HACKING

for Beginners

48 Things Every Hacker Must Know About HOW TO HACK

Daniel James

Hacking

Hacking for Beginners: 48 Things Every Hacker Must Know About How to Hack

Table of Contents

Disclaimer

While all attempts have been made to verify the information provided in this book, the author does not assume any responsibility for errors, omissions, or contrary interpretations of the subject matter contained within. **The information provided in this book is for educational and entertainment purposes only. The reader is responsible for his or her own actions and the author does not accept any responsibilities for any liabilities or damages, real or perceived, resulting from the use of this information.**

Introduction

Hacking. For some people, an art. For others, a dreaded curse. For certain groups, a necessity. For the celebrities and the famous people a blatant disrespect of their privacy. For the politicians a two edge sword that can work both in their favor and against. For the information technology professionals, another two edged sword as some of them may get a job trying to fight hackers and some others will get a salary out of trying to hack protected systems. For many youngsters just a pass time and something to do for fun.

The philosophical issues behind hacking are many and the debate is strong with meritorious points for both sides of the coin. However, this is not the scope of this book nor what will be discussed. This book will focus on the technical and practical issues that every hacker should know about, before his first attempt to break through even the lowest levels of network or web security.

The one objective concept that characterizes hacking is knowledge. Knowledge of the way software works, knowledge of the thinking behind the security systems, knowledge of the algorithms upon which the security systems and software are based and knowledge on how to bypass, circumvent or overwhelm the barriers that safeguard the information to be accessed.

Most of all hacking requires a specific state of mind. One that commands no hesitation in breaking the rules and the laws should the case be that you may not be interested in anything other than money and profit.

As the saying goes “if you can’t do the crime, don’t do the crime”. Make no mistake. Hacking outside the teaching class, a controlled contest or a business arrangement is illegal and is subject to imprisonment sentences depending upon the severity of the action taken.

It is not under any circumstances to be considered that the contents of this book intend to provide motivation or a basis to any person or group to engage in illegal activities. The contents are solely for informational and educational purposes and they are not to be viewed under any other context.

Now that this point has been made clear, it is time to proceed to the basics that every person that wants to learn about hacking should become aware of.

Chapter 1 – Hacking

To put it simply hacking refers to the processes used to overcome the barriers raised by security software and other methods for the purpose of safeguarding any and all pieces of information that must remain private and confidential.

Most constitutions and legal systems have put in place laws that decree that personal details like names, addresses, telephone numbers, credit card numbers, pin numbers, judicial information, photographs, videos and every other piece of information that was not produced for public use, are not to become known to the general public without the express and written permission of the person that the information pertains to.

The same stands true for governmental information, professional and corporate plans and projects, military information, business ventures, online stores and in general for any condition that requires information that must be kept safeguarded at all costs.

The question of why do people want to hack such security systems has a lot of responses. Some youngsters do it just to pass their time and for no other reason than hacking for the sake of hacking. Some others want to gain profit out of it by stealing credit card numbers and buying things without having to pay out of their own pocket.

More serious hackers do it for reasons of blackmailing or for reasons of divulging secret information to the general public based on a notion that says that the people have a right to know what their government is doing at all times.

Other reasons that hackers do what they do have to do with an aversion to corporate policies that want to make a profit out of services and software that should be offered for free, or as a resistance to governmental policies that are considered as restricting the rights of freedom and personal disposition.

The first thing to now about hacking is that there is not network that is completely safe and that there is no computer that cannot be hacked unless it is turned off and disconnected from a power socket.

With these two details in mind let’s begin with the background that a hacker should have in order to begin exploring the possibilities of hacking.

Chapter 2 – The Background

An everyday user that opens up a personal computer, a tablet or a laptop, surfs the internet, downloads a few files and photos, uploads info to a cloud drive, writes a few documents or edits a few videos and pictures cannot be considered as a person who knows enough to become a hacker.

Neither does an employee going to work and spending eight hours per day for five days a week typing into a specific application on a most probably locked hard drive as required by his ir her employer.

There are three things that are considered as prerequisites for the first step of becoming a hacker.

A) Knowledge of operating systems

Each operating system works differently and may have a different set of weaknesses that can be exploited. Keep in mind that hacking is nothing more than exploiting those weaknesses.

All operating systems have knowledge bases that describe such weaknesses as they are been discovered by users or by the creators of the operating system.

While the specific weaknesses may have been corrected, they show a hacker which aspects of the operating system were not paid enough attention to, by its creators. And always the best way to hack an operating system is from the inside.

B) Knowledge of security software

The security suites released for the general public and the security systems build in to routers and switches are rather easy to overcome once you become acquainted with how they work.

More advanced system administrators use a process called SIEM (security information and event management) which should be thoroughly studied as

it is a multi-stage multi-layered security system. Furthermore, hackers need to seek information on paranoid levels of system administration which include turning off ICMP protocol and laying down traps and honeycombs for hackers to fall in.

C) Knowledge of a programing language

Actually this is incorrect. You should learn at least three languages beginning with assembly which will allow you to get in touch with the processor directly, C which will allow you to learn exactly how memory works and bash scripting which will allow you to write scripts that will do all the work for you. Assembly has been released in many variations. The more of them you learn the better.

Other languages that can be very useful in hacking are Python, Ruby, Pearl and off course PHP which will allow you to break through the security of internet pages.

Assuming that you got yourself familiar with all of the above, the next important step to be aware of is how not to walk barefoot on glass. That means how to protect yourself.

Chapter 3 – Self Protection

The point of the exercise in hacking is to acquire the information you want and not get caught in the process. In fact if it is very easy to penetrate the security and walk away unscathed, it will never let you become a good hacker.

The part of not getting caught in the process requires three more basic level issues that need to be discussed:

A) Secure your computer

Securing your computer means implementing security measures that will not allow someone else to get inside your system. In this case you need to consider your computer as your target, attack it, find out about its vulnerabilities and shut them down.

If you are not in a learning class or in a contest which implies that you already have permission to try hacking another system, if you are trying to test your skills, make sure that you have written permission from the person who owns the system you are trying to attack.

B) Secure your identity

While your computer could be secure, this is not necessarily the case with your identity. There are tracking systems that can follow your signal and determine your ip address and from there your physical address and consequently who you are.

Using proxies or spoofing your ip address are good ways to mask your location and by extension your identity.

C) Cover your tracks

The system administrator or the system owner must never know that you were ever inside their system. If you break user names and passwords make

sure that they are hard-coded. Do not erase files, do not create files or user accounts and stay in the system only as long as it is absolutely necessary.

Remember that every activity is recorded in a log file. Do not erase the entire log file but just the dangerous entries along with some other random lines. Do not forget to look for a backup log file and hope that there is no tertiary log file kept somewhere else.

Now you are ready to begin. And the first thing to do is learn everything there is to know about TCP/IP protocols and networking as every network and every internet connection is based on this protocol. And off course you will need a fast running computer, an optional but strongly recommended proxy server and an IP scanner.

Chapter 4 – TCP/IP

All modern networks, the internet, even private networking works over TCP/IP protocol. For the uninitiated it stands for transmission control protocol / internet protocol. Its purpose is to determine how the data transmitted from one computer to another is packetized, routed, transmitted, addressed and received.

TCP/IP does not recognize any specific operation system. It just needs that the sending and receiving computers have some kind of hardware and some kind of software installed that can identify and translate the packets of data sent back and forth.

Through this neutral property, TCP/IP has become the standard for communication of all devices including personal computers, laptops, netbooks, smartphones, tablets and every other device that can communicate through any network.

Programmers that create the applications for the common users acquire access to the four layers of TCP/IP through internet sockets and APIs.

The internet socket is a combination of an ip address and a port. An ip address is the single number that is assigned by a DHCP (dynamic host configuration protocol) server to identify a single computer. It has the format of xxx.xxx.xxx.xxx, subnet (usually) 255.255.255.0 and it is unique for any computer in a network or the internet. A port is like the door that allows the data packets to go back and forth.

API stands for application programming interface and it is the platform provided by every operating system to allow the applications that are based upon this interface to control and transmit data through TCP/IP protocol.

Just like programmers, hackers use exactly the same tools and similar processes to acquire access to TCP/IP protocol and consequently to the information they need. So it is actually more than imperative that the more you know about how TCP/IP works, the better hacking you will be able to do. Especially with the IPsec architecture that has been implemented with IPv6.

Deep knowledge of the protocol will actually render the new concept of a third access prerequisite irrelevant. The current encryption concept

requires two elements of identification (user name and password). The new concept will require a third element which will be determined by each user. It too will be based on TCP/IP and therefore on the same processes.

The learning process will actually need to take into account two aspects. The first one concerns TCP/IP administrator processes and the second one the TCP/IP blueprints which will explain everything in full detail.

Let's discuss now the first steps that you need to take in a first attempt to become a hacker.

Chapter 5 – First Steps

Computer technology has not yet advanced to the point of receiving commands through someone's thoughts. Hacking still requires that you type commands to the keyboard of a computer. This computer, to understand your commands, needs to be running on an operating system. And here lies the first choice you need to make.

If you are working with Windows you will need a *nix terminal or Cygwin to type your commands in. What they do is actually import a Linux, BSD or Unix environment inside your Windows environment. The environment is similar to a virtual machine one only simpler and faster. It could be a better choice to work directly on a Linux or BSD operating system which offer a plethora of embedded applications and tools that you can use.

The second step is to know your target. In hacking terminology the process of gathering information for a target is called enumeration. For your first few attempts you should opt for another computer in your own network of for a computer of a friend that has been advised of what you are trying to do before you do it.

The next set of steps has to do with testing and identifying the specifics of your target. A simple ping command may show you if the target is active but it is not reliable as it is based on ICMP protocol which may have been turned off. Instead you may want to try running a scan for open ports.

Use pOf or Nmap to run the scan if you are working with Windows, or one of the tools embedded with Linux or BSD. This scan will tell you which ports are active, what the target operating system is and it can even identify the router used and the type of firewall. You will need all this information to plan what you are going to do next.

This plan will be based on whether or not you will be able to find an open path to your target. Ports like FTP 21 or HTTP 80 are usually well protected and should be avoided even if they seem open. Some paranoid administrators may leave them open deliberately to set a trap. Some others may have put in place warning processes sounding the alarm whenever anyone tries to do anything with these ports.

Instead, try to find TCP and UDP ports like Telnet or gaming ports that may have been forgotten or left open as required by the game they are playing.

If you find port 22 open this usually indicates that there is a secure shell running which is susceptible to brute force decryption. If you find an open port in the range of 47000 this could mean that a torrent client is in operation which means that you can piggyback the packets received and go straight in.

All secure networks will ask for a user name and password before they allow access. It is now time to discuss what to do to overcome this initial barrier.

Chapter 6 – Cracking a Password

Most beginner hackers fall into the trap of trying to crack the passwords that allow access to the information they want. The newer encryption protocols do not even allow for weak passwords. However, if you insist on trying to crack someone's password, this is what you need to know.

Password cracking works after you are able to get the hashing algorithm that the passwords are based upon. Most cracking techniques are based on brute force that uses a pre-defined set of passwords in a dictionary. This process may take too long which is contrary to the instruction of staying inside a system only as long as absolutely necessary. It will be easy to get discovered.

You can increase the speed of brute force cracking by cutting down the MD5 algorithm to ¼ or by using the graphics card processor which is many times faster. You can also try to use Rainbow Tables which at this time is considered as the fastest technique.

Trying to crack a password will violate a second of the self-protection rules. Brute forcing techniques get recorded to the log files completely polluting them, which means that you will not be able to cover your tracks.

There are alternative methods to try to discover a password. One of them pertains to a rooted tablet equipped with a TCP scanner. Uploading the signal to the secured location will open the ip address and the password will appear on your proxy.

It could be a far easier process to try to get into the router menu or gain super user or administrator privileges. Most people forget to change the passwords to their routers or do not set passwords for accounts with administrator rights. This situation is gradually changing as the router manufacturers start shipping their products with unique passwords that are printed on the shipping box.

However there still are a lot of older routers that still keep the "admin" "admin" as user name and password. If you can get in the router menu you can get access to the stored password which will also give you access to an internet connection. Gaining super user or administrator rights will give you

access to all the files including the password file which you can open and see all the passwords for all users.

To gain the super user or administrator rights it may be necessary to trick the machine. One such trick is a buffer overflow which will force the memory to dump consequently allowing you to run a higher level programming and load scripts that will give you the access you need.

Supposing that your first attempts on friendly systems were successful, it is crucial to keep in mind a few things before attempting any sort of hacking to an unknown system.

Chapter 7 – Things to keep in mind

Let's face it. Hacking is illegal unless you receive a written permission from the owner of a system or a system administrator. Some of the most experienced hackers will tell you that there is no chance of becoming a good hacker unless you take a risk of facing a real time challenge and do something illegal. We strongly advise against something like this.

If you have decided to learn more about hacking opting to become what is called a white hat hacker, then there are some things that must be brought to your attention before your first unfriendly hacking endeavor:

1) There is only one practice legally acceptable to hack a system. To sign a contract with the owner of a system or with the system administrator of a company that will allow you to try to hack their system for the purpose of improving their security.

2) Never remain confident that once you have gained access to a system and managed to come out of it unscathed, you went unnoticed. Many administrators allow you to gain further access in an effort to make you further incriminate yourself before they take legal action against you. A repeat offense gets a higher punishment than a single attempt.

3) The people that create the security systems and are behind all attempts to keep the information that must be protected safe, are quite knowledgeable and they will do their best to keep you out. This means that you must follow a learning path that will constantly improve your skills. You actually must listen to master Yoda's advice here: "There is no trying. You either do or do not!"

4) There is a major distinction that you must decide upon. Those who deserve the title "hacker" do what they do to gain knowledge through exploration and exploitation not necessarily for evil purposes. "Crackers" do what they do for money. A "hacker" is actually a person to respect. A "cracker" deserves nothing more than a cell in prison.

5) Never bite more than you can chew. In this case do not attempt to hack a system if you are not completely confident in your abilities and skills that you can pull it off.

6) Even very experienced and seasoned hackers avoid hacking systems that have to do with governmental or military networks. Even if you succeed, they have the money and the resources to hunt you down, catch you and throw you in jail. There has never been a case of hacking to such networks that did not result in the perpetrators eventually getting caught.

What all the above should tell you is that to become a successful hacker you need to accumulate knowledge. The first hackers accumulated this knowledge through trial and error and experimentation that got most of them behind bars.

However, one way or another, they managed to transmit what they learned to others who added more knowledge on top, so that now you can have access to the database of many years of experience.

This database is given to you mostly in published books that you need to read and through some other means that you need to be aware of, in your effort to become a better hacker. Let’s take a look at these resources.

Chapter 8 – The database of hacking resources

We have already discussed that you need to study how the operating systems work, how the security suites work and how to program. We also talked about acquiring a deep knowledge of TCP/IP protocol. Are those enough? Certainly and most definitely not! If you ever visit a hacker's house you will find an entire library of relevant books. Without referencing specific titles and authors let's discuss what they talk about:

The mindset

This is probably the most important issue. If you want to become a hacker you must learn to think like one. These books talk about the mindsets of the White Hat hackers and the Black Hat hackers (those we called crackers) but most of all they will teach you how to protect your own system by someone who thinks the same way you do.

The tricks

In the previous chapters we used the term "buffer overflow" mentioning that it is a trick used in hacking. There are a lot more such tricks to learn and a lot of books to read on that subject as the deeper you go into hacking, the more advanced and complicated these tricks become.

The concepts

Let us introduce you to some terms:

- Footprinting and social engineering
- Session hijacking
- Sniffers
- SQL Injection
- Denial of service
- Evasion
- Cryptography

These are just a few of the concepts explored in hacking. You will actually have to read a couple of books on each of these concepts.

Web specific hacking

Hacking a web site or an online store requires the same way of thinking but a different approach than hacking a network or a computer. There are other issues involved and other methodologies to follow. Actually most books that have been written about this kind of hacking refer to both attacking and defending against a web attack.

Probably the most important source of information and insights about all kinds of hacking is provided in the blogs of the hacking community. Whenever something new comes up, a new weakness to be exploited discovered, a new tool to use has been released, there will always be a relevant posting with details and all the pertinent information. So you need to make it a point to always keep visiting these blogs to remain informed with the latest in hacking technology.

The last place that you need to look into to gain knowledge, is the publications presenting the latest updates in the development of security software and techniques. If you know what is been deployed to stop you, it is easier to find out how to circumvent it beforehand.

Hacking is all about knowledge. Remember that it was hackers who created Linux, hackers who created the internet and hackers who created open source software. Being a hacker commands the respect of a person who knows a lot. Consequently you need to learn a lot if you want to enjoy this respect and acknowledgement.

Conclusion

The topic of this book and its context is hacking for beginners. Therefore the approach chosen was the one that assumed that you had no prior knowledge of any of the issues involved in hacking. This approach required that a presentation was made on the initial steps that a person would need to take in his journey to becoming a hacker.

It also required that we introduced you to what you needed to know before even thinking of becoming a hacker. To put all the issues discussed in a simple list:

1) There is no network that is completely safe

2) There is no computer that cannot be hacked

3) You need to have deep knowledge of operating systems

4) You need to have deep knowledge of SIEM

5) You need to learn at least three programing languages

6) You need to secure your own computer

7) You need to hide your identity

8) You need to cover your tracks

9) Acquire the deepest possible knowledge of TCP/IP protocol in both blueprint and administrator levels

10) To begin hacking you need a fast computer, an IP scanner and a proxy server (optionally)

11) Choose the operating system that you will work with

12) Acquire knowledge of your target

13) See if your target is active

14) Determine which ports are active

15) Find out what kind of security safeguards are in place

16) Find an open path to your target

17) Try to crack a password only if you have the hash of password

18) Increase your brute force password cracking speed by cutting down the MD5 algorithm to ¼ or by using the graphics card processor or by using Rainbow Tables

19) There are better and easier ways to gain access to a computer or a network than trying to crack usernames and passwords

20) Gaining super user or administrator privileges will give you access to all the files stored

21) There is only one legal way for hackers. To cooperate with companies to improve on their network security

22) Never assume that you were not noticed hacking a system even if it appeared so

23) When hacking do not try. Do or don't

24) You need to decide if your title is going to be "cracker" or "hacker"

25) Never attempt any hacking if you are not confident of your own skills and abilities

26) Stay away from governmental and military networks

27) Read books that will introduce you to the mindset of a hacker

28) Read books that will introduce you to the tricks that you will need to use

29) Read books that will introduce you to the concepts and the terminology

30) Read books that will introduce you to the methods of hacking web pages

31) Always visit the blogs of the hacking communities

32) Read books that present the updates in security software

All the above is just the tip of the iceberg. Some of the deeper issues of hacking cannot be discussed unless you have acquired a level of understanding first. It would be pointless to present issues that you would not be able to understand.

The purpose of this book was to inform you of the basics and to present the learning process that you would need to get involved in. A process that once you get yourself into, will never end unless you remove yourself from the ranks of the people who deserve the respect of being called hackers.