HACKING

THE BEGINNER'S COMPLETE GUIDE TO COMPUTER HACKING AND PENETRATION TESTING

MILES PRICE

Hacking

The Beginner's Complete Guide to Computer Hacking and Penetration Testing

By Miles Price

Table of Contents

Introduction

Cyber crime is the biggest threat that every organization on the planet faces today! And it's not just the organizations that are vulnerable. People too are at risk of being targeted by hackers.

Inside this book we aim to show you the importance of staying on top of this threat by learning how to hack. While it is true that hackers have received a bad rep over the years, mostly due to biased media reporting, not all hackers have criminal intentions.

This book is meant to serve as an educational guide for people who are interested in learning some simple hacking tools, tips, and techniques in order to protect yourself and your computer networks.

It is to be used for ethical hacking and not malicious activities. If you have ever been curious about hacking and have wanted to learn the art of the hack, then you have found the right book.

We live in a world where everything is interconnected. Back in the day, we relied on the government and major organizations to provide enough security for our personal data. This is no longer feasible in a world where the security agencies themselves are the major targets of malicious hackers.

In fact, in most cases, the biggest cyber threat will come from your very own government!

So what do you do? Sit back and cross your fingers, hoping that your firewall and antivirus program will be enough to protect you? Whether you like it or not, you will have to learn how to hack if you are going to stand a chance of keeping your own cyber systems secure.

By understanding how malicious hackers do what they do, you will be able to detect and prevent any potential threats to a computer system or network. This book will help you do that.

We start off with a general overview of the state of global cyber security. You will learn how to make a distinction between the different types of

hackers out there, their motivations, and the skills that you need to start hacking right away.

We will also cover how to conduct penetration testing to check for any potential loopholes in a network. Every network, no matter how secure, has some kind of weakness. You will learn what goes into targeting, scanning, and analyzing a target, and how to gain access into a system.

There are different ways of hacking a cyber system. We take an in-depth look at some of the top tactics that malicious hackers use to launch attacks on their targets. Finally, what can you do to stay safe as a hacker? Read about all this and more right here.

I hope you enjoy the book!

Chapter 1: It's a Hacker's World!

The days of resting easy knowing that your private information is safe from prying eyes are over! The world we currently live in is no longer what it used to be. Cyber crime is a real, dangerous, and persistent threat that every organization and individual needs to take seriously. Right now we are living in the digital age and in a global village. With everything and everyone interconnected in such a mass scale, it is safe to say that this is a hacker's world.

The new US president himself, Donald Trump, stated that cyber theft is the fastest growing crime in the America. This isn't just his personal opinion. The cyber security community agrees as well.

You don't believe me? Let's check out some statistics.

1. Did you know that the damage done by cybercrime in 2016 cost $3 trillion, and is expected to rise to $6 trillion annually by the year 2021?
2. Did you know that organizations all over the US spent a total of $80 billion on products and services to protect themselves from cyber crime? This figure is expected to surpass $1 trillion in 2017.
3. Did you know that there is virtually no chance of unemployment if you work in the cyber security industry right now? Analysts have concluded that there is an extreme shortage of cybersecurity talent all over the world, with the cyber security unemployment rate dropping to zero percent as of 2016!
4. Malicious hackers are now after blood, not silicon. According to Microsoft, there will be 4 billion people online by the year 2020, and humans, not computers, are now the primary target of hackers.
5. Did you know that the average hacker is able to stay dormant in your network for an average of 200 days without being detected?

These statistics are not meant to scare you. They are meant to open your eyes to what is taking place all over the world. If you watch and read the news,

then you should understand how big this issue will get in the future.

Hacking Defined

What comes to your mind when you hear the word “hacking?” Do you imagine a hooded character hunched over a computer trying to gain illegal access to a network to steal data? Or maybe some geeky nerd with nothing to do all day but send out encrypted programs to infect networks and systems?

Whatever images may have popped into your head, the fact is that most people believe that all hackers are intent on stealing information or spying on people. The majority of people think that all hackers are criminals and hacking is wrong. That may be what is portrayed in movies and TV shows, but it is simply not the case.

Hacking can be defined as an attempt to solve a problem or improve an application by re-engineering hardware or software. In other words, if you have a problem with your computer and are unable to resolve it using conventional techniques, then you may be forced to use whatever technology is available but in a new way. If you look at the history of how hacking started, it all began with the intention to solve a problem using creative means.

The first recorded “hackers” were a bunch of MIT geeks who used old telephone equipment to control their model trains way back in the 1950s. These guys were so into model trains that they took the telephone equipment they had received as a donation and engineered it so that multiple operators could control the train track by simply dialing the phone.

Some of these guys even went further and started modifying the recently introduced computer programs on campus. Their aim was to customize the programs for special use and make them better. They simply used what they had available to get creative, invent a new way of doing something, and solve problems.

This is what hacking is about. Today, hacking may represent a breach of cybersecurity, damaging systems, and illegal access, but that is not the whole story.

So how do you distinguish the good guys from the criminals?

The Psychology of Hacking

In order to stop a hacker, you must first understand what drives them. In the hacking community, there are several diverse and complicated skill levels and motivations. It is important that you understand the different types of hackers so that you can be able to predict their attempts and understand their mentality. Even as a beginner who is learning how to hack a system, you do not want to leave yourself vulnerable to a counterattack.

Categories of hackers

The biggest mistake people make is putting all hackers in the same group as if they have a single purpose. This is often what the media does, and the public has fallen for this lie. You cannot attempt to categorize a hacker without first knowing why they performed the hack and what their goals were. The hacking community is somewhat divided on how to name different types of hackers, but generally speaking, these are the categories that most people agree upon:

- **White Hats** – Also known as '*ethical hackers*,' these hackers operate within the law. They stick to the hacker ethic, which states that a hacker should "do no harm." They also work as cyber security experts and are hired to detect potential vulnerabilities in a system or network, and fix them. This type of hacker works with software vendors to patch any vulnerability in their software. White Hats usually do what they do as a public service. Their intent is to make the public aware of the threats out there so that people know how vulnerable a system is. However, they never publicly publish such data until the vendor of the software has done so themselves.
- **Black Hats** – This type of hacker is often convinced that they are doing a public service, but in reality, their major motivation is power and money. They tend to penetrate networks so that they can steal or cause damage to data. They are driven by malicious hatred or anger against an organization or country. It is interesting to note that they got their name from the fact that villains in most cowboy Western movies wore black hats.
- **Gray Hats** – This term was originally introduced by a very famous

old-school hacking group who didn't want to be associated with Black Hats yet weren't keen on being branded as corporate security testers. Gray Hats can be described as hackers who used to be Black Hats but have reformed and are now working as cyber security experts. They are sometimes defined as hackers who consult as well as gain illegal access to networks.

Classes of hackers

There are specific classes that fall under the Black and White Hat hacker categories mentioned above. These include:

- **Elite** – These are the gurus of the hacking world. They have the skills and knowledge nobody else has. But what makes them extremely rare is their ethics and integrity. They often act as White Hats who know network infrastructure and have the programming knowledge to write their own tools. They aren't motivated by criminal intentions and are more intent on detecting coding problems or security flaws and informing system administrators. You can only become an elite hacker by performing a well-known hack or exploit or maintaining longevity as a hacker.
- **Cyber Terrorists** – This class of hacker goes beyond just crashing a network using a Denial of Service (DoS) attack. They thrive and love the fact that they can hide behind the veil of the web as they share information with each other. They are able to hide encrypted data in plain view such that only a fellow cyber criminal can find it. Governments all across the globe tend to hire these types of hackers to do their dirty business, ranging from simple spying to cyber warfare.
- **Script Kiddies** – Nobody is as maligned or ridiculed as a script kiddie. This class of hacker is young, inexperienced, and unskilled in creating their own exploit tools. They use tools made by elite hackers, and can only hack systems that others have identified vulnerabilities in. They mostly hack for fun and are the ones whose exploits are commonly mentioned in the media. Their main achievements are usually DoS attacks and web page defacements.

- **Hacktivist** – This is a combination of a hacker and an activist. They carry political, social, or religious agendas and can be quite tenacious. They deface websites and perform DoS attacks to put pressure on governments or organizations they consider are causing harm to a particular group of society.
- **Angry employees** – These are people who have inside knowledge about an organization and use their access to gather information for themselves or others. They are considered extremely dangerous even though the public rarely gets to hear about them. Such hackers are normally quiet and shy but have narcissistic personalities. They turn on their employers whenever they believe that they have not been recognized for their work.
- **Virus Writers** – These are people who take advantage of any weaknesses that a hacker has exposed, and go on to write code to exploit those vulnerabilities.

Skills Required for Hacking

As a beginner, there are some basic skills that you will need to develop if you are to progress in the world of hacking. These include:

1. **Computer skills** – You have to be knowledgeable in computer use and be able to understand written instructions. Browsing the internet aimlessly doesn't count. Can you use the Windows command module? These basic skills are critical for every hacker worth their salt.
2. **Working knowledge of Linux OS** – Linux allows you to customize your programs, which is why hackers prefer it over Mac and Windows.
3. **Database skills** – Learning how to use database management systems like Oracle and MySQL will help you understand how to penetrate databases.
4. **Networking skills** – As a hacker who will be engaging in a lot of online activity, you should know about concepts like subnetting, DNS, ports, WPS passwords, and so on.
5. **Scripting skills** – You may not know how to code right now, but sooner or later you will have to learn. Every hacker needs to have their own hacking tools rather than depend on what others have created. Relying on tools made by other hackers leaves your system vulnerable to exploitation. Take time to learn some scripting languages such as Ruby on Rails or Python.
6. **Reverse engineering skills** – One of the most effective ways to develop a great hacking tool is to take an existing one, take it apart, and find a way to make it better. Such skills are invaluable for a hacker.
7. **Use of virtualization software** – This type of software allows you to safely test your hack on your own computer before you unleash it on somebody else. A good example is VMWare Workstation.

What Motivates a Hacker?

It used to be that hacking operations were conducted by some college or high school teen hiding in their parent's basement. Nowadays, cyber attacks are more sophisticated and widespread. Yet despite the fact that cyber crime has advanced at an alarming rate with better technology, the motivations of today's hacker isn't much different from that of the previous generation.

So what drives a cyber criminal to hack a network or system? There are four fundamental motives:

1. **Money** – Financial gain is the biggest motivator of most of today's cyber attacks. You have heard of hackers exploiting system vulnerabilities of financial institutions and making off with credit card numbers, email accounts, passwords, usernames, and etc. A malicious hacker will sell anything they can find for a price. Some Black Hats even blackmail organizations using *ransomware*.
2. **Political/Ideological agenda** – This is where hacktivists fall under. They attack the networks of government institutions, organizations, and prominent personalities to further their ideological, political, social, or scientific agendas. One group known for having such motivations is *Anonymous*.
3. **Entertainment** – The majority of Gray Hats tend to exploit networks for fun or pride. They are seeking a challenge and will violate ethical laws to satisfy their curiosity. However, they are not malicious and will even inform the network administrator about the vulnerabilities they find.
4. **Cyber Security** – White Hats generally exploit a system to find weaknesses so that they can make them more secure. Organizations often employ hackers to work for them, patch vulnerabilities, and create codes of practice for employees to follow to avoid cyber breaches.

Chapter 2: Penetration Testing

Penetration testing refers to the testing of a cyber system, network, or application to detect weaknesses that may be exploited by a malicious hacker. You are essentially trying to gain access to a system without having any usernames or passwords. The aim is to see how easy it is to acquire confidential information about an organization, and then increase the security of the system being tested.

So what exactly is the difference between a penetration test and an attack? *Permission*!

A hacker who conducts a penetration test will be given the authorization by the owner of the system, who will then expect a detailed report at the end of it all. As the tester, you may be given user-level access to allow you to gain entry into the system. From there, you will be expected to see whether it's possible to gain access to confidential information that an ordinary user should never see.

The other option is to go in blind. In a blind or covert assessment, you are not given any information except the name of the client organization. The rest is up to you, which is exactly how most malicious hackers do it anyway. The only issue with a covert assessment is that it will take more time than an overt one, increasing the chances of you missing some flaw.

You may be hired to find just one weakness, but in most instances, you will be expected to keep searching to find all the potential vulnerabilities in a network. Once identified, you will have to find ways of fixing these holes. This is why you will have to write down detailed notes regarding your test procedure and results. Keeping notes enables the client to determine the effectiveness of your work and check to see if the issues you discovered are indeed fixed. However, it is highly unlikely that you will detect every single security flaw or hole in the system.

Detecting Vulnerabilities

The steps taken by a penetration tester and a malicious hacker are usually the same. In most cases, a malicious hacker will move slowly through a system in order to avoid being detected. You may also follow the same tactic to see just how effective a client's system is in detecting such attacks. Once this is done, these loopholes should be sealed.

The first step is usually reconnaissance. You attempt to collect as much information about your target network as you possibly can. This is normally a passive process that involves using resources available to the public. You can identify the organization's web servers, OS it is running, the software version, patches or modules the server has enabled, IP addresses, and in some cases, even the internal server name.

When you have gathered your information, it is then time to verify it. This can be achieved by comparing the network or system information gathered with known vulnerabilities. Once you test the vulnerabilities, you will know for sure whether the information you had gathered is accurate or not.

Reasons for Performing Penetration Testing

1. Identify weaknesses that malicious hackers may exploit

Even as you read this book right now, it is possible that there are malicious hackers launching tools and network attacks to try to penetrate your system. These attacks are never-ending and you cannot predict when a system will be hit. In most cases, these exploits are well known and thus preventable. The IT department of an organization may be keen on knowing where the weaknesses are within their network and how a malicious hacker may take advantage of them. As a penetration tester, you will be required to attack the system and fix the holes before someone with bad intentions finds their way in. A system may be secure today but tomorrow it may fall victim to a breach.

2. Justify to management the need for more resources

There are times when upper management just doesn't see the need to allocate more financial resources toward cyber security. In this case, penetration testing is the best way for the company's security team to justify their claims for more funds. The cyber security team may be aware of vulnerabilities but management is resistant to support changes being made to the existing system. By outsourcing the testing to an external consultant, management is more likely to respect the results obtained.

3. Confirm that the internal security team is doing its job

The penetration test report will show whether the cyber security department is efficient in its work. It may identify whether there is a gap between knowledge of system vulnerabilities and implementation of security measures.

4. Training for network staff

Imagine if a hacker were to gain access to an organization's system without the staff even knowing. By performing a penetration test, it is possible to discover just how vigilant your security is and whether the staff needs extra training. It also highlights the effectiveness of the countermeasures that have been put in place in case of a cyber attack.

5. Testing of new technology

Before launching a new piece of technology, for example, a new wireless infrastructure, it is critical that the system is tested for vulnerabilities. This will definitely save more money than performing the test while customers are already using it.

The Penetration Testing Report

Once you have completed the test, you have to compile all the data in a proper format and submit a report. Keep in mind that the majority of the management staff may not be technically oriented, so the has to be split into appropriate sections for easy reading. You should have an Executive Summary, a Technical Summary containing all the specific IT jargon, and a Management Summary that explains what needs to be done to fix the flaws detected.

Chapter 3: The Hacker's Methodology

Imagine a soldier going into a battlefield fully kitted in the latest and most advanced weaponry. They are full of confidence and know for certain that they are going to win. However, when the fighting starts, the soldier discovers that he walked into an ambush. He may take down most of the enemy troops, but because he was never prepared for the battle, he ends up losing.

This scenario isn't so far-fetched if you consider the number of so-called "hackers" who don't bother to prepare for their attacks. This is where a hacking methodology comes in handy.

A hacking methodology is what a hacker uses to guide them from the first step to the last. To effectively exploit any vulnerability in a system, you need to identify some key things that will help you achieve your objectives. Without a proper methodology, you are likely to end up wasting time and energy fighting a losing battle.

Target Mapping

Finding the perfect target for your attack is not as simple as it sounds. You have to be strategic in the way you conduct your research and search out the target with the most potential. You have to analyze their habits and then use the information collected to come up with the most appropriate strategy. The objective of mapping your target is to determine what and who you are attacking before penetrating the system.

Hackers usually go after one or several targets at once. Depending on the kind of information that you are looking for, you can decide to attack web servers storing personal information. You could also decide to go big and hack into a financial institution. Your target could be a specific website that you want to take down using DoS attacks, or you could deface its web page. You may be interested in a specific individual in an organization.

When you are searching for potential targets to attack, you have to consider the level of security that you will be trying to overcome. Most hackers only go after targets that they know are easy to beat, so the level of vulnerability is often a key factor in mapping your target.

Another factor to consider is whether the information gained from the attack is worth it. This will help determine how long you are willing to take trying to access the system.

So how do you go about gathering information about your intended target?

- **Conducting online searches**

You can Google the target's name and check out their Facebook or LinkedIn account. This may bring up their contact information. If your target is an organization, then you can search for job openings that the company has advertised for, specifically in the IT department. You may be surprised to learn just how much useful information is given out in a job advert, for example, the software that potential recruits need to be familiar with.

As a hacker, you need to know which keywords will bring up the most information. Use Google's *advanced search* feature to identify any websites that have backlinks into your target's site. If you want to access any files that may be within a company's website, then you will have to use a switch as

shown below:

site: www.abc.com keyword

Another technique to use is the Whois tool. Whois is a great way to perform a social engineering attack or scan a network. You can find the DNS servers of the target domain as well as the names and addresses of the people who registered the target domain.

Google Groups tends to store a lot of sensitive data about its users, for example, usernames, domain names, and IP addresses.

- **Web crawling**

Acquire what are known as "web crawling tools" to create a mirror image of the target website. Once you have done this, every file within the site that is publicly accessible will be downloaded onto your local hard drive. This will allow you to scan the mirror copy and find names and email addresses of employees, files, directories, the source code for its web pages, and much more information.

- **Websites**

By now you should be aware that there are certain websites that are a treasure trove of key information about individuals and organizations. Good examples include www.sec.gov/edgar.shtml, www.zabasearch.com, and www.finance.yahoo.com.

Scanning the Target Network

So far you have been collecting information that will allow you to see the entire target network as a whole. The hostnames, open ports, IP addresses and running applications should now be visible to you. Remember that if you are to perform an effective exploit, you must learn to think like a malicious hacker.

You can begin to use scanning software to find and record any hosts that are accessible online. Your own operating system should have its own standard ping tool. However, there are third party tools like SuperScan and NetScan Tools Pro that are able to ping the hostname of the domain or multiple IP addresses simultaneously.

Analyzing Open Ports

As a beginner, there are tools that you can use to check for the presence of open ports to penetrate the target network. Examples of some effective tools include SuperScan, Wireshark, and OmniPeek.

Exposing System Vulnerabilities

Assuming that you do find some vulnerability in your target's system, you can then start checking if these security gaps are exploitable. You can either go the manual route or use an automatic evaluation tool.

The manual method will require you to link to any of the open ports you uncovered earlier. Test these ports until you find a way in.

The automated method involves the use of tools such as *QualysGuard*, which is a cloud-based tool that is designed to scan open ports. Another tool that is available is Nexpose, which can scan a total of 32 hosts simultaneously.

Chapter 4: Gaining Physical Access

Picture this: A multi-million dollar corporation invests millions of dollars on technology-oriented cyber security countermeasures to protect its data. They have totally locked down their networks and system, and have conducted multiple penetration tests using elite hackers to keep out any malicious hackers who may have been hired by their competitors.

Now imagine that this company goes on to hire a security company that has lazy security guards. They never do any physical checks around the facility and even leave some doors open. Visitors are rarely scanned or asked to sign in. Even the computer rooms are normally left open.

Would you say this is a smart company that cares about protecting its data from hackers? Yes, they have plugged the electronic holes, but they have literally left the door wide open for hackers to physically breach their security!

You do not have to hack into a network remotely to gain access to data. You can gain physical access to a facility and perform your exploit from within. Over the last couple of decades, most companies have found it extremely difficult to maintain physical security. Thanks to advancements in technology, there are now more physical vulnerabilities that a hacker can take advantage of.

In today's world of USB drives, tablets, smartphones, and laptops, more and more data is being stored in smaller handheld devices. It is not that hard to get your hands on such devices, especially considering the fact that most employees take data with them when they leave work at the end of the day. Once you identify your target, you may not even have to enter the building; they will bring the data to you.

In this chapter, you are going to learn about how to take advantage of some of the physical security vulnerabilities in buildings that you have targeted. Once you have breached the on-site security and gained physical access, be prepared to penetrate the system from the inside.

Types of Physical Vulnerabilities

- Failure to establish a front desk to monitor visitors who enter and exit the building.
- Failure to enforce mandatory signing-in of all employees and visitors.
- Aloof employees and security staff who aren't fully familiar with the IT repairmen, vendors, or suppliers.
- Tossing sensitive corporate and personal documents into the trash instead of shredding them.
- Failure to lock doors leading to computer rooms.
- Leaving digital devices lying around the offices.
- Failure to fix doors that can't shut properly.

Creating your Plan

One of the first things you will have to do is to come up with a way of breaching physical security. This will require some extensive reconnaissance work on your part. You must identify the kind of security measures that the facility has put in place, the weaknesses and vulnerabilities present, and how to take advantage of them.

This may seem simple on paper but it is not that easy once you get on the ground. The assumption here is that you are working without an inside man to feed you the vital security information. It may be a couple of weeks before you are able to collect all the information you need to launch your attack. A physical security breach means you must have the right skills and knowledge to not only enter the building, but also to maneuver your way inside, and then exit without being detected.

If you lack the patience, physical fitness, and mental agility necessary for such a task, then do not attempt a physical breach. Stick to performing your attacks from a remote location.

There are a number of physical security factors you will have to consider when planning how to gain access to your target. These are categorized into two distinct classes: Physical Controls and Technical Controls.

Physical controls

You will have to consider how the security team controls, monitors, and manages access into and out of the facility. In some cases, the building may be divided into public, private, and restricted sections. You will have to determine the best technique to enter the section that contains the target.

1. Perimeter Security

How do you plan on circumventing the perimeter security? You will need to know whether the facility has a wall, fence, dogs, surveillance cameras, turnstiles, mantraps, and other types of perimeter security. These are just the deterrents that you may have to deal with on the outside. A well-guarded

facility will have secondary security layers as you get closer to the building.

At this point, you should know where the weaknesses are in the design of the facility. If there is a high wall that has big trees all around it, you can climb up the branches and jump into the compound. Of course, you will have to be physically agile and fit enough to do this.

Learn the location of the security lights and where the dark spots or shadows fall. These can provide great hiding spots if you plan on gaining access at night. You should also consider dumpster diving as a way to gain access to sensitive data. Check the location of the dumpsters and whether they are easily accessible. It would be a good idea to know when the garbage is collected so that you can fake being part of the garbage crew.

2. ID Badges

Organizations use ID badges and user IDs to monitor and control the movement of employees. They are also used to track the files and directories that an employee creates or modifies. Getting your hands on an ID badge may require you to steal one from a legitimate employee, or making your own fake badge. If you can't get an ID badge, then your other options would be:

- Enter as a visitor and evade your escort.
- Use the tailgating technique, assuming the building doesn't have a mantrap.
- Befriend an employee in the smoking area and follow them in as you continue your conversation.
- Get a fake uniform and impersonate a contractor, salesperson, or repairman. If you want to go all-in, then consider acquiring a service truck and equipment to make you appear more legit.

3. Intrusion Detection Systems

These generally include motion detectors and intrusion alarms.

You will have to know the types of motion detectors you are dealing with. Are they infrared, heat-based, wave pattern, capacitance, photoelectric, or passive audio motion detectors? Each of these works differently and understanding its strengths and weaknesses will help you in your mission.

You will also need to know the type of alarms inside the building. The facility may have sensors on the doors and windows, glass break detectors, water sensors, and so on. While some alarms are meant to silently notify security of a potential breach, others are designed to deter or repel the attacker. A deterrent alarm will close doors and activate locks to seal everything and everyone in. A repellant alarm will make loud noises and emit bright lights to try and force an attacker out of the building.

Technical controls

This is usually focused on controlling access because it is the most vulnerable area of physical security. Technical controls include smart cards and CCTV cameras.

1. Smart Cards

These have microchips and integrated circuits that process data and enable a two-factor authentication. Smart cards contain employee information and the areas of the facility they are authorized/not authorized to access. Having the card alone will not get you access to a facility. A biometric scanner and PIN/Password must also be used for authentication. However, smart cards have certain vulnerabilities.

One method of bypassing smart cards is through *fault generation*. This is where you reverse-engineer the encryption in order to find the encryption key and access the stored data. This involves inputting computational errors by altering the clock rate and input voltage or changing the temperature fluctuations.

You could also use a side-channel attack to figure out how the card works without damaging it. This involves exposing the card to different conditions through electromagnetic analysis, differential power analysis, and timing.

Another way is to use software to perform a noninvasive attack. This involves hacking the software and loading commands that enable you to extract account data. Finally, there is a method known as *micro-probing*. This is an intrusive attack that involves connecting probes directly to the chip. The goal here is to take the chip out and reset it.

2. CCTV Cameras

The standard of video surveillance is CCTV cameras. They are located at strategic places and are monitored by security guards sitting in a control room. However, there are always blind spots to be exploited, so you need to know where these are. The cameras can be wireless or web-based, which means you can either hack the camera feed and manipulate the images being shown on screen or jam the signal.

Physical security is a critical part of cyber security. Hackers will always look for any weakness that they can find, whether online or offline.

Chapter 5: Social Engineering

Did you know that in the year 2016, the top three cyber-threat concerns were social engineering, insider threats, and advanced persistent threats? This shows you just how rampant social engineering attacks have become in cyber security.

Why do you think social engineering is number one on that list? A hacker is supposed to attack the system or network, so why would they focus on another aspect of an organization's security system?

The answer lies in the people. The biggest weakness of every element of security is the people involved. We saw in the last chapter how the most advanced technology cannot protect you against cyber attacks if the people guarding the building are sleeping on the job. Through social engineering, you can hack the people by gaining their trust and exploiting them for the information you need. However, you will require a certain degree of boldness and skill to get people to trust you, considering that you are a total stranger.

One aspect of social engineering is that it is usually done together with a physical security hack. The aim is to make contact with someone who has specific information that can help you gain access to the files or resources of your intended target.

For example:

- Send the target an email that contains links. When they click the link, malware or a virus is downloaded onto their computer, thus allowing you to control the system and acquire data.
- If you are an employee in a company and want to gain unauthorized access to confidential data, you could inform the security department that you have lost your access badge. They will give you the keys to enter the room thus allowing you to get to the physical and digital files you want.
- You could impersonate a genuine product vendor and claim that your

company needs to update or install a patch on the client's software (e.g. accounting software). You could then request to be given the administrator password. Alternatively, you could just ask them to download the fake software, which would then give you remote access to the target's network.

These examples may seem too simple or easy, but remember that social engineering is the most used tactic by hackers to breach cyber security. By learning how malicious hackers commit their exploits, you are better placed to prevent your own system, or others, from getting hacked.

Social Engineering Strategies

Let's look in depth at some of the strategies that hackers use when performing a social engineering attack.

1. Gaining Trust

One of the best ways to build trust for a social engineering hack is through words and actions. You have to be articulate, sharp, and be a good conversationalist. There are instances when a social engineer fails in their mission because they were careless in their talk or acted nervously. This often happens when the hacker displays the following signs:

- Talking too much or showing too much enthusiasm
- Acting nervously in response to questions
- Asking odd questions
- Appearing to be in a hurry
- Having information only reserved for insiders
- Talking about people in upper management within the organization
- Pretending like they have authority within the company

As long as you practice good social engineering skills and techniques, you will be able to conceal these signs.

One extremely effective tactic to use to gain someone's trust is to go out of your way to do someone a favor and then immediately ask for one in return. Another tactic is something that you've probably seen in a movie. You set someone up by creating a particular problem for them. When the victim cries out for help, you dash to the scene and save them. This works to create a bond between you and the potential target.

A fake work ID and uniform can sometimes help you impersonate an employee in a company, thus allowing you to enter the facility undetected. People will even give you passwords and other sensitive information as long as you appear to be one of them.

2. Phishing

Hackers who use social engineering attacks are able to exploit their targets using technology since it's easier and more entertaining. People can be very naïve especially when they are online. It is simply amazing how trusting people are in this day and age of increasing cyber attacks.

Phishing involves sending the target emails that appear to be from a legitimate or trusted source. The aim is to get them to share sensitive or personal information either by sending it directly or clicking on links.

The email will look like the real deal to the intended target but that is because you will have spoofed the IP address to display an email address that appears genuine. You can pretend to be a close friend, relative, or colleague and request them to send you their personal information.

You can also pretend to be a financial institution and ask them to click the link in order to update their account information. When they do so, they will be directed to a fake website that mirrors the real one. As they log in, you can gain access to their usernames, user IDs, passwords, bank account number, or social security number.

Spamming is another tactic you can perform. You just send them a ton of emails and wait for them to become curious and open at least one of them. The email will contain a request to download a free gift (ebook, video, coupon, etc.) in exchange for some personal information.

One of the most common tricks is to claim to be a verified software vendor. All you have to do is send the target a software patch via email and ask them to download it for free. What they don't realize is that the software is actually a Trojan horse or backdoor that allows you to have complete control of their system.

Phishing scams work so well because they are very difficult to trace back to the hacker. The tools that social engineers use, for example, remailers and proxy servers, provide adequate anonymity to keep them from being found out.

How to Prevent a Social Engineering Hack

As a budding hacker, you are probably more interested in learning how to perform an attack rather than preventing it. However, as we said in the beginning, hacking can work both for good and for bad. It is important, therefore, that you understand how an attack can be prevented so that you can advise a client accordingly. This information will also help you perform more effective exploits. After all, there's no need to waste time and energy attacking the target using a technique that they have already protected against.

Organizations will generally use two techniques to prevent social engineers from exploiting their vulnerabilities:

1. **Developing and enforcing strict policies** – The organization can create hierarchies of information, where users are permitted to access some but not all data. There should also be strict enforcement of wearing ID badges by all employees and consultants, and every guest must be escorted by security. When fired employees, contractors, or suppliers leave the premises, they should be stripped of their IDs. The same password should also not be used for more than a set duration. Finally, in the event that a breach or suspicious behavior is detected, there must be a quick response by the security personnel. The most important aspect of any organizational policy is observance. The people involved must understand the requirements and follow them at all times.
2. **Training the users in security awareness** – Most employees simply do not know what to do when they are faced with a social engineering attack. There has to be some kind of user awareness and training in order to teach people how to identify and respond to hackers. This training should be continuous rather than a one-time event. The training program should be easy enough for those who are not technically-minded to understand. It is also important for upper managers to lead by example and undertake the training too.

Since social engineering attacks aren't just targeted at organizations, we need to examine how individuals can protect themselves. Some of the ways of preventing this kind of attack include:

1. Avoid giving out passwords to random people.
2. Avoid sending your personal information via email or social media without verifying the identity of the receiver. Make sure that you know who is sending you a friend or connection request on Facebook, LinkedIn, or Twitter.
3. Avoid downloading attachments from unidentified IP addresses, or clicking on links in spam mail.
4. Avoid the tendency to hover your cursor over an email link. Hackers are able to embed malware in a link and trigger a download the moment the mouse moves over it. Anti-malware is a good way to prevent this type of hack.

The truth is that while social engineering can be a bit complicated to pull off, preventing it is also very difficult. An organization cannot control all the people linked to it at all times, and as individuals, everyone has their own unique weakness. It is your job to find it and exploit it.

Chapter 6: Hacking Passwords

One of the most common ways to ensure the safety of your data is to password-protect it. We have become so used to putting passwords in all our digital devices that we actually believe that this measure is enough to keep our information safe.

However, the truth is very different. Passwords do a good job of keeping unauthorized users out of a system but as we all know, malicious hackers have been having a field day cracking passwords. In most cases, a user may not even realize that someone else is also privy to their password. Passwords may make people feel safe, but there are a number of vulnerabilities within them that a hacker can easily exploit.

Types of Password Vulnerabilities

There are generally two types of password vulnerabilities: *User* and *Technical*.

User vulnerabilities

User vulnerabilities are those weaknesses that result from lack of proper password policies or weak enforcement of such guidelines. For example, how many times have you seen someone use the same password for their laptop, smartphone, tablet, and all their digital devices? Imagine someone using the same password for their Yahoo, Gmail, LinkedIn, Facebook, and Twitter accounts! There is no need to imagine because this is exactly what most people do!

The majority of people simply find it too difficult to memorize every single password. We live in a world of convenience, so most people just look for the fastest and easiest ways to get things done. This usually results in people repeating the same password for all their accounts. Unfortunately, this has simply made the job of hackers that much easier.

With all the letters and numbers available for use, there are potentially three trillion password combinations, eight characters long. Yet you would be surprised at the number of people who choose weak and silly passwords just to make cramming them easier. Some even don't bother with passwords and skip the process altogether!

So what are some of the user vulnerabilities that a hacker can take advantage of?

- Passwords that are never changed. When was the last time you changed your Twitter or email password? Why go through the hassle, right?
- The same password being used in several different accounts across different networks and systems.
- Passwords that are too simple and are linked to your name, location, school, job, and so on. Most users just look around the room when asked to create a password. Whatever they see is what they will use.

This may sound funny but it’s true.

- Passwords that are long and complex are usually written on pieces of paper or stored in a file. As long as the location of the file is unsecured, it can get stolen.

Technical vulnerabilities

Exploiting user vulnerabilities is usually the first step for a hacker. After that, you try to see whether there are any technical weaknesses you can take advantage of. The most common ones include:

- Failure to utilize applications that hide the password as it is being typed on the screen. Though most applications immediately hide the characters being typed on the screen, some do not. If a user doesn’t set up the settings appropriately, they leave themselves vulnerable to *shoulder surfers* (this is explained later on).
- Using programs or databases to store all your passwords, but failing to secure the database appropriately. Some users store all their passwords in one MS Word, Access, or Excel file but fail to secure the document itself.
- Use of unencrypted databases that can be accessed by large numbers of unauthorized people. This is often the case with organizations.
- Use of weak encryption techniques by software vendors and developers. The majority of developers tend to have too much faith in the fact that their source codes are unknown. What they don’t realize is that with enough time and patience, any experienced hacker can crack a source code. A hacker who has enough computing power can even use tools that are designed to hack weak encryptions.

Understanding Password Encryption

A password is said to be encrypted when it is stored in a system using an encryption or one-way hash algorithm. Once the password is hashed, all a user sees is a fixed-length encrypted string. The basic assumption is that once a password has been hashed, then it cannot be cracked. LINUX even goes further and adds a random value (a salt) to the hashed password, just to make it more secure. The salt is what makes it possible for two people to use the exact same password yet generate totally different hashing values.

There are a number of tools that can be used by hackers to crack passwords. These tools work by taking several well-known passwords, running them through a hashing algorithm, and then generating encrypted hashes. Once the encrypted hashes have been generated, the tool compares them to the password that needs to be cracked. Of course, this process occurs at a very fast speed, and the password is cracked the moment the original hash and the encrypted hash match.

At times a hacker may find a password that is very complex and strong. Such passwords are quite difficult to crack, but with the right tools, enough time, and adequate patience, all passwords can be hacked. If you want to make sure that your system is safe from malicious hackers, you need to get the same tools that they use, search your system for vulnerabilities, and fix them.

Password-Cracking Tools

There are a lot of advanced tools in the market right now for cracking passwords. Some are more popular than others due to their effectiveness across diverse systems and operating software. For example:

- **Ophcrack** – This tool is used for cracking passwords in Windows applications.
- **Cain and Abel** – This is one of the most effective tools. It can be used for cracking hashes, VNC and Windows passwords, and many other applications.
- **John the Ripper** – This is definitely one of the most well-known and loved programs for cracking passwords. It combines a dictionary style of attack before launching a complete brute force attack. It is used for cracking LINUX and hashed Windows passwords.
- **Brutus** – This tool works well for cracking logins for HTTP, FTP, and etc.
- **Elcomsoft Distributed Password Recovery** – This tool works extremely fast by incorporating a GPU video acceleration program and using thousands of networked computers simultaneously. It is able to crack Windows, Adobe, iTunes, and other applications.
- **Elcomsoft System Recovery** – This tool uses a bootable CD to reset the administrative rights on a Windows system.

There are many other tools that you can use to hack passwords on a variety of applications, systems, and networks. The most important thing is to understand how encryption works and how these tools can be used to overcome the encryption.

Techniques for Cracking Passwords

We have all tried at some point to crack a password. It could have been the home computer, in the school lab, or maybe a friend's device. It is likely that you used a conventional method rather than an advanced one. The techniques below are a combination of some old-school approaches and some high-tech methods.

1. **Guessing** – This is probably one of the most overused techniques. It is also the simplest approach since most users tend to pick passwords that they will remember easily. All you need to do is use logic to guess what may have been used to create their password. This technique works best when you are familiar with the target or have easy access to their personal data. The password is often the user's or a family member's name, their ID, their birthday, or even their favorite animal.
2. **Shoulder surfing** – This is where you hand around a person as they key in their password. You can either watch the characters on the screen or memorize their keystrokes. It is important that you blend in to avoid detection, and be discreet about your moves. If you want to get passwords from people in a public location such as a café, you can place a camera in a strategic place to monitor their login keystrokes.
3. **Social engineering** – What if you could get a password by simply requesting for it? The vast majority of people tend to believe what they are told especially if it is in an official setting. You can literally get access to employee records from anywhere these days, thanks to social media and company websites. A hacker can impersonate a staff member from the IT department of a company, call a user, and inform them of some technical hitches within the email system. The hacker then requests that the user gives them their password so as to sort out the glitch.
4. **Dictionary attacks** – This is where a program is used to create a list of plain-text dictionary words that can be compared to the actual password. It involves hashing plain-text words, salting them, and then comparing them to the user's password. The word that matches is then

considered to be the user's password. Programs that can help you launch a dictionary attack include *John the Ripper, LophtCrack,* and *Cain and Abel*.

5. **Brute force attacks** – This should never be your first choice when it comes to cracking a password. It is an inefficient and extremely time-consuming technique. It is considered a fall-back option that is used when all other methods have failed. It is primarily used to crack passwords that are 6 characters or less, which is why you are always advised to make your passwords 8 characters or more. The more characters a user puts into their password, the harder it is to crack using a brute-force attack. However, a brute force attack is very exhaustive, which means that sooner or later the password will be cracked. Unfortunately, nobody can predict when this will happen. Programs that use this technique include *John the Ripper, Rarcrack,* and *Oracle*.

The above methods are the simplest and most commonly used ways to crack passwords. There are other approaches that are available, for example, password probability matrix and rainbow tables. However, for a beginner, these would be simply too complex to cover here.

Using John the Ripper and pwddump3 to crack a password

The pwdump3 tool is an effective way to extract hashed passwords from a Security Accounts Manager database. John the Ripper, as stated earlier, can work on both LINUX and Windows passwords. This procedure requires that you have administrative access.

If you are trying to crack a Windows system, follow this procedure:

1. On the computer, go to drive C. Create a directory and call it "passwords."
2. Make sure that you have a decompression tool (such as WinZip) installed on the computer. If it isn't, then download and install it.
3. Download pwdump3 and John the Ripper and install them immediately. Extract them into the directory you created above.

4. Type the command

   c : passwordspwdump3 > cracked.txt

   The output of this step will be Windows Security Accounts Manager password hashes, which will then be captured in the .txt file.

5. Type the command

   c: passwordsjohn craked.txt

This will run John the Ripper against the password hashes, and the output will be the cracked user passwords. However, this process may take a very long time, depending on how complex the passwords are and the number of users in the system.

If you are cracking a LINUX system, use the following procedure:

1. Download the source files for LINUX.
2. Type the command

   [root@local host yourcurrentfilename] #tar – zxf john – 1.7.9.tar.gz

   This will extract the program and create a /src directory.

3. In the /src directory, type the command

   Make generic

4. In the /run directory, type the command

   . /unshadow /etc/passwd /etc/shadow > cracked.txt

   The unshadow program will be used to merge shadow files and passwords and input them into the .txt file.

5. Type the command:

   . / john cracked.txt

   This will launch the cracking process, which may also take quite some time. The output should be the same as that for the Windows procedure.

Creating Secure Passwords

When it comes to strengthening the security of data within an organization, it becomes necessary to hire a White Hat to help design better password policies. The aim is to teach the system users how to create more secure passwords as well as the effects of poor password security. For individuals who want to secure their personal information, the same techniques can also apply in most cases.

The criteria to be followed include:

- Forming passwords that combine upper and lowercase letters, numbers, symbols, and special characters.
- Adding punctuation marks in-between separate words
- Deliberately misspelling words
- Changing words every six to 12 months. In the event of a security breach, all passwords are to be changed.
- Ensuring that passwords are of different lengths to make cracking more difficult.
- Storing all passwords in a password manager program rather than an unsecured MS Excel, Access, or Word file.
- Avoiding the tendency to recycle old passwords.
- Ensuring that passwords are not shared at all, not even with friends or work colleagues.
- Locking the system BIOS using a password
- Establishing more advanced authentication methods, for example, digital certificates or smart cards.

In order to hack a password, you have to understand what a strong or weak password looks like. Having the right knowledge of how to create a strong password will help you become a more effective hacker.

Chapter 7: Wireless Network Attacks

Wireless networks have become so commonplace these days, but unfortunately, they are also very vulnerable to hacking threats. This is due to the fact that they involve the transmission of data through radio frequencies, thus making information vulnerable to interception. In cases where the encryption algorithm is weak or transmitted data is unencrypted, the situation becomes much worse.

WLAN Attacks

There are a number of ways that a wireless network attack can be launched. These include:

1. **Unintentional association**

There are instances where one wireless network overlaps with another, allowing a user to unintentionally jump from one into the other. If a malicious hacker takes advantage of this, they could acquire information contained in a network that they never intended to be on in the first place.

2. **Non-conventional networks**

These are networks that do not have the proper security that is usually reserved for laptops and access points. They tend to be soft targets for hackers. They include wireless printers, barcode readers, Bluetooth devices, and handheld PDAs.

3. **Denial of Service attacks**

This type of attack involves sending hundreds or thousands of messages, commands, or requests to one access point. In the end, the network is forced to crash, or users are prevented from accessing the network.

4. **Man-in-the-middle attacks**

This attack involves a hacker using their laptop to act as a soft access point and then luring users to it. The hacker connects their soft access point to the real access point through a different wireless card. Users who attempt to reach the genuine access point are thus forced to go through the soft access point. This allows the hacker to grab whatever information is being

transmitted in the network. Man-in-the-middle attacks are usually performed in public areas that have wireless hotspots.

5. MAC spoofing

This can best be described as theft of the identity of a computer that has network privileges. A hacker attempts to steal the MAC (Media Access Control) address of an authorized computer by running software that “sniffs” it out. Once the hacker finds these administrative computers and their IDs, they use other software that enables them to use these MAC addresses.

Verification of Wireless Networks

The majority of wireless networks are secured by passwords in order to control how users access and use the network. Two ways of authenticating a wireless network are *Wired Equivalent Privacy (WEP)* and *Wi-Fi Protected Access (WAP).*

Wired Equivalent Privacy (WEP)

WEP offers as much privacy as a wired network and encrypts all data transmitted over a network. However, due to its numerous vulnerabilities, it has largely been replaced by WPA.

Cracking a WEP network can be done either actively or passively. Active cracking is more effective, causes an overload of the network, and is thus easier to detect. Passive cracking, on the other hand, does not affect traffic load until after the network has been cracked.

The tools that you can use to crack a WEP network include:

- **WEPCrack** – This is an open-source tool that you can download from wepcrack.sourceforge.net.
- **Aircrack** – This tool enables you to sniff a network, and can be downloaded from aircrack-ng.org
- **WebDecrypt** – This tool utilizes a dictionary attack to generate WEP keys. It can be downloaded from wepdecrypt.sourceforge.net
- **Kismet** – This is a tool that can be used for many different purposes, such as sniffing network packets, detect visible and invisible networks, and also identify intruders.

Wi-Fi Protected Access (WAP)

This authentication was designed to overcome the weaknesses of WEP. It depends on passphrases and encryption of packets using temporal keys. One weakness of WAP is that it is vulnerable to dictionary attacks if weak passphrases are used. The tools for cracking WPA include:

- **Cain and Abel** – This tool decodes files sniffed out by other programs
- **CowPatty** – This tool uses brute force tactics to crack pre-shared keys

How to Carry Out MAC Spoofing Attacks

One of the most popular ways of preventing a MAC spoofing attack is to use MAC filtering. A MAC filter is used to block unauthorized MAC addresses from joining a wireless network, even if the user has the password. However, it is not an effective way to lock out a determined hacker.

In the example below, you will learn how to spoof the MAC address of a user who has the authorization to connect to a network. Make sure that your Wi-Fi adapter is in monitoring mode. The tools that will be used are *Airodump-ng* and *Macchanger*.

1. With your adapter in monitoring mode, type the command

   Airodump-ng–c [channel]-bssid [target router MAC Addres]-I wlan0mon

This will enable you to detect the target wireless network. All users who are using the network will be displayed in a popup window, including their authorized MAC addresses.

2. Choose one of these MAC addresses to use as your own address. However, you must first switch off your monitoring interface. Type the command

   Airmon-ng stop walnomon

3. You then have to switch off the wireless interface of the MAC address you have chosen. Type the command

   Ifconfig wlano down

4. Now it is time to run the Mcchanger software. Type the command

   Macchanger –m [New MAC Address] wlan0

5. Switch on the wireless interface of the MAC address you had chosen. Type the command

Ifconfig wlano up

You have now successfully changed your MAC address to that of an authorized user. Log in to the wireless network and see if you are able to connect to it.

How to Secure a Wireless Network

There are a number of approaches that you can use to secure a wireless network. Every ethical hacker should know these tips so that they can prevent malicious hackers from exploiting system vulnerabilities. These include:

- Install firewalls, anti-virus, and anti-spyware. Make sure that all your security software is updated and the firewall is turned on.
- Encrypt your base stations, routers, and access points by scrambling your network communications. These devices are manufactured with encryption switches, though they are but are usually switched off. Ensure that you switch on the encryption feature.
- Change the default password of the wireless router. Ensure that they are long and complex.
- Switch off the network whenever it is not being used.
- Turn off the router's ID broadcaster, which is how the device broadcasts its presence. This is unnecessary since genuine users already know that it exists.

Chapter 8: Hacking a Smartphone

This chapter will cover the procedure that you can follow to hack an Android Smartphone. You will have to download some specialized software from legitimate third parties in order to make the process easier and faster.

This procedure is totally anonymous and you will be able to gain access to all the data in the target's phone. It is a remote exploit that is performed over a secure internet connection.

Steps to Follow:

1. Go to the MasterLocate website (*MasterLocate.com*) to use the online app. You do not have to download the software onto your computer or phone to use it. The tool will enable you to track the real-time GPS location of the target, monitor their SMS and WhatsApp messages, listen to their calls, and keep track of their Facebook account.
2. Run the MasterLocate app on your phone or computer.
3. A dialog box should pop up with the field *Victim's Mobile Number*. Enter the number of the target here. Ensure that the target's phone is online when you are doing this step.
4. In the same dialog box, right underneath the *Victim's Mobile Number* field, there is the *Verify* tab. When you click on it, the program will attempt to establish a connection. Wait for the target's country to come up.
5. Once the connection is established and verified, go to the right side of the dialog box. Browse through the *Reports* section to view the target's messages, call logs and files. If you wish to download anything onto your device, just click on *Export Method*. This will present you with options for download formats, such as .zip and .rar.

This method of hacking Smartphones is simple and straightforward. All you need to do is ensure that both you and the target are online throughout the

entire hacking process. Any interruption to the internet connection will stop the process. Another thing is that you must know the victim's phone number as well as their mobile number country code.

Smartphone Hacking Countermeasures

As long as a phone is connected to unsecured Wi-Fi or contains compromised malware, it is vulnerable to exploitation by hackers. So what are some of the measures that can be taken to secure a Smartphone from malicious hackers?

1. Ensure that your phone is running a reliable, trusted, and updated antivirus.
2. Only connect to secure Wi-Fi when browsing the internet, especially in public places. Such places are a hacker's best hunting ground for stealing data from unsuspecting victims. Public Wi-Fi should not be used for activities that require entering your bank account details, for example, shopping or banking.
3. Avoid the tendency to download apps that ask for access to your personal information.
4. Make sure that all firmware is constantly updated, either automatically or manually.
5. If you have any doubts about the source of a piece of software, leave it alone. Only buy or download from verified app stores. Check out what the reviews are saying to better understand what others who have used it are saying.
6. Lock your phone every time that it is not in use. Ensure that your password is strong and change it regularly.
7. If you receive text messages containing links, don't click on the link, especially if you do not know the sender. It is best to delete such spam messages as soon as they come into your phone. Hackers tend to send out texts to thousands of phone users claiming to be from legitimate companies or websites. When the link is clicked, malware is installed onto the phone, thus allowing data to be accessed.

There are billions of mobile phones all over the world, and this is one area of hacking that provides the fastest and easiest way to attack a target. Most people tend to be wary when they are on their computers but somehow drop their guard when browsing on their phones. It is, therefore, extremely crucial

that people remain vigilant at all times.

Chapter 9: Hacking Tips for Beginner's

You bought this book because you wanted to learn some of the fundamental skills and techniques for hacking. Wouldn't it be a shame if you ended up getting busted, or worse still, hacked by a fellow hacker with more experience?

It is very important that you make sure that you take extreme care when starting out. Yes, it is a lot of fun when you first start to see the results of your work, but you need to understand how to maneuver and remain undetected.

Here are five key tips that every beginner should follow:

1. Avoid the trap of buying hacking software from random websites. There are thousands of scammers who pretend to have software and tools that are "guaranteed" to work, but these are usually set up to lure rookie hackers. You will lose your money in exchange for useless software. You may even have your own personal data stolen as well. Make sure that you only deal with legitimate or verified websites. Do your research well and find out what other hackers are using and where they are getting them from.
2. Avoid the temptation to download freeware of the internet. These mostly include keyloggers and Trojan horses. If you are serious about hacking then you need to be prepared to spend some cash to get stuff that works. The best and most effective software is not free. Being a cheapskate and going for the freebies will expose you to malicious scam hackers who won't hesitate to exploit your system.
3. When buying hacking tools, try to use bitcoins. There are some tools that you don't want to be traced back to you, for example, virtual private servers, anonymous VPS, and domain registration servers. If you use your personal credit card, you may expose yourself in more ways than one, and a quick check of your account will reveal your hacking activities. The best move is to always keep your real identity

separate from your online activities.

4. Learn to develop your skills. If you are skilled in web development alone, then you will have to learn some programming. If you are a programmer, then learn script writing. The goal is to know something about everything rather than getting comfortable being in a box.
5. It is OK in the beginning to use other people's software to launch your attacks. However, every hacker worth his salt sooner or later learns how to write his own codes, programs, and scripts. If you can create your own hacking tools, then you will have moved on to the next level and onwards toward being an elite hacker.

Conclusion

We have come to the end of a long journey through the world of hacking. If you didn't know anything about the subject, then you should have enough knowledge now to start performing small exploits.

There is a lot of potential in hacking, and it is not all malicious. Learning how to hack effectively is the best way to stay safe in a world where checking your email is dangerous, and talking to that cute stranger may lead to more than what you were expecting (and not in a good way)!

Whether it is a mobile device or a desktop computer, total vigilance must be maintained. The malicious hackers are always on the prowl, so you have to learn their tricks and counter them. As an ethical hacking guide, this book has shown you the first steps to hacking as well as protecting yourself.

Keep learning and applying what you have learned here. Remember to stay safe at all times, and don't get in over your head.

Good luck!

Resources

www.csoonline.com

www.giac.org

www.whitehatsec.com

www.sans.org

www.2-spyware.com