot computers into a bot network, and these computers are used to send infected files to thousands of other computers. If the attack is caught and traced, it is traced to you, not to the hacker. There are a few symptoms that your computer is a BOT--mainly that it slows down because the hacker is using your resources, but often you get pop-ups, and the computer starts performing unusually and locking up. Often the ISP (Internet Service Provider) will catch this, and shut down your Internet connection.

We have people come in our business all of the time who are incensed because their ISP has shut them down for sending spam. They are always understandably upset, and don't understand until we explain to them that they have been hacked. Once we fix their computer, the ISP will hook them back up. Don't worry, the Internet Police are definitely not going to show up at your door and arrest you for sending spam, everyone knows what is going on here, but your computer MUST be cleaned up before it is put back on the Internet.

Your computer is being used to steal identities, and rob people--by a person who may be on the other side of the world! There are actually businesses who sell time on their bot-nets, for bad guys to send their malicious software to thousands of unsuspecting computers! This leads me to the next type of hacker--the phisher.

The main goal of hackers is to gather information to steal money. Phishing is pronounced fishing--and it is the same thing--fishing for information. The phishers have a variety of ways to steal your information, all of which require YOUR action--clicking on something. A main way for phishers to gather your banking information is to send you an email (through a bot-network) that tells you that your banking information needs updating, and that your account has been frozen until you resolve this.

You may have gotten such an email, it may be confusing because it is not from your bank. These guys know that among the thousands of phishing emails that are sent, some of the recipients will be customers of that bank. According to the FBI, as many as 3% of the recipients of these phishing emails actually input their bank passwords and pins. With one click, their identity is stolen, and their bank account drained.

Another type of phishing works like the bot-network, you download a file, and get hidden software installed deep in your computer, hidden from view. This type of software is called a Key logger. This creepy software allows the hackers to see everything you type-and remotely see, and go through your computer files.

The goal is to find passwords, credit card numbers, names, addresses, social security numbers, email passwords--in other words, your identity. When you log onto your bank account, or type in your credit card number, it is as though the hacker is looking over your shoulder.

These identities are gathered and sold on websites to bad guys who will steal your identity and rob you. They are sold in groups--like complete identities (including name, passwords, mother's maiden name address and credit cards), partial identities. Sometimes these creeps even have buy-one-get-one-free sales of people's identities! The FBI has a whole department that monitors these websites, and works diligently to catch the cyber-crooks. However, many of them are in places in the world where extradition to the US for prosecution is complicated, often Russia or Nigeria.

I do not mean to give you the impression that you are helpless in this, and that you should never use your computer again! There are ways to out-smart them. First, if you haven't read my articles about hackers and cyber-intrusions, read them.

However, I am finding that one of the best new tools to combat key loggers is software where you enter your log-ins and passwords (and credit card numbers), and when you need to log in or enter your passwords, pins, credit card numbers, name, address--anything that can be stolen from you, the software automatically enters it in an encrypted format. You never type this on your keyboard so the keys can't be captured, and if the bad guys can see your computer, what they see is encrypted.

We also recommend that the time has come to make your passwords tough to crack--long, a combination of numbers and letters, unpredictable. For example, your first grade teacher's name followed by a number combination followed by the name of a river you know. I know this is hard, but it is important to have unpredictable and long passwords as a part of your cyber-safety routine.

This problem is not going away, in fact it is slated to get worse. Hackers are not only targeting individuals, but governments, banks, and large companies. So strap on your cyber-pistols and meet those creeps on their own turf--knowledge!

Chapter 5 – Types of Malware

An alarming majority of internet users are either ignorant or careless about the prevalence of threats in the worldwide web. Whenever something goes wrong in their computer, they immediately dismiss it as an episodic malfunction that will not cause serious damage.

Those who are aware of malware infiltration only wait for their entire system to crash before they seek repairs and avail the aid of antivirus protection software.

Cyber criminal activities are not performed by bored high school students during summer breaks - they are attacks by underground organizations, hackers, and hacktivists who intend to cause mayhem in large corporations and governments. Those who target individuals are no less malicious, as they can now install a virus into your computer that will open a backdoor for them to gain administrative control over your entire system.

Accounts will be hacked, confidential documents will be stolen, and worse, webcams will be turned on to spy on you and your family.

Gaining a thorough awareness of these grave threats and the damages they can cause will help a lot in preserving your privacy and your security.

Introducing Malware

Malware, for starters, is short for malicious software. It is a collective term for every kind of harmful software created and launched with the intention of vitiating people through the internet.

The most infamous categories under it are viruses, worms, Trojan Horses, spyware, and rootkits. We will discuss their mode of penetration and the variety of ways they can endanger you.

Worms

Its name can give you a very clear summation of its behavior. This internet pest is an extremely common, self-replicating malware. Because it can be acquired nearly everywhere in the web, it may give you the impression that is something you can easily pluck off your skin and thrown outdoors. We are warning you to alter that mindset.

Worms can enter your computer and remain undetected for months long. After some time, it will begin to delete your files, slow down your programs, instigate avenues for other malwares to pass through, and even create backdoors for hackers.

Prevention is better than cure, especially in this case, because it forces your infected gadget to suffer a slow dead with an impact you will certainly be in agony from.

Worms attach themselves to files and are efficiently spread through mass mailing. Be careful what you open in the internet.

Viruses

You must have heard about the ILOVEYOU bug, the Chernobyl, the Melissa and many more that have caused companies millions of dollars during their debut and their succeeding hype.

The most notorious of its kind steal the contact information of an infected computer's address book, whether through MS Outlook or email accounts, and sends themselves as attachments with a luring prompt that have fooled many people.

It is a difficult malware to get rid of, as it clings stubbornly to every removable hardware plugged into an infected gadget.

Viruses behave in a slightly similar manner to worms; they will infect files and slow down your computer beyond usage. Reprogramming will require that all your files be deleted, because they are probably contaminated with the virus you acquired.

Trojan Horses

This malware initiated the most serious cases of infiltration through trickery. Once it gets inside, like it did in Troy as told by Homer, defeat will be a difficult ending to avoid. Plenty of victims have felt the melancholy that had befallen the Trojans upon realizing that they have been fooled into letting the enemy in.

On the outside, it will appear as an inoffensive photo, document, or application, mimicking authentic ones in its presentation. Your war starts the moment you make the mistake of clicking its ploy. Although it does not self replicate, which is fortunate for us, it does deploy an army of worms and viruses that ensure little chance of survival on your part.

These malware will almost always cost you your files, and eventually your gadget.

Rootkits

The previously mentioned malwares can enhance the destructive forces of Rootkits, as it is created by cyber criminals to gain complete control over its target's computer.

The complexity of its design makes its creators difficult to locate. With control over numerous infected computers, hackers will have an easier time tormenting others as much as they wish to do so.

Spyware

This is the least malevolent malware of the bunch. Spywares usually cause annoyance with the way it can reprogram your applications and encourage the appearances of pop-ups. When this happens, antispyware software is a suitable solution.

Safety Measures

First and foremost, use reliable antivirus software such as Cloud, and be diligent in updating it. Antiviruses do a great job at keeping malware at bay and your gadgets from crashing.

Be extra cautious with the files you download, and get applications only from trusted websites. If you do simply as you will in the internet, even the best antimalware software cannot save you from corruption.

Chapter 6 – Spy Programs and Computer Viruses

In reality, there are various types of programs that can be used for spying purposes. Spy software is very common in the internet today. We can see millions of them found in freeware websites and forums. Software developers are practically giving spyware programs away. Most spy apps are free while others are not. For the free programs, we simply need to download them and install to the unsuspecting victim's computer, but for the paid versions, we will need to pay a certain amount in order to use the program.

Why use such programs?

There are many reasons as to why most people use this type of program. One of which is for personal interest. Some people doubt the actions of their families and friends. They suspect that there is something fishy about the actions of their lovers or friends and they want to know what it is. Through the use of a spying program, they can now find out if there are really some secrets that they need to know. Wives can finally know if their husbands are cheating on them and parents will be able to know if their children are visiting smut websites.

Another reason why most people use spy programs is for management purposes. Most employers want to know if their employees are just slacking off and browsing social networks online. Through the use of spying software, they will be able to find out untrustworthy and lazy employees. They will also be able to increase employee honesty and efficiency since no worker wants to be caught.

Key copying programs

One of the most common types of spyware based programs that we can download today is a keylogger. This type of program secretly records every typed word and phrase that we do in a keyboard. The data collected by the program is then sent to its owner. Some of the things that can be recorded by the software are passwords, usernames, secret phrases, bank account numbers and bank passwords. Basically, anything that a person types in the keyboard gets recorded. The data is either sent as a text file or through email. Since the program is anonymous in nature and is effective in recording everything, black hat hackers often use it for their nefarious schemes.

Spy applications

Another type of software for spying which we can use today is remote spy software. This type of program is often desktop viewing based. In terms of desktop viewing, the user can actually see through the actions done by the victim through tapping the information found in the desktop. Everything is monitored remotely and the unsuspecting victim does not know that he is being watched. A spy based program can be sent through two ways. It can be sent either through remote desktop connection or as an email. It can also work like a virus, infecting a victim's computer without the victim knowing about it. Such are the different types of spy apps that we can download from the internet today.

Dynamic antivirus software plays crucial part in working process of your PC as it protects your personal information from online malicious virus threats. Since the vulnerability of nasty Trojan viruses is increasingly dominating and destroying your computers, it is wisest idea to choose among the best antivirus programs that can serve the purpose of safeguarding your PC. Though online viruses are advancing their approach, software developers across the world are trying their hardest to block such malicious practices and virtual bugs to provide users peace of mind.

One of the harmful categories of online virus threats is a Ransonware Trojan, such viruses plant encrypted files on your PC and hold it in exchange of cash or something valuable. Such virus hostage security of your PC, as in one such case security systems and televisions connected through internet were controlled by third person from far location.

Overwriting virus threats are dangerous as these malicious malwares hold the ability of overwriting and eventually deleting important contents off your system. Such virus threats are rarely spread and if infected, your PC can gradually lose all of the data and programs.

Another form of Trojan virus threat is Root Kits, which if gets on your PC can completely hold access of it. Hackers typically hideaway files, folders, registry edits and other important components it uses. Storm virus is under such category which spreads away through e-mails and if a person clicks on it your PC can eventually die.

Of course, intention behind the virus description was not to scare you but to make you aware of various viruses out there in the world. The key is not to click on anything you're not familiar with on the internet. However, having the best free antivirus security software is always a good backup because it will protect you from pop ups, which are certainly harmful for your PC as clicking it is like welcoming one of such malicious viruses intentionally.

Conclusion

The Newest Target: Your Mobile Devices

Whether you have an iPhone, Blackberry, Android, or any other internet connected phone, your device is just a miniature computer. And exactly as you protect your vehicle with locks, you should also always "lock" your smartphone by setting up a password. At first, it may feel inconvenient to constantly enter your PIN before accessing your phone applications; however, your phone contains enough personal information to seriously compromise your identity in the event your phone is lost or stolen.

Without a security PIN or password, your emails, your saved passwords and your network access is easily accessed by anyone who finds your phone. In fact, many scammers buy stolen phones because it is so easy to request a password reset on your web email or even on your bank account. Consider the financial impact and hassle that would create for you, your company, or even worse, your customers! Put a password on your smartphone and use it consistently to protect your information.

Passwords: A Str0ng Pa$$w0rd is Essential

Effective passwords are critical to keeping your data safe. This cannot be emphasized enough! You may have different passwords for your email and your desktop/laptop or they may be the same. Whatever you choose, it is imperative that you do NOT use your username as the password. You must also avoid using any words in the dictionary, something obvious like your company name, your pet's or children's names, or any password less than 8 characters long.

You should incorporate numbers, capital letters, and symbols (if symbols are supported in your environment) in the password as well. Without a $tr0ng password, hackers can easily gain access to your email account, steal your information, and then send malicious emails to everyone on your contact list. Don't be the one who infects everyone else because "password" was your password.

Thumb/Flash Drives: Beware of Strangers

What if you are leaving your office or walking through a parking lot and you find a flash drive? Should you plug it into your computer to browse the contents to try finding the rightful owner? Probably not. Once you plug the little memory unit into your USB port, you risk silently installing a Trojan that will give hackers direct access to your network. Even worse, a program that hides in the background can capture every keystroke, take screenshots of what's on your monitor, turn on your webcam to watch you, and even turn on your microphone to listen to your conversations.

If you really want to view the contents of the thumb drive, plug it into a computer not connected to the internet, perhaps an old one you don't use and haven't yet recycled. Just remember, even if your computer is not connected to a network, a virus on the flash drive can still destroy all your data. Use your antivirus software to scan the drive for viruses if you have that feature.

Wireless Networks: War Driving is NOT Dead

If you have notebook computers and smartphones that connect to the web, you're using a wireless network -another favorite entry point for hackers. Consumer models of wireless network devices are so easy to setup that you just go to the store and buy what's on sale. By following the simple diagram, you have all the connections made within minutes.

The result: Instant wireless internet! Hooray! It's working! "I can get out to the Internet and everyone is happy!" Yes, everyone, especially hackers, are thrilled. Why? Because there are devices that hackers use to lock onto "unsecured networks" that don't have a password. When wireless technology first emerged, hacking wireless networks was called "war driving".

Now hackers can sit in their homes or public places and use "unsecured networks" to gain full access to your network and shared files as if they were sitting at a desk in your office. Other times, hackers use unsecured wireless networks to engage in illegal, credit card fraud that can be traced back to your location. Moral of the story: Secure your wireless network. If you don't know how to do this correctly, ask a professional.

Compromising Friends: Compromised Email Accounts

In addition to never opening emails from people you don't know, you must be careful with emails that appear to be sent from your friend's account. If you receive a message from someone on your contact list but the subject line is blank, strange, or ambiguous, do NOT open the message.

The result ranged from the recipient's own email accounts being compromised to getting a nasty virus that sent out more emails to the rest of the contact list. Rule of thumb: If you're not sure your friend or associate sent you a particular email, you can always ask them on the phone or send them a separate message to inquire about the subject line. It is better to delay opening that message and error on the side of caution than it is to be a victim of your friend's compromised email account.

Safe Surfing: Just a Few More Reminders

You should avoid clicking on links in emails. The link may appear that it is going to your favorite website; however, the code behind the link can redirect you to the wrong site that looks identical to the official site. NEVER click links in emails to reset passwords unless you have just requested a password reset less than 5 minutes prior.

If you receive an email with a link telling you that you must change your password for any account, delete it immediately and contact the company directly. Finally, never give out personal information unless you know 100% that you are on the correct website. You should always type the official URL into the browser address bar or bookmark/add the official site to your favorites.

Thank you for taking time in reading this book. I believe you have learned something on hacking and how to be safe from black hat hackers.