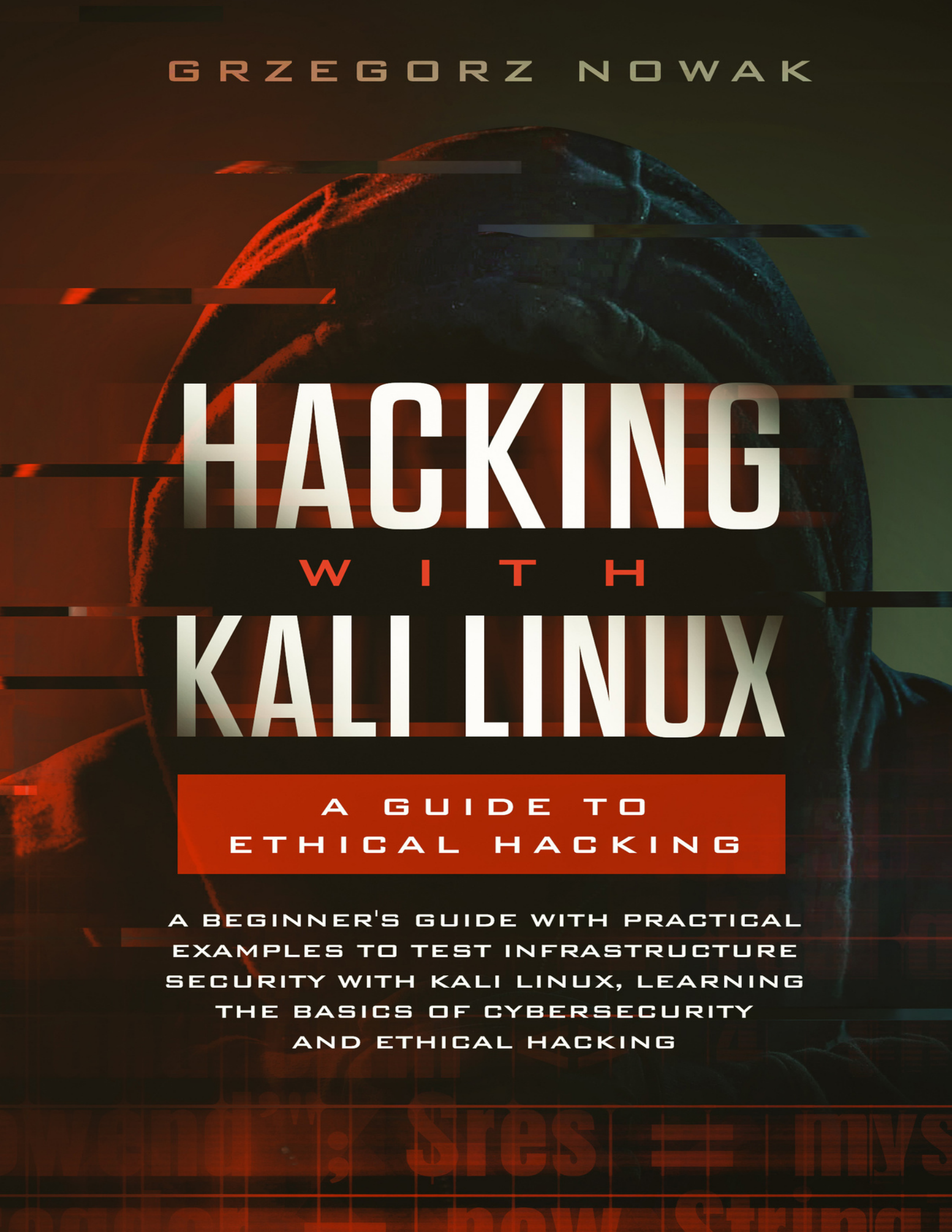
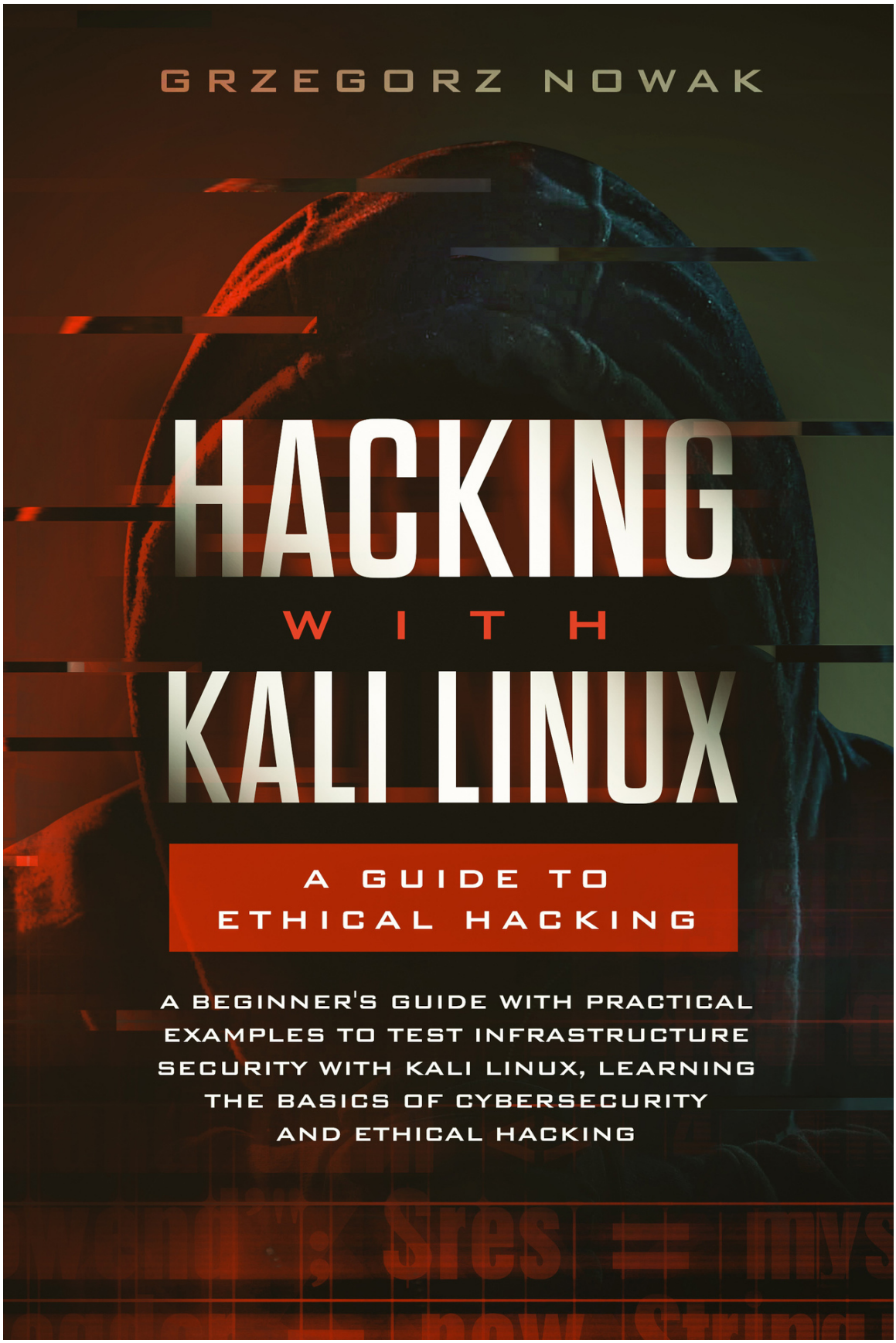
GRZEGORZ NOWAK



HACKING WITH KALI LINUX

A GUIDE TO ETHICAL HACKING

A BEGINNER'S GUIDE WITH PRACTICAL EXAMPLES TO TEST INFRASTRUCTURE SECURITY WITH KALI LINUX, LEARNING THE BASICS OF CYBERSECURITY AND ETHICAL HACKING


GRZEGORZ NOWAK
HACKING
WITH
KALI LINUX
A GUIDE TO
ETHICAL HACKING
A BEGINNER'S GUIDE WITH PRACTICAL
EXAMPLES TO TEST INFRASTRUCTURE
SECURITY WITH KALI LINUX, LEARNING
THE BASICS OF CYBERSECURITY
AND ETHICAL HACKING

Download the Audio Book Version of This Book for FREE

If you love listening to audio books on-the-go, I have great news for you. You can download the audio book version of this book for **FREE** just by signing up for a **FREE** 30-day audible trial! See below for more details!

Audible Trial Benefits

As an audible customer, you will receive the below benefits with your 30-day free trial:

- FREE audible book copy of this book
- After the trial, you will get 1 credit each month to use on any audiobook
- Your credits automatically roll over to the next month if you don't use them
- Choose from Audible's 200,000 + titles
- Listen anywhere with the Audible app across multiple devices
- Make easy, no-hassle exchanges of any audiobook you don't love
- Keep your audiobooks forever, even if you cancel your membership
- And much more

Click the links below to get started!

For Audible US

For Audible UK

For Audible FR

For Audible DE

Hacking with Kali Linux:
A Guide to Ethical Hacking

A Beginner's Guide with Practical Examples to Learn the Basics of Cybersecurity and Ethical Hacking, Testing Infrastructure Security with Kali Linux

Grzegorz Nowak

Table of Contents

Introduction

The following chapters will discuss the different aspects that come with hacking on the Kali Linux operating system. This is one of the best operating systems to use when you want to begin learning how to hack and how to keep your own network safe. It ensures that you have all of the tools that you need to get started, and as we will explore in this guidebook, it is set up so that we can dual boot with other operating systems, making it easy to work on any computer that you would like.

This guidebook is going to take some time to look closer at hacking with Kali Linux, and all of the different parts that go with it. We will start out with some of the basics of hacking, such as the most common types of hackers and the differences between a black hat, white hat, and gray hat hackers. From there, we will move on to some of the hacks of the hacking process, including the steps that a hacker would take to help them learn more about a network and find their way onto that network through vulnerabilities without being detected.

We will then move on to some of the steps that are needed to work with installing this Kali Linux operating system on our system. We will look at how to dual boot it on a Windows computer and the different steps that we need to take to ensure this operating system is ready to go and can take on all of our hacking duties. From there, we can move on to looking at an introduction to cybersecurity and why this is so important for us to understand in order to keep our own networks safe.

Now that we have some of that introduction out of the way, it is time to dive into some of the different types of hacks and how we can prevent them from our own network. We will take a look at the malware attacks, cyberattacks, and how to scan our own networks and servers to get the best results in the process. Remember that the techniques that we use in this guidebook in ethical hacking are the same ones that a black hat hacker or malicious hacker would use, but this is a great way to make sure that we can protect our systems and networks from those with malicious intents.

Some of the other topics that we will spend time on in this guidebook include how to keep our networks safe from online attacks, the importance

of a firewall, and how to understand the basics of cryptography and how this works with our hacking needs.

Hacking is a term that most people associate with something bad, and they may be scared to even learn more about how this process works. With this guidebook, we are able to take a look at how to hack with the Linux system and the best ways to protect ourselves from some of these bad attacks before they can take our information and wreak havoc. When you are ready to learn more about hacking with Kali Linux, make sure to check out this guidebook to help you out!

Chapter 1: The Different Types of Hackers

The first thing that we need to take a look at here in this guidebook is the different types of hackers. Often, when we hear about a hacker, we think of someone who is trying to get onto a system, usually one they have no right to access and stealing identities, personal information, and more things that they should not have control over. But there are actually a few different types of hackers out there.

The first type is someone who likes to try and get onto systems where they are not allowed. Usually, this is for their own purposes, and they are not concerned about how this will negatively affect the other person. For example, these kinds of hackers are likely to get onto a database for business and steal names, addresses, phone numbers, and credit card information of those who have shopped at that store.

But this is just one kind of hacker that is out there. They get the most attention because they are the ones who cause the most damage, but there are two other types of hackers that we need to discuss as well. For example, one type of hacker may try to get onto a system that they do not have access to, but they are not doing this to cause harm. Instead, they do this to show some of the weaknesses in that system or because they are bored and want to see if they can actually succeed with it.

Then there are actually those hackers who do the hacking legally. They have permission to be on the system, and they hack through it to see where the vulnerabilities are. They are often hired by the organization they are hacking, either as a fulltime staff or as a freelance worker, to help them protect against actual bad hackers and keep the information safe.

Even though there are different motivations behind the three types of hacking, they will all use some of the same techniques to get the job done. We are going to focus our work with the last type of hacker, looking at how you can perform and protect against a variety of attacks, but the same kinds of methods can be used with someone who has malicious intent on the system. With this in mind, let’s dive a bit more into the three types of hacking, including the black hat hacker, the gray hat hacker, and the white hat hacker, and see how each one of these is a bit different.

The Black Hat Hacker

The first type of hacker that we are going to take a look at is the black hat hacker. This is the kind that is going to be heard in the news the most, the one that we think about when we hear about hacking in the first place. A black hat hacker is going to be someone who searches around for vulnerabilities in a security system and then will exploit them. The exploitation often occurs for either financial gain or some other kind of malicious reason.

These people are not usually worried about the harm that they cause to other people. They will want to gather this information to use for their own needs at some point. Often, this is done so that they can steal money and make themselves rich before disappearing without a trace. They have no wish to make things safe for others. They just worry about their own benefits and how this process can help them in some manner.

Depending on how far into the system the black hat hacker can get, they have the potential to inflict some major damage on the individual users of that computer, the shoppers at that store, and the organization itself. They can really work hard to steal personal financial information, compromise the security that we see in the major systems, and even shut down or alter some of the functioning of networks and websites.

These kinds of hackers can range from those who are teenage amateurs who want to spread a virus across the computer all the way to networks of criminals who have the goal of stealing numbers on credit cards and other important financial information.

There are a lot of different methods that the black hat hacker is able to utilize, and these can be similar to what we will find with the gray hat and the white hat hackers as well. For example, the activities that a black hat hacker may rely on could include something like adding keystroke monitoring programs to a system to steal data or even launching a whole attack that can disable a whole website, and keep people from accessing it at all while they steal the information.

Sometimes, these malicious hackers are going to employ methods that are not on the computer in order to obtain the information that they need. For

example, they could call into a system and assume the identity of another user in order to gain access to that user's password and access to the system through that manner instead.

The main difference that shows up between these kinds of hackers and what we see with a gray hat or a white hat hacker is the intention. They may use the same techniques as the other two, but their point is to benefit themselves without any care about how it is going to affect the other party at all. This can be dangerous for a business. If a black hat hacker can get onto their system and steal information, it could make them lose their reputation, lots of money for their customers, and so much more .

Gray Hat Hacker

Now that we have a better understanding of what a black hat hacker is, it is time to take a look at the gray hat hacker. A gray hat hacker is going to be someone who is breaking some ethical principles and standards, just like with the black hat hacker. But the difference here is that they are doing this without the malicious intents of the black hat hacker.

What this means is that the gray hat hacker can engage in practices that seem dishonest and are illegal. But they are doing this more in the name of the common good, or at least not with the intention of harming others. These hackers are kind of like the middle ground when it comes to the black hat hackers and the white hat hackers, the ones who are going to work on behalf of the company that is maintaining a secure system, and the black hat who will act in a malicious manner in order to exploit some of the vulnerabilities that can show up in a system.

Often, when we think about hacking, we assume that it is all in black and white. We think that there are ethical hackers and unethical hackers. However, even though gray hat hacking is somewhere in the middle, it is still able to play a big role in the security world. One of the most common examples that we are able to see when it comes to a gray hat hacker is someone who is able to exploit a vulnerability in a security system in order to help spread some awareness to the public that this vulnerability is actually there.

The hacker did not get on to steal money, cause chaos, and steal all of the personal information from the users. They got on to show the public that there is some kind of vulnerability that is in the system, in the hopes that this will alert others to make smarter decisions, and even for some changes to occur.

Sometimes, this information can go wrong, though. If the gray hat hacker announces that they found the vulnerability and the company does not work to change this issue and fix it, it is possible that black hat hackers can get through this vulnerability and use it for their own needs as well. This can cause a lot of damage and issues to the company as they suffer more attacks and have to deal with the fallout.

Technically, the work that is done by the gray hat hacker is going to be seen as illegal. They still did not have the permission that they needed to complete the hack that they did, and this makes it something that they shouldn't have been doing in the first place. But since they were able to alert the public to a problem in a system that they may have been using, or because they alerted the business of a potential problem ahead of time, before other hackers got there, often they may not face as much punishment as some of the black hat hackers who will use this to help themselves get money or information or something else for personal gain.

There are many examples where a gray hat hacker was able to get onto a system and then alerted the company about these vulnerabilities. They may have even explained exactly how they did it and how they would be able to fix it. Some of these have been able to get prominent positions in these companies, helping to close up the vulnerabilities a bit, and then keeping the system and the network as much as possible.

The White Hat Hacker

The third type of hacker that we need to look at is going to be a professional in computer security who will break into a system that is protected and other networks in order to test and then assess the security. These are going to often work for the company they are trying to break into, with the goal of checking that all the vulnerabilities are taken care of and that no other hacker is able to get onto that system.

These hackers are going to use their hacking skills to help improve security by exposing any vulnerabilities that are there before a malicious hacker or the black hat hacker can find these and exploit them for their own needs. Although the methods that are used with this are going to be similar and often identical to those that a black hat hacker will use, the white hat hackers have permission to get onto the system and employ these tactics to get the job done. These hackers also have the intention of protecting the information on the system rather than exploiting them.

When it comes to a white hat hacker, these are the ones who are seen using their skills in a manner that will benefit society. They could be reformed black hat hackers in some cases, or they could just be well-versed in the techniques and methods that hackers use. Companies often hire these individuals to do tests and to implement best practices to help them keep malicious hacking to a minimum and to ensure they are not as vulnerable as before.

For the most part, a white hat hacker is going to be synonymous with an ethical hacker. They will do the work to help out a business and to make sure that any potential vulnerabilities and issues are taken care of in a timely manner rather than letting a black hat hacker onto the system to cause a mess.

The white-hat hacker is often someone who has gone to a degree of schooling in order to learn a lot about computer systems and how they work. The other two types of hackers are going to spend their time learning computers and are often self-taught with the work that they have. Some may have a degree in IT or computers in some form, but most just had an interest in this kind of system and then worked on honing their skills through practice .

With the white hat hacker, these are professionals who spent quite a few times working with computers, computer technologies, and more and would have learned about hacking in the process. This allows them to be prepared for handling the large networks and systems for companies and protecting them as much as they can. These professionals don’t do the work of hacking in order to cause mischief or to work on their own personal gain. They do it as part of their job to keep companies and the customers who work with these companies as safe as possible from other hackers.

As we can see, there are a lot of differences that come with the world of hacking, and each of the types of hackers out there is going to work in a slightly different manner from one another. The black hat hacker is going to spend their time getting into a system for their own malicious intents. The gray hat hacker is somewhere in the middle and will exploit the system in order to tell the public about this issue. And then the white hat hacker is going to come in as someone who works for the company and ensures that the information with that company stays as safe and secure as possible.

Each of these types of hackers is going to be vital to the world of hacking, and we need to be able to explore each of them and how they work. Remember that each one is going to use the same techniques. The differences here is that we need to look at some of the intentions behind those actions, and the reasons why each hacker is doing the activity that they are. Once we can understand how that works, it becomes easier to see how to use the techniques that we have in an ethical and safe manner.

Chapter 2: The Basics of the Hacking Process

Many beginners don't understand that hacking or any kind of penetration testing will follow a process that is very logical. They assume that they just get lucky when they can find a vulnerability in the system and that it is not worth their time to learn a process. But in reality, the hacking process is actually pretty logical, and we can break it down into tasks and goals that we are meant to follow in order to get things done.

Like all of the other IT or security projects that you want to work with, an ethical hacking plan is going to be something that we need to create in advance. Issues of strategy and tactics in ethical hacking need to be determined and agreed on ahead of time. To ensure that you see some success with the efforts that you are using, you also have to spend some time planning things out ahead of time. No matter what kind of process you are working on, this plan can be important.

It is important to notice the steps that are needed when a hacker is ready to begin working against their target. These steps are going to be similar whether they are working with a target that they know or someone they have no knowledge of, whether this is an individual, or they are more interested in attacking a large company and all of the personal information that is inside. These steps will ensure that we are able to handle all of the different parts that come with a hacking attack. All hackers will follow some form of these to help them get started.

There are five main steps that we need to take a look at when it comes to some of the basics of the hacking process. These are going to include:

Reconnaissance

The first phase of the hacking process that we are going to look at is known as reconnaissance. For us to be able to collect as much data as we can, this process can be used. Since all of the information and the data that we can collect during this time can be useful to us when we get to the later phases, this is often seen as the most important phase of them all.

Of course, some people think this phrase is boring. It doesn't involve some of the more advanced techniques, and it will include you just sitting around

and watching the system to see what information is going to show up on the system and how you can use this later on. There are also a lot of tools and techniques that you are able to use to help out with this phase, and some of them are free to use depending on your own needs .

Within this phase, there are going to be two types of reconnaissance that we are able to work with. The first kind is passive reconnaissance. When we are working with the passive form, we are going to get on the system, but our interaction will not be direct with the target system. For instance, when we check and look around the company's website, we like to target or if we like to see the job hirings in that specific company.

During this phase, we want to do a quick search on Google and look through some of the public records, including those on WHOIS, to help us get to gather data of the company we like to target as well as their website and such. Now, all of the techniques we use are not going to include direct interaction with the target company itself. It is mostly just research done on the company for now. These examples will be referred to as passive reconnaissance.

The scope of what we are going to gather during this phase is not going to include just the systems, servers, and hosts. But we can also use it to include some of the clients of our target system and the employees that we think we can use for our goals. Social engineering could then help us collect more data from the employees. Social engineering is going to be a technique that a hacker can use to manipulate a person to give any data that they don't usually give out .

The hacker hopes that with the help of social engineering, they will be able to fool the other person into giving up some personal information. They may even ask for information like the username and password of the employee so that they can get onto the system when they are ready.

Another example of what can be done with this process is known as dumpster diving. This is a place where we are going to look through different means to figure out important information. It can include going through the trash, but sometimes, just gaining access to some websites, the desk of employees, and more can help us to get the ATM slips, phone numbers, and bank statements that we are looking for.

The second type of reconnaissance that we can work with here is going to be known as active reconnaissance. With this kind of search, we are going to work to actively engage with the target we want to hack. Since this kind of process is going to involve us interacting directly with the target, there is going to be an additional level of challenge that comes up. Making telephone calls directly to the target and getting them to talk would be one of the examples of how this process works.

Also, some hackers like to work with a ping service. The reason that they like to work with this is that it permits them to determine if the system will respond or not. If it isn't responding, then it may be time to look for another method of entering into the system rather than the one you were looking at before.

Now, this is often one of the last types of reconnaissance that we want to work with. It is hard to know what is going to be present on the other side. The passive method is often easier because it allows us to stay hidden a bit more, and we can still gather up a lot of the information that we need. If the ping service is used to ping one of the servers of your target, though, then realize that this is active because you are still actively touching the server.

Any time that we work with the active process here, we have to be careful. There is always a possibility that you are leaving your mark behind. If any traces are there with you at any time, then it is possible that it can lead the target company right back to you.

Scanning

After the process of gathering information in the step from above, it is time to move on to the scanning phase. In this phase, we are going to use a variety of tools in order to gather up more of the information that we need about the target. There are a variety of tools that we are able to bring out when we get to this point, but some of these tools are going to include vulnerability scanners, sweepers, ping tools, network mappers, and port scanners. With all of these tools for scanning, it is surprising how much information we are able to gather about the target network.

For example, these tools will be used to determine the closed and opened ports at any given time. We will also know what type of operating systems

the company uses and what types of devices are on that network, to name a few things we can look up.

You will notice with this phase that the scanning is going to be more active than before, but the good news is that we can also use the other passive forms of scanning. So, when determining the type of operating system being used, we can send some network traffic to the systems. The response that we get from the operating system to that traffic will vary based on the kind of system in place.

All of the operating systems are going to respond to the traffic that is sent through in different manners. This means that a computer with the Windows operating system is going to respond to any traffic that is sent through in a different manner compared to a Linux computer and a Mac computer. And the same can be said to all of the other operating systems as well.

One example that we are able to take a look at when it comes to scanning passively is sniffing out the traffic on the network. We can work with a few tools for this, but Wireshark is a great option to help us sniff out the network traffic. Knowing the whole network infrastructure will be easier as a result of this phase.

From here, we are able to work on making sense of some of the data that we have collected in this phase, as well as in the first phase. Then we are able to convert all of the data into useful information. This is a great thing to work with because it provides us with a blueprint of what is going on in the entire network we are on.

Gaining Access

Now that we have had some time to gather a bit of information on the target system that we want to work with, and we have been able to add in a bit more activity and look at how to scan some of the networks to get a good blueprint, it is time to work on the third step of gaining access. This is actually the phase where some of the real hacking is going to take place.

When we are in this phase, we are going to try to get into the target system and see how we can use the vulnerabilities that we were able to use during the scanning phase. Figuring out a good path that will help us, the attacker,

to get into the infrastructure of the network is important so that we can take control over the whole thing .

There are a variety of methods that we can see in order to gain the access that we want to the network. And it is likely that you will have to use at least a few before you are able to gain that access. We can get access through the network, through a vulnerability in an application that is on that network, or even through the specific operating system that is on the network.

When we are in the gaining access phase of this process, there are also a few different methods that can help us reach our goals. We can do something like a denial of service attack or session hijacking in some cases. The denial of service attack or DOS on a system is a good option to work with because it will expose some of the hidden vulnerabilities that show up in the system.

As soon as we are able to find at least one vulnerability, but hopefully more, you are then able to use these to help us gain access to the system. This can take some time, especially if there is a white-hat hacker working for the company and trying to keep other people out of the system. But once we have gained the access that we want to the system, we are doing with this phase of the process with hacking.

Gaining access is a part that can take us some time in order to get things done. We want to use some of the different parts that we discussed earlier, the information that we were able to discover and learn about the business and the network, and then gain access. Remember that with this one, the best place to get in is to look for those vulnerabilities and focus on how we can exploit some of those for our needs.

Many systems have some kind of vulnerability that happens to them. But sometimes, it takes time to find them. It could be a vulnerability that shows up in the operating system or another piece of hardware or software that the network is using. Sometimes, it is going to be by finding a port that is not closed off and monitored the way that it should. But often, the way that you find a vulnerability and exploit it is through human error.

For many hackers, a human error is going to be the easiest way for them to get onto a system, no matter what operating system they are on or anything else. When humans are not paying attention to what they are doing, and they do not follow the proper security protocols, it is the best thing for the hacker to get what they would like. Hackers can get on when users share their information with others, when they don't log out of the system, when they open up emails that they shouldn't, or even when they are not careful about the websites they are visiting and the information that they share on those websites while they are at work and on the network.

Finding where this vulnerability is and putting in some protocols along the way to make sure that everyone follows the rules and doesn't put the whole system at risk can be so important to your network. Whether it is some of the software that you are working with or someone who is on the network who is creating these openings, it is time to find the best ways to fix these issues as we can.

Maintaining Access

Once we have had some time to penetrate into the network, and we have the access that we need into the system, the next challenge that we need to work on is maintaining the access. If something on the network suspects that you are there, then you will be kicked out, and the vulnerability that you exploited is going to get fixed. Getting onto the system and being careful until you are ready to make the attack is key here.

Once we have had a chance to get onto the network, it is likely that we would like to, in the future, return to the same level of access or greater. To do this, we would need to implement some features to get this done, including a backdoor, Trojan, or rootkit that can help us get access to that same network even in the future.

Take note that it will be better for us if we keep control of the system for a longer period. This system can then be used as a source that can help us infect some of the other devices that are on the network until we reach our ultimate goal with this process .

While we are on this system and maintaining our access, we are in the perfect position for doing a lot of things. We can intercept some of the emails that we see coming in. We can watch what users are getting onto the

system and what they are doing there. We can watch the network traffic that is coming in and causing problems. And we can even work on adding in a keyboard logger so that we can learn the passwords and usernames to get onto more of the system.

There are a lot of benefits that the hacker is able to get when they work with continuous access to the network. These benefits could include data manipulation and monitoring of the network for a long time, which include additional time in launching some added attacks in the process.

The overall goal here is for you to stay on the system for as long as you can. The quieter you are here, and the better you are at doing the hacking, the easier it is going to be for you to stay put and not get noticed. Be more of an observer in the beginning, at least until your attack is made. It is unlikely that even with a vulnerability present that the target network doesn't have anything on it to help keep things protected and safe. If you make the wrong move and aren't careful before your attack, it is likely that something on the network will find you and your access and your control will be lost .

Clearing the Tracks

And now, we are in the last phase of hacking at this point. This phase is going to include clearing or covering our tracks. The network's IT professionals should not notice that the hackers are on their system. That should be the hacker's main goal. If we have done anything malicious to the network or system, we should try to hide it.

The reason is that we, as the hacker, can still continue and maintain access on the network if no one notices what we have done. Since no one has caught or noticed the attack, we will not be pushed out of the system and can still have access in the future. The more subtle that you can be and the less noise that you make in the process, the better it is for you overall.

The hacker should also ensure to cover up their tracks on the system by overwriting, destroying, or deleting any logs that may document their activities in the system. This ensures so that no one is able to take a look at the logs later on and notice that there is some strange activity going on, or a system that should not be present causing issues.

It is so important that you go out and clear your tracks when you are all done with your work. Leaving anything behind when you are done may seem like a good idea, but remember that other hackers, such as the white hat hackers who work for the company, are often going to be looking around. You may have beaten them to that vulnerability and made it onto the system, but, at some point, they are going to find it and can use that to find you as well.

Clearing out your tracks helps to end the process and makes it easier for you to not get caught. There is a level of anonymity that is present in this kind of hacking. But as soon as someone finds you and figures out what you are doing, they can trace you down and even cut out that access point you had in the first place, and neither of these things is good for you and any of the hacking that you want to do.

And these are the basic parts that come with the hacking process. The goal is to get onto the system as secretly and quietly as possible, with the hopes that no one is going to notice that you are there or cause a stir because they see something strange going on. If you are able to get through the five steps that are above, it is much easier to gain the access that you want to a system, and then you can complete the attack that you want to do.

Chapter 3: How to Install and Use the OS Kali Linux for Hacking

Now that we have had some time to look at some of the basics that come with the methods of hacking, it is time to download the operating system that we want to use to get this hacking done. While we can work with some of these hacking options no matter what operating system we are on, we are going to focus on how we can get this done with Kali Linux. Before we are able to utilize this, though, we need to install the operating system and get it ready to go on your computer.

Linux is often the top operating system that hackers will use, mainly because it is easy to work with, and will have all of the software that is needed to complete a hacking project. It is free and open-source, which means that we are able to make modifications and use them in any manner that we would like.

Installing the Kali Linux is sometimes a bit complicated for beginners, but that is what we will spend some time on in this chapter. We are going to take a look at how to dual boot with Kali Linux and then look at how we can work with this in the other operating systems, including Windows and Mac OS, for our needs .

A Dual Boot of Kali Linux

The first option that we are going to take a look at in this guidebook is how to work with a dual boot of Kali Linux. This helps us to make sure that we can get it to work with a Windows operating system, mainly Windows 7 8 or 8.1. So, if you are not a fan of working with the newer version of Windows, we can get that under control as well. Let’s get started then!

Before we get started with the dual boost, we need to make sure that we have the right materials present to work with here. Some of these include:

1. Windows 10 or any of the other versions of Windows that are already installed on your computer.
2. A laptop or PC that is able to handle some of the different hacking processes that we want to do.

3. A minimum of 4 GB Pendrive
4. At least a Dual Core in your system, either AMD or Intel, works well for this, and the RAM must be a minimum of 1 GB.
5. The latest version of Kali Linux
6. Rufus
7. And patience to get it all done.

To begin, we will know how to use the Windows 10 program in doing a Dual Boot of Kali Linux v2019.2. The first step is to download the latest ISO file of Kali Linux. You will be able to get this by visiting kali.org. You can choose whether you would like to download the 32 bit or the 64 bit while you are there. After Kali Linux has had some time to download, the next step is for us to create our own bootable USB. For this, we need to work with the Rufus extension. This is a utility that can help us to create these USB flash drives that are bootable. Go to Rufus.ie to download the extension before installing it in the system.

With these two items on your computer, we want to start by making a bootable USB. First, connect the USB that we want to use. As we said above, this needs to have at least 4 GB of memory in order to work and have enough space to handle the Rufus extension and the Kali Linux. When the USB is inside the computer, we can run Rufus and use the steps below in creating a bootable USB drive.

1. First, an image will show up on the screen about the Rufus program that you are running.
2. Check that the USB drive is the one selected on there, then click on the small drive icon for the CD.
3. Locate the ISO file for Kali Linux that we downloaded earlier and then click on Start. Give this process a few minutes to complete before moving on.
4. After the process is complete, you can click on the close button to get the Rufus window to close. This will give you the bootable USB drive for Kali Linux.
    a. Other than using this to help with the dual booting of Kali Linux in Windows, you can also do a Kali live boot using this USB. This means that we are able to run Kali without having to install it on our system.

Keep in mind that it does limit the functions and the features a little bit when you work in this matter.

From this point, for the installation of the Kali Linux, a separate partition should be created. So, to do this part, we can open up the settings for Disk management, or we can run in Windows the command of “diskmgmt.msc.” If we created a 15 to 20 GB minimum-sized partition, it might shrink the volume that we already have.

At this point, we noticed that the first processes were through. The Kali Linux’s ISO was downloaded, a programmed bootable USB drive was created, and a separate partition for the Kali Linux installation was created. Before we continue, we should remember that the Fast Boot and Disable Secure Boot options are available in the BIOS if we would like to use them on our program .

We can now restart our laptop or PC. Go to the boot manager as it starts up again. Choose USB on the option boot. Remember that the different brands will slightly have different options. You can now see the Kali Linux’s installation on your screen. There are a few choices that come up at this point about how to install Kali Linux. You will want to choose the option for “Graphical Install” to help get the Kali Linux to start with some ease. We can take this further and add in a few of the settings and features that we want. For example, you can choose what language you would like to use for the installation process and the country as well.

After we have been able to go through and add in some of the preferences above and the other options that the system asks for, it is time to work on the hostname. Your installation is going to ask for the Hostname. You are able to choose any name that you want because this will be like your username. The password for the root user should then be entered. After the password that you want for the administrative account is entered, you can click on continue.

Now, we want to choose the partitioning method that we want to use, and the option that we will work with is Manual. The next step needs some caution. We want to only choose the partition that we took the time to create earlier for the installation of Kali and then press on Continue. When you are sure you have chosen the right option, you can select “Delete the partition”

before continuing. If you did this the right way, you will notice the “FREE SPACE,” which is the partition in the Kali Installation. We want to choose this free space partition before continuing on with the process.

Here, the installation is going to ask us how we would like to use that free space. Our goal is to click on the “Automatically partition the free space” and then continue. After that, select the option that says, “All files in one partition.” This is going to be the recommended option for new users in case this is worded differently with your version. And then, we want to choose the option that says “Finish partitioning and write changes to disk.” It wants you to grant it permission to write these changes into the disk. You can choose Yes and then Continue.

This is where the installation process of Kali Linux is going to happen. This can take a bit of time, so expect to take about 15 minutes or so before the process is done. About halfway through the process, the network will ask for a network mirror. Select the one that you want. This setting is about the update option, so it is best if you can choose no for now and then make changes later if you would like to.

Next, the installation is going to ask for installing the GRUB boot loader. You want to click on Yes before continuing. Next, it is going to ask you where you would like to install the Kali GRUB boot loader. The best choice will be the hard disk that has the 2nd option. We want the GRUB to happen on your hard disk, or the option to select the operating systems will not be displayed by the installation of Kali Linux when the computer starts up, and that is a big goal of ours with this process.

After you have completed these steps and are successful with the installation process of Linux, now you are going to see a screen that is going to ask you whether to continue or go back. Click on Continue and then eject the USB drive. You will need to restart the system at this point. During the process of Start-Up, you will be able to see the Kali Linux through our GRUB Loader. The computer can be booted with the Kali Linux by selecting the Kali GNU/Linux. Or, if you would like to just work with your Windows environment, then you can choose the option that says Windows Recovery Environment.

And that is all there is to it. You just need to go through some of the steps that we did above, and you can get it set up so that the Kali Linux distribution is ready to go, and you can use it at any time that you want. Each time that you restart your computer, you will be able to choose whether you would like to work with the Kali Linux operating system or the Windows operating system for your needs, making it easy to switch back and forth between the two.

Chapter 4: An Introduction to Cyber Security

The next topic that we need to take a look at here is the idea of cybersecurity and what this is all about. As someone who is working on Kali Linux as part of the hacking process, it is important to know as much as possible about cybersecurity and how you can protect your system and all of the networks that you need to protect from outside threats. So, let's dive right in.

Cybersecurity is going to be the state or the process of protecting and recovering programs, devices, and networks from any type of cyber attack that a hacker or someone else may want to get into. These cyberattacks are more common than ever before. There are a lot of hackers and other individuals who want to get access to a large number of computers, whether this is a large number of personal computers and the information on those or that of a large company holding onto a big set of data about their customers.

There are a lot of benefits to someone completing these cyberattacks. If they are successful and no one ends up catching them or what they are doing, then this can really help them to gain access to information that they should not have. Many hackers want to do this to destroy a business, steal personal information from customers and employees, and even to steal money. Some companies may try to unethically attack another competitor in order to get information on new products and services and take them over for themselves.

No matter what the reason is for the attack, there is going to be some benefit to the hacker, and it is often going to cause a mess for the company and everyone else who is affected in the process. And it is the job of a white-hat hacker and the rest of the IT professional team to keep some of these cyberattacks down to a minimum.

These cyberattacks are an evolving danger to consumers, employees, and organizations. They are going to be designed in a manner that helps them to access or destroy any sensitive data that may be in a system or even to extort money when necessary. They can, when they are successful and depending on the scale of them, really destroy businesses and damage the financial and personal lives of those who were on the system.

Many companies spend a lot of time and money trying to protect the information they have for their customers. Any time that you shop online or do another activity, there is quite a bit of personal information that gets left behind as well. This could include your name, address, telephone, defining features (such as gender, age, occupation, and so on), and your payment information .

These companies know that if the information gets into the wrong hands, it could cause chaos. The hacker could steal many identities and use the payment options as much as they want, causing a lot of lost money and time in the process before someone could notice. And this would effectively cause a good deal of damage to the businesses that allowed it to happen.

So, what is going to be the best defense to slow this down and make sure that it is not going to happen again? Basically, a strong cybersecurity system is going to have multiple layers of protection that are spread across programs, networks, and computers. But a strong cybersecurity system is going to rely not only on cyber defense technology but also on people who are able to make some smart choices for cyber defense.

The good news here is that you don’t need to have a specialist in cybersecurity, and you don’t have to be one in order to understand and practice some of the cyber defense tactics. This chapter can be a great place for you to start with this process and can get it all done for you. We are going to take a closer look at cybersecurity and how we can use this to defend ourselves, as much as possible, against these threats. It could be the exact thing that you need to help recognize and avoid some of these online threats before they have a chance to get onto your device or your network :

The Different Types of Cyber Threats

The first thing that we need to take a look at here is the different types of cyber threats. There are quite a few of these out in our world, and as technology changes and hackers become more adept at what they can do online, it is likely that this problem is going to become much worse. Some of the most common types of cyber threats that all businesses and even individuals need to watch out for on their system will include:

1. Social engineering: This one is going to be a process where the hacker is going to psychologically manipulate others. The goal is

to get the target to perform certain actions or give away important information.

2. Advanced Persistent Threats or APTs. These are going to attack where the unauthorized user is able to infiltrate the network without being caught and then will stay in that network for a longer period of time without detection.
3. Malware: This is a type of software that has been designed to specifically help the hacker gain access to the system or to cause some damage to the computer without the owner knowing what is going on.
4. Ransomware: This is going to be an example of malicious software. It has been designed in a manner that will extort money by blocking access to files or to the system of the computer until the target has worked to pay the ransom. While the hacker may take the ransom and make it look like they have left the system, this payment is not going to guarantee that all of the files will be recovered or that the system is going to be restored to what you want it to be. In fact, it is likely that the hacker is going to keep something on the computer so that they can get back on later if they would like. And it is even possible that they will take the money and disappear without fixing anything at all.
5. Phishing. Another type of attack that individuals and businesses need to pay attention to is known as phishing. This is the process of sending out emails that are fraudulent and that are going to resemble emails from some reputable sources. The aim of this one is to steal some of the sensitive data from the individual, including their login information and credit card numbers. This is actually one of the most common attack types. You can protect against this by going straight to the website that is asking for the information, rather than providing it through email, and work with a technology solution that is able to filter through some of these malicious emails.

There are actually a few different types of cyber threats that are able to attack your networks and your devices, and it is important to pay attention to what these are and how we can avoid them. Generally, though, they will fall into three categories. These are going to include attacks on the

availability, integrity, and confidentiality of our systems. Let’s take a look at each of these that we can experience if we do not provide the right kind of cybersecurity on our networks and systems.

The first on the list is the attacks on confidentiality. These are going to include any attack that is able to steal your personal identity information, such as your credit card information or your bank account. Many of these attackers are going to take your information and then will sell it on the dark web, usually for others to purchase and use as they want.

Then there are the attacks that happen on your integrity. These are going to be the attacks that consist of either enterprise or personal sabotage, and they are often what we hear about as leaks. A cybercriminal is able to access and then release any of the sensitive information that they have, usually for the purpose of really exposing that data and influencing the public to start withholding their trust in that company.

And the third type of cyber threat that we need to watch out includes the attacks on availability. The aim of a hacker who uses this kind of attack is to make it impossible for users to get their own data until they are able to pay a fee or a ransom to the hacker. Typically, the cybercriminal is going to work on getting into the network and blocks you from getting important data until you are able to pay a ransom .

In some cases, the company is likely to pay the ransom in order to try and get their data back and get the attack to go away. They may do this to avoid halting some of the business activities that need to happen. However, this doesn’t always solve the problem, and often, the hacker is going to leave something on the system that allows them to come back on unless a white hat hacker or another professional in IT can come and fix that problem.

As we mentioned before, these are a few other types of cyber threats that a company needs to watch out for, and we need to always be on the lookout for some of these things happening. Going back to the social engineering that we talked about before, the hacker is able to actually convince or manipulate someone to give up their personal information.

Social engineering, as we mentioned, is a type of attack on confidentiality. It is the process where the hacker will be manipulated into performing an

action that the hacker wants or giving away their information. Often, this would include a phishing attack with a deceptive email. For example, the email may look like it comes from the target's bank, asking them to check a message in their account. The user will click on it, provide their user name and password, and then the hacker has access to this information any time that they want .

Back to the APTs, or Advanced Persistent Threats, that we talked about earlier, we are able to see a type of attack on integrity. Basically, with this one, an unauthorized user is able to get onto the target network without anyone realizing that they are there, and then they can stay on that target network for a long period of time. The main point of this one, though it may take some time, is to steal data without causing harm to the network, at least for now. These attacks are most likely to happen with companies and sectors that have a lot of valuable information. We may see this in the finance industry, manufacturing, and national defense, for example.

And then we can go back to the idea of malware that we briefly discussed above. This is basically a malicious software, and it is going to be a good example of an attack on availability. It is going to refer to software that is designed to gain access or damage a computer, without the owner having any knowledge of what is going on. There are a lot of different types of malware that we can pay attention to, and they may include things like worms, true viruses, keyloggers, and spyware.

What is this Cyber Security all About?

A successful approach to cybersecurity is going to have many different layers of protection that are going to be spread out across all of the data, programs, networks, and computers that you would like to keep safe and sound. In business, the processes, technology, and people have to be able to complement one another to make sure that we have a very effective defense form cyberattacks. If one or more of these is off or one missing a link, then it is going to cause a break in the armor and can increase the amount of risk that is there for everyone.

A unified system of threat management can automate the integrations across all of your processes and will make it easier to keep all of your network and the information that is inside as safe as possible. We have to

make sure though that all of these parts are going to come together and work in the manner that we want.

The first thing to consider is the people. This is often the weakest part of the process. Someone in the organization can get careless, fall for a phishing scam, or do something else that can put the security of the whole network at risk. Users of that network need to understand and be willing to comply with the basic data security principles that your business sets up. This can include things like choosing out a password that is strong, backing up their data, and being wary of any attachments that may show up in emails.

The next thing that we need to take a look at here is some of the processes that may show up on your network. Your organization has to have some kind of framework in place for how they are going to deal with all types of attacks, including those that were attempted and failed, and those that are successful. One well-respected framework is able to guide everyone in the network. It is going to help everyone see how they can identify these attacks, protect the whole system, detect and respond to some of the threats, and even how to recover from the attacks that end up being successful.

And finally, we have to focus on technology. If the technology is not secure and not taken care of the right way, such as doing the needed updates and software changes, then it is going to leave a lot of openings for an experienced hacker to get into the system. Technology is going to be essential when it comes to giving individuals and organizations the computer security tools that they need to make sure they are protected from these attacks.

There are three main entities in your network that you need to make sure are always protected to keep the whole network safe. These include the endpoint devices, such as the routers, smart devices, and computers, the networks, and the cloud. Common technology that is often used to help protect these entities are going to include a lot of features, including email security solutions, antivirus software, malware protection, DNS filtering, and next-generation firewalls, to name a few.

All of these three parts need to come together in order to create a system that is safe and secure. When one of these parts fails or is not maintaining the job that it should, that means that all of the others could be at risk, and it

is likely that someone is going to try and get on your system and use the vulnerabilities that are there. Remember that if there is a way to get onto your system, whether it is through the people, the processes, or the technology, then there is a hacker out there who will try to do this.

Having a white hat hacker, or even a big team of these IT professionals if your company is larger, working to find and protect against the vulnerabilities can be your biggest asset overall. This will ensure that you are able to find the issues and solve them before a black hat hacker is able to find the information and exploit it to their advantage.

Why is this Cyber Security so Important?

The next thing that we need to take a look at here is why this cybersecurity is so important. In the connected world that we see today, everyone is able to benefit when we can advance some of the programs of cyber defense. We can take this all the way up to the highest cooperation and down to the individual level. When we look at this from the individual level, the attack can result in a lot of issues, including extortion for money attempts, identify theft, and even the loss of some important data, including family pictures .

In addition to some of the individual issues that can show up with these cybersecurity issues, everyone is going to rely on some of the more critical of infrastructures in our modern world, including financial service companies, hospitals, and power plants. Being able to keep these kinds of industries and businesses safe from an attack can be essential to many people in our society.

Everyone is also going to benefit when it comes to the work that researchers of cyber threats are able to do. One example of these researchers is going to be the team of 250 threat researchers from Talos. These individuals investigate some of the new and emerging threats and cyberattack strategies that are being used by hackers in our modern world.

This group can be helpful because they will do a number of tasks that help out with the cybersecurity that we have been talking about. They are able to reveal some new vulnerabilities that have been found, educate the public when it comes to the importance of cybersecurity, and can strengthen some of the open-sourced and readily available tools. Basically, the work that this

team and others are able to do will ensure that the internet stays as safe as possible for everyone .

Ways to Protect against the Cyber Security Attacks

Of course, as a business and even as an individual who wants to keep their information as safe and secure as possible, you are probably curious about some of the methods that can help you to do this. Many white hat hackers working for companies are full of knowledge about the best ways to avoid a hack and how to make sure they can stay safe. But anyone, whether they are an IT professional or not, can have the resources to keep their information safe. Some of the best steps to help out with staying safe with your network include the following:

1. When you provide your personal information, make sure that you are only working with sites that you trust. A good rule of thumb for this one is to check on the URL. If the side includes the https:// in the beginning, then we know that it is a secure site. If the URL is missing that “s,” it is important to avoid entering any kind of sensitive information like your social security number or data on your credit card because it could be a bad site.
2. You should never open up any email attachments or click on links that are in emails from sources you do not know. You should also make sure that others are on the same network as you do the same. One of the most common ways that people are going to be attacked is with these emails that are disguised and sent out, looking like they come from someone you really trust.
3. Keep the devices up to date. If you personally, or your workplace, isn’t keeping the devices as up to date as possible, then this can cause some problems for everyone. Software updates are going to be important because they contain some of the patches that you need to fix security issues and to keep the cyber attacks out. Cyber attackers love it when a device is out of date because it is much easier for them to get onto that network and cause issues.
4. Make sure that you back up your files on a regular basis in order to prevent attacks on your cybersecurity. If you get attacked and need to wipe all of your devices in order to keep the attack off

your computer, it is going to be much better to have the files stored in another place so you can get them back when you need to.

Cybersecurity is going to be something that is always evolving, which is sometimes going to make it even more difficult for us to stay up to date and current on all of the information that we need to take care of. But whether we are talking about a company or an individual, it is important to make sure that we can keep our network safe so that no one is able to come on and steal our personal information, ask for money, or cause some of the other issues as well.

Staying informed and making sure that you and others around you are as cautious online as possible are two of the best ways to make sure that you are protected and that someone is not likely to cause these kinds of attacks on you.

Chapter 5: Malware Attacks

Now that we have spent a bit of time talking about the importance of cybersecurity to make sure that our networks and systems can stay safe, it is time to move on to learn about a few of the different prominent types of malware attacks that we can watch out against. These are going to be similar whether you are trying to protect your own personal computer or you are protecting larger amounts of data and personal information for a big company.

Malware attacks are a big problem for many companies, and they can be one of the biggest issues when it comes to the world of cybersecurity. If even one part of the system, whether it is the processes, the technology, or one of the people on the network, falls prey to this, then it can spell trouble for the whole organization. It is important to recognize some of the most common malware attacks and how they work so that we can stay protected and safe from all of them while making sure that our personal information is always safe and sound.

Three Categories of Cyberattacks

For all of the supposed mystique and mystery that are around things known as cyberattacks, they are actually pretty much all the same-old property and financial crimes, but sometimes add in some new tools. Because of the assumed anonymity that people can take on when they use the internet, there are a lot of people who will be enticed to doing these crimes, and many people need to be on the lookout before they are taken advantage of overall.

Many of these cybercriminals are going to be able to get in and out without you noticing, unless you are being vigilant and watching your system and how things are going. Others may spend too much time bragging about what they did and will get into trouble that way. But one thing is for sure, because of the anonymity, many people wouldn’t want to attempt breaking into a house or do any other crimes could be tempted to give cybercrime a try because they think that they won’t get caught.

For the average user, this means that there are more attacks on their systems and networks than ever before. This can be a problem for those who want to learn how to keep their information safe, even if that information is just their family pictures. The good news is that there are ways that we can protect ourselves, we just need to be on the lookout ahead of time so that we are not taken advantage of.

To help us get started, we need to take a look at some of the things that come with a cyberattack and how to watch out for them. For the most part, these cyberattacks are going to fall into one of three categories that include:

1. The target and the criminal are going to know each other in some manner. The motivating factor in this one can often be revenge or money, and the many distinguishing features that we will look for are that the culprit perpetrator has or had computer access to their target. This allows them time to do preparation on the attack ahead of time, plant in some malware, and more. In this category, we will see things like cyber-spying taking on more of a role with the help of keyloggers, microphones, and webcams.
2. The second option is that there is some kind of relationship between the criminal and the target, or, at the very least, the criminal knows the victim. They may have made a connection on any social media platforms, they are famous or rich, or they own something that the hacker wanted. Selecting a victim is not random, though they haven't met yet physically, and they don't have physical access to the computer of the target. Financial gain will be the motivation in this kind of situation.
3. The victim is not known to the criminal or is just a random person who was caught up in the phishing scam of the criminal or another similar technique. The victim nor the criminal has any idea who the other one is.

Examples of Malware Attacks

With this information in mind, it is time to take a look at some of the malware attacks that are out there and how we can be on the lookout for some of them. Often, the reason that these attacks work is human error. A person, the target, is not going to be on the lookout for trouble and will give

up information that they never would have if they were thinking critically. This can be good news if you learn how to use it for your advantage and stay on the lookout.

You will find that cybercriminals, cyber spies, and hackers are going to use a lot of techniques and vectors in order to break into a computer network and steal customer information, intellectual property, sensitive information that can identify a person, including social security and credit card numbers numbers, health and medical insurance records, business plans, personal records,tax records, and any other data that they can gain money from or use to exploit to their own advantage.

Remember that anyone can be a target. Many individuals assume that they don't need to be careful at all, but hackers will go after you even. They can steal your credit card information, your personal information, and more to get what they want, and it could take years to get things back in order after this happens. It does not matter the location, the industry, or the size of the target; the hacker will go after them if they think there is something to gain.

There are a number of different methods that the hacker is able to employ in order to get their work done and to see some of the results that they want. Some of the most common malware attacks that a target needs to be on the lookout for includes:

Emails that have an attachment with malware and viruses. This is an older technique that most people know how to avoid. It is common knowledge that we need to avoid opening attachments unless we are certain that we know the sender and that the information in it is legitimate. And yet, there are still many people who fall for this one, and it proves successful for the hacker over and over again. This may be one of the most well-known methods of disseminating malware, and all it includes for the hacker is to hide the malicious software in an attachment in an email. Once the target opens up the attachment, then the malicious software is going to execute or will download it on the computer.

The best thing that you can do to prevent this happening is to not open up attachments from unsecured emails. Unless you are expecting an attachment from someone specific, it is often best to just ignore emails that have this kind of thing. Hopefully, the spam detection that you have on your

email account will put most of these out of your sight, but sometimes a few sneak by, and it is best to exercise caution rather than get some malware on your computer.

The second malware attack that we need to watch out for is similar to the one above, but instead of an attachment, the link inside the email is going to be the problem. This is going to be something that is known as phishing. Often, these emails are going to appear as legitimate correspondence from an institution, usually your bank, that the recipient is likely to trust and respond to.

However, the hacker has designed the email to track the target, and the link, when it is clicked on, will take the target to a fake website in order to get that target to send over sensitive information to the hacker. This could include things like the account number or the username and password of the bank. In addition, the malicious website can sometimes install spyware, virus, or malware onto the computer of the recipient, making it extra dangerous to work with.

The best thing that you can do to prevent this kind of attack is to be extra careful about the websites that you choose to visit through links. Verify that the email is actually from where you think it is. Even better, if it is something like your bank or another website that you trust, go directly to them through a search rather than clicking on the link. This way, you have protected whether the link is a good one or not .

Next on the list is going to be a social networking profile or page that has links over to a malicious website. This is going to be a similar kind of thing like what we see with emails and links, but this is a method that is growing in popularity thanks to all of the hype around social media. It can be found on almost any social media account that you may use, including LinkedIn, Twitter, and Facebook, to name a few.

This technique is one that is pretty effective since a lot of people are less likely to have their guards up when they are on social media, and they may not be as wary of these sites as they would with some of the other websites that are out there. With this method, though, the hacker is going to set up a fake profile that will entice real users to follow the links that are there. These links are going to take the user over to a malicious website.

Sometimes, the fake profile can even get the targets to provide personal information that is sensitive to get the hacker what they want.

Always be careful about what you are doing on social media. Even if the link seems to come from a close friend or someone else, verify with them first. Too many times, a fake account can be created, and it will look exactly like a friend or family member. If you are careful and verify everything before you click, you will find that it is much easier to keep yourself protected online .

Another attack that we need to be careful about is probing firewalls, DSs, and PSs for weaknesses, including a backdoor. This is something that the hacker is going to do behind the scenes. The target usually does not have to click on anything to make this happen, but if they use certain applications and sites, or if they don't keep the right protection on their computer, it could leave an opening for the hacker to get on.

With this one, the hacker is simply going to send out transmissions, usually en masse, in the hopes of compromising any kind of firewall or another thing that they can come across. The hope here is that they are able to gain some access to a computer and the system that is behind it. This method is pretty much just going to be a numbers game for the hacker, and the system that they do get on isn't going to have any connection to them at all. The hacker will often send out millions of transmissions, and they hope to catch even a few computers in the process that have unpatched, misconfigured, or malfunctioning equipment. This type of attack is also going to be hard to trace without some packet capture along the way.

The best way that we are able to protect against this kind of attack is to make sure that your system is up to date as much as possible. This can close up a lot of the vulnerabilities that maybe there, and makes it that much harder for a hacker to get on your system and cause some problems. If you can keep the system up to date and be careful about the kind of software and more that you put onto the system, then you will find some tremendous results on what you can get done with your system.

Hackers may also choose to insert some malicious packets onto a legitimate communication stream to get the results that they want. This is going to be seen as a newer type of technique, one that is going to rely on the hacker

being able to access a stable of zombie computers. When they are able to do this, large quantities of packets can be sent out to a large number of recipients, which targets a certain port that seems to have the vulnerability the hacker wants.

The hope with this one is that, by chance, the hacker is going to be able to hit upon a firewall or router with that port open, and then use it as their way to access the whole system. This is a more difficult kind of attack. But if the hacker is successful with it, it is pretty much impossible for someone to trace who got into the system without a packet capture.

Another type of malware attack that we need to be wary about is advertisements that are able to send out malware to the viewers. This one is even harder for people to avoid simply because some of these can show up, even when you visit a page that is legitimate. If one of your favorite websites, for example, is not taking care of its firewalls, you could go in and get malware on your computer by clicking on one of the options there .

This method of attack is going to be hard for us to avoid because of all the paid advertisements that we can find on websites across the internet. It is possible for a cybercriminal to place these ads, ones that have malicious code in them, on legitimate and, otherwise, safe websites that visitors would trust. This makes it hard because while you should be able to come in and trust that website, and it is unlikely that you will purposely go through and pick out a bad website. These hackers are still able to cause problems.

There are a few ways that the hacker is able to get their ads on the website in the first place. Sometimes, they will actually purchase the ad space directly and then put the bad malware there. Sometimes, they will hijack the ad server. And other times, they can hijack themselves into the ad account of someone else and use that for their needs.

Always be careful about the kinds of ads that you are clicking on. Even if it is a website that looks safe, make sure that the ad is something that looks legitimate, and that will be able to work for what you think it claims. There are many times that the ad is going to look fake and like it is going to cause a problem, and if ever your intuition is speaking up and telling you not to click on something, then go ahead and listen to it.

We may also see that pre-installed malware can be a problem. Over the past few years or so, there have been a lot of reports about foreign-manufactured IT equipment, including switches, routers, and computers. And these parts already have malware pre-installed on them. In fact, this is such a widespread problem that in 2012, Microsoft declared that they found that there is already pre-installed malware in the new computers sold. HP also publicly announced, later in that same year, that there are Flashcards loaded with malware on some of the switches they have shipped the previous year.

This means that we need to be really careful with the computers and programs that we are using on a regular basis. These, when not purchased from reputable sources, and often when they come from other countries, could put our information and safety at risk. Double-checking where you get your products from and what issues may be coming out of that area can ensure that we get the safest programs and computers and their parts as we can.

Another issue that can come up here is malware that is sold as a legitimate type of software. Buying malware from a seller without a name can present some dangers, as well. Though the software is able to provide the promised function in some cases, it is possible that it could have some malicious software that is included in the bunch as well.

For example, fake antivirus programs have been able to infect millions of computers over the years. And in this same manner, anything from spyware to trojans can be added to your computer if the malware is allowed to be there. In research that IPCopper was able to conduct in 2013, it was found that there were at least a few instances of free software that was readily available through the internet and would include options like free audio and video players, including malicious executables.

To avoid this kind of issue, we need to be careful about the kinds of programs that we are allowed onto our systems and be aware of how they could cause some harm to our systems and to us. For example, when downloading something for free from the internet, make sure to check out whether it is legitimate, and whether others have complained about the product and the malicious extensions that come with it.

The final kind of malware threat that we need to take a look at here is going to include APTs or Advanced Persistent Threats. The term doesn't mean a certain kind of technique or type of attack. Instead, it is going to refer us to a persistent and sustained multi-pronged effort of breaking into the data network of an institution or organization.

With these APTs, the hacker is going to utilize a number of attack vectors from the creative to the mundane, and they may even go as far as sending out some fake promotional materials. These can range based on the goal of the hacker and could be something like a free flash drive to someone who is higher up in the organization. When it is used, though, the intention is to give the hacker what they want. The flash drive would be able to upload and install a file that is malicious onto the computer and allow the hacker the access that they want.

These APTs are often going to be used by groups of attackers that aim to get certain information that they want from an organization or another business. These are not short-term, either. Often, these can last at least a few months, and often, into a few years or more.

As we can see here, there are a lot of different types of malware attacks that we need to be careful about on a regular basis. Hackers would love nothing more than to get onto a system they have no access to, whether it is an individual account or the account of a big organization, and then get the financial, personal, and more information from that system. Learning how to recognize the different types of malware and figuring out the best ways to avoid falling prey to it can really go a long way in keeping your system as protected as possible.

Chapter 6: Cyber Attacks

Now that we have a little better idea of what malware is about and how it is going to work, it is time for us to move on to something known as a cyberattack. This is going to be a big issue for businesses and individuals alike, and it is important that we are able to recognize the different ways that a hacker can try to get onto our system and cause issues.

Cyber attacks are going to hit businesses on a regular basis. According to Former Cisco CEO John Chamers, “There are two types of companies: those that have been hacked and those who don’t yet know they have been hacked.” This means that even if you feel like they have never been hacked and that the information they are storing on their systems is safe, it is possible that there is a hacker right now who are either working on getting into your system and going to exploit any vulnerability that maybe there or you actually have a hacker on your system and you just don’t realize it yet.

The truth is that cybercrime is something that is increasing on a yearly basis, and those who use computers all the way up to those who are responsible for protecting a lot of personal and confidential information need to be on the lookout more now than ever. People are working to do these kinds of crimes because they think they can stay hidden, and they want to be able to benefit from it in some way. Often, attackers are going to do this to get some kind of ransom. In fact, 53 percent of the cyber attacks that have happened recently resulted in damages that were $500,000 or more. And many more were for lower amounts.

These cyberthreats can also be launched with a few ulterior motives attached to them, as well. For example, there are some hackers who will do this process as a way to obliterate a system and the data that is on it. They may see this as a form of hacktivism that can help to protect others.

Before we move on with this, though, we need to take a look at one more term that will help us in understanding what is going on with some of this. This term is botnet. This is going to be a network of devices that have been infected with some kind of malicious software, including a virus. Attackers are able to control this botnet or this network as a group, without the knowledge of the owner, with the goal of increasing how strong and powerful their attacks will be in the future.

Often, the hacker wants to do this slowly, and they may contain the botnet for a bit, watching the information and waiting for the right time to strike. But once they decide that it is the right time to strike, the botnet is going to be under the control of the hacker, and the owner of that network will not know. Often, the botnet can be used to help overwhelm the system in a DDoS attack or something similar.

Malware

The first type of cyber attack that we need to watch out for is malware. Malware is a type of malicious software. To put it simply, malware is going to be any kind of software that was written with the intent of damaging devices, stealing data, and causing a mess. Ransomware, spyware, Trojans, and viruses are among the different types of malware that we may have to deal with.

Malware is often something that is going to be created by a team of a hacker, usually when they want to make money by spreading the malware on their own or selling it to the highest bidder on the Dark Web. However, there are times when it is a tool that a hacker uses for protesting, to test out the security of a system, or even as a weapon of war between different types of governments. No matter why or how the malware comes to be, it is never good news when it ends up on your own computer.

First, we need to be able to understand what malware is able to do. Malware is able to do all kinds of things. It is going to be a category that is very broad, and what malware does or how it works is going to change based on the hacker and the file type that they try to use. The following are going to be some of the most common malware types and what they are able to do when they infect a computer or a system:

1. Virus: Like the namesake that they come from, these viruses are able to attach themselves over to some clean files, and then will infect other files that are clean. These have the potential to spread uncontrollably, damaging the core functions of the system, and even deleting or corrupting files. These are often going to appear as a file that is executable.

2. Trojans: This is going to be a malware option that can disguise itself as a legitimate type of software, or it is going to be hidden inside some legitimate software that the hacker has been able to tamper with. It is going to act in a more discreet manner and can create some backdoors into your security, effectively letting in other types of malware in the process.
3. Spyware: This one is going to be a type of malware that is designed to really spy on you. It can hide in the background and then will take notes and information on everything that you do online. It can include your surfing habits, numbers of credit cards, and your passwords.
4. Worms: The malware attack known as a warm is able to infect an entire network of devices, either local or across the internet, with the use of network interfaces. It is going to use each consecutively infected machine to help it infect some more along the way.
5. Ransomware: This is going to be a type of malware that is able to lock down your computer and files and is able to threaten to erase everything unless you come up with a ransom that they want. Often, this is not going to solve the problem, but the hacker still gets the money.
6. Adware: Although this is not always something that is malicious, aggressive advertising software can sometimes undermine the security of your system just to serve you with more ads. And if this continues to happen, it is going to provide malware with an easy method of getting in. Think about pop-ups when it comes to this kind of attack.
7. Botnets: And finally, we can deal with a malware attack that is known as a botnet. These are going to be networks of computers that are already infected that will work together based on the work that the hacker wants them to accomplish.

There are certain types of malware that are going to be easier to detect compared to others. Some like adware and ransomware are going to make their presence known right away, either by encrypting your files or streaming an endless amount of ads to you. You will be able to detect these

right away and can take the necessary actions to help get them off your system and prevent further issues .

Then there are other options, like spyware and Trojans, that are going to go out of their way to hide from you for as long as possible because these are used when the hacker wants to be able to stay on the system for a good deal of time. This means that they will be on the system for days, weeks, and even months, and you have no idea that they are even there.

And then there is the third type. These can include options like worms and viruses that are going to be able to operate and do their job in secrete for some time, and then the symptoms of them being there and the infection they cause start to appear. In these cases, it is likely that we will see some issues like freezing, deleted, or replaced files, the system shutting down suddenly, or a processor that is hyperactive.

The only surefire way that we are able to detect all of this malware before it can infect our computer or our mobile device is to install an anti-malware software, which is going to be packaged with detection tools and scans that are able to catch any of the malware that is already on the device, and then can block off any of the malware that is trying to infect you.

Each form of malware that you encounter is going to come with its own way of damaging and infecting data and computers, which means that each one is going to need a different method of removal. Working with anti-malware software, no matter what kind of computer or operating system you use, can help to keep some of these attacks out.

Phishing

There are times when a hacker is going to use a technique that is known as phishing. This is going to be a type of cybercrime in which the target is contacted by text messages, telephone, or email by someone who is posing as a legitimate institution in order to lure individuals into providing them with sensitive data, such as banking and credit card details, personal information, and passwords for the hackers use.

The hacker wants to do this in order to get as much information from the target as possible. They hope that the target, not paying attention, will hand

over this information, and then the hacker can access any website or another account that they want based on the information that they are provided.

There are a few common features that are going to show up when we look at a phishing email. First, the offer in the email is too good to be true. You may find that these kinds of texts or emails are going to offer lucrative points and a lot of statements that are attention-grabbing. These are basically designed to grab the attention of the target right away. It could be something as simple as saying that you won some big prize if you just Click Here! Make sure that if you receive any of these email types that you do not click on it. If something seems too good to be true, then in all likelihood, it probably is.

Another thing to watch out for with these kinds of attacks is that there is a sense of urgency that is provided inside. A favorite tactic that a lot of cyber criminals like to work with is to ask the target to act fast because the deal is only for a limited amount of time. Often, these types of attacks are only going to give you a few minutes to respond. It is often best to just ignore them and not even open them.

Remember that a reputable company is never going to rush you. If someone is going to close your account, for example, because you haven’t used it in some time, they will give you a month or so to go and check things out and decide if you want to keep it or not. If the email says that you have to act right now, then this is a good sign that you are dealing with a phishing attempt. Never give off the information on this because you will give the hacker exactly what they want, and this could really ruin you financially and more.

Hyperlinks should be another red flag that you are watching out for. A link is not always what it appears, and if we are not careful with the links that we are using, then it could take us somewhere, we do not want to be. Hovering over a link is a good way for us to see where that actual URL is going to take us if we clicked on it .

We always want to double-check when it comes to this kind of thing. Hackers are good at taking a well-known website and then changing just a bit about it, causing us to believe that the website is a safe one. But if we looked a bit closer at it, we would see that there is something wrong and

that this is not really the website that we want to be on. For example, a hacker could take the Bank of America website and change the mover to an r and an n to confuse us, and then send us over to an unsecured website.

If you are not certain whether the website is the correct one or not, it is always best to do your own check. Type in the name of the company you think is emailing you, and go straight to their website without clicking on the link. If they did actually message you for something, you will be able to find it out this way. and if not, you avoided an attack by a hacker.

We also need to be aware of any attachments that are coming in with our emails. If you see an attachment that is in an email that you weren't already expecting to come in, or it doesn't really make sense for that attachment to be there in the email, then never open it! These attachments are going to contain a lot of tools for the hacker like viruses and ransomware, and downloading them can really cause a mess on your computer. The only file that is always safe for you to click on is a .txt file, or if you are actually expecting an attachment from someone in the first place .

And the final thing that we need to look at here when being careful of phishing is the sender. If the sender is unusual, then this is at least an invitation to look a little bit closer at what is going on. Whether it looks like it comes to form someone you don't know or someone you actually do know, if you look through the email and feel that something is out of character, unexpected, out of the ordinary, or makes you suspicious, then it is best to not click on it at all.

Keep in mind with this one that, in most cases, the emails that are sent by these cybercriminals are going to be masked in a way that they appear like they were sent by a business whose services are used by the target or the recipient. A bank and other companies are not going to ask you for some personal information through email or put a suspension on your account if you do not update some of the personal details within a certain period of time. Instead, they will provide the personal details and account number in the email to help you see that it comes from a reliable source.

Man in the Middle

The next type of attack that we are going to take a look at is the man in the middle attack. This is where the malicious user, or the hacker, is going to

insert themselves between two parties in communication, and then will try to impersonate both sides of that exchange. The attacker is then going to intercept, send, and receive data that is meant for either of the two users, including things like passwords and account numbers.

Typically, when there is some communication going on with our computers, the flow is going to occur between the client and the server. So, if you would like to access your own bank account through the website of the bank, then your own computer, which is the client, will send over the needed login information to the servers of the bank. If the bank servers see that this information is right, they will send back verification of a login attempt that was successful, and then you are able to access the account.

Another example of this is when you shop on Amazon. An interaction between the financial institution and the server needs to be created, which will be used to charge your account when making a purchase. In either of the two scenarios, the man in the middle attack is able to come on and change up the flow of this information in a dramatic manner.

A communication relay between the server and the real client will then be established by the malicious user where he can modify and monitor all the communication shared by both people to one another. Instead of the server receiving the information straight from the client, the information will head straight to the malicious user first .

Now, there are a few things that can happen here. Sometimes, the man in the middle attack is just happening so that the hacker can gain some useful information. They may gather the data, look it over, and then send it on its way. This allows them to stick around for some time and learn more about the system before they do any more with the attack. In addition, it is possible for the hacker to take the information and use it for their own needs, such as with username and passwords, or they can alter the information and send it on its way instead.

For example, it is possible that the sender is going to communicate that they would like the receiving bank account number to be 123456789 for a specific transaction. But a hacker who is using the man in the middle attack could intercept that information and change around the bank account number. The account number will be then notified to the bank, and because

they don’t realize that anything is wrong here, they will send the money over to the account the hacker specified, rather than the one the user actually wanted. And often, this is not caught until it is too late.

There are a number of other attacks that can fit in under this kind of category. The man in the middle attack is basically a form of session hijacking. A session is going to be a period of activity that occurs between a user and a server during a specific period of time. For example, each time that you access your own bank account and then interact with it in an active manner, this is a session. When you log out of that account, then this means the session has ended.

Of course, there are actually quite a few other types of attacks that will prey on session hijacking similar to what we are going to see with a man in the middle attack, and these can include some of the following:

1. Sniffing: This is going to entail the hacker using software that can intercept the data being sent from or to the device that you are using.
2. Sidejacking: This kind of attack is where we sniff data packets that are being sent between the client and the server so that the session cookies can be stolen, and we can gain access to a session. These cookies are important to the hacker because they include some unencrypted login information, whether or not the site is secure in the first place.
3. Evil twin: Sometimes, the hacker is going to take this process so far that they create a rogue wireless network that seems to be legitimate. Unknowing users are going to join that network and then use it for a regular activity online without realizing that, during this time, their information is being collected. This often makes it easier for one of the men in the middle attacks to happen.

There are a few things that we can do to make sure this man in the middle attack is less likely to happen to us. On the client-side, there are not as many defenses that we can work with for this attack. Most of the protective measures that happen on the server-side are going to be in the form of strong protocols of encryption between the server and the client. For

example, a server can authenticate itself by presenting a digital certificate, which is basically a verification that allows the client and the server to establish their own encrypted channel for exchanging data. But this only works if the server has these kinds of encryption measures in place in the first place.

From the perspective of the client, the best kind of strategy that we are able to employ is to make sure that we never connect to open wireless routers, or we need to make sure that we use browser plugins like HTTPS.

Denial of Service Attack

Another type of attack that a hacker is able to work with is known as a Denial of Service or DoS attack. This is going to be an intentional type of cyberattack that is carried out on websites, online resources, and networks so that the access that legitimate users have to that source can be restricted. This attack is going to be highly notable, and it could last for as long as the hacker would like. Sometimes, this is just a few hours while they get in and get out with the information they want. And other times, it could last for a few months. For example, one DoS attack that is pretty prevalent on the web right now is known as a DDoS attack, or Distributed Denial of Service.

The DoS attacks are rising because many consumers and businesses are working with more digital platforms in order to transact and communicate with one another. These cyberattacks are going to target digital intellectual property and infrastructures. Often, these are going to be launched in order to steal some of the personally identifiable information that is on that system, which can cause a considerable amount of damage to the finances and the reputation of that business.

Data breaches, for example, are going to attack a certain company or a group of companies in the same period. High-security protocols placed ahead of time by a company could still face an attack through a member of their supply chain if that member does not have the right measures of security in place.

When more than one company is selected by the hacker for this attack, the perpetrators are able to use the Denial of Service attack in order to get onto the system and cause some more trouble before. In the DoS attack, the

hacker is typically going to use just one device and one internet connection in order to send out a rapid and continuous request to the target server. The point of doing this is to overload the bandwidth of the server and cause it to crash .

The hackers of this kind of attack are going to try and exploit the vulnerability of the software in the system, and then they will move on to tire out the server's RAM or CPU if they can. The loss or service's damage done with this attack can be fixed pretty quickly with the help of a firewall and by allowing and deny rules, but it does take a little bit of time to accomplish.

Since this kind of attack is only going to work with one IP address on the part of the hacker, it is easier to fish out this IP address and then deny it further access with the help of the firewall. This makes it easier to stop the DoS attack if you can get the firewall to do its job. However, some kinds of attacks, like this one, for example, can be slightly tougher to detect and stop, and that is known as the Distributed Denial of Service, or DDoS, attack.

When we look at a DDoS attack, it means that the hacker is working with connections and devices infected multiple times, usually ones that are spread all over the world and have been turned into a botnet. This is going to be a network of personal devices that have been compromised by a hacker without the owner of that device having any idea what is going on.

The hacker will infect the computers they want to use. In order for them to have control of the system, they will use some malicious software. They can then send out fake requests and spam to some other servers and devices. If this attack victimizes a target server, they are going to basically experience some overload because hundreds or thousands of phony traffic will hit them, all at the same time.

Because the server is being attacked from many locations, rather than just from one, detecting all of the IP addresses is harder and could prove really difficult. And the firewall has the added issue of separating legitimate traffic from the fake traffic, and the server will find that it is almost impossible to withstand one of these attacks.

Unlike some of the other types of cyberattacks that are initiated in order to steal information that is more sensitive, the initial DDoS attacks are launched in order to make the website inaccessible to legitimate users. However, sometimes, these attacks are more of a screen for other malicious acts. When servers have been successfully knocked down, the culprits may go behind the scenes to dismantle the firewalls of the website, or otherwise weaken the security so that they can continue on with some of the other attack plans that they have.

A DDoS attack can sometimes be used as more of a digital supply chain attack. If the hacker is not able to penetrate and get through the security system of other websites, they can find a weak link that is connected in one way or another to all of the other targets. Then the hacker will choose to attack that link instead of working on the big ones individually. When this link has become compromised, the primary targets would be automatically affected in an indirect manner, as well.

Zero-day Exploit

The last type of attack that we are going to take a look at is known as the zero-day exploit or the zero-day vulnerability. This is going to be a vulnerability that happens in software security, that the software vendor does know about, but they do not have a patch in place at the time to fix the flaw. This means that it has some potential for a cybercriminal to use and make a mess with.

In the world of cybersecurity, these vulnerabilities are going to be the unintended flaws that are found in our programs or the operating systems. These can be a result of improper computer or security configurations, and sometimes, they are just a programming error. If it is not handled, then these are going to cause some holes in security that a cybercriminal is more than happy to exploit.

These are going to pose a big security risk to someone who is using that program or operating system. Hackers are going to write out some code that is meant to target the specific weakness insecurity that is there. Then they can package it into malware that is called a zero-day exploit. The malicious software that is designed here is set up to take advantage, as much as possible, of the vulnerability to compromise a computer system or cause

some other behavior that is unintended. In most cases, if the company is able to make a patch for the vulnerability, then the attack will be stopped.

But then, we have to worry about what will happen if your computer is one of the options that gets infected? This kind of malware is able to steal your data, allowing the hacker to get any control over the system as they would like. The software that is on your computer can also sometimes be used in a way that it was not intended in the beginning, like installing other malware that will corrupt files or access your contact list to send out spam messages to anyone on the account. It could also install some spyware that steals sensitive information from the computer. Basically, if the hacker is able to get through one of these vulnerabilities before a patch is designed for it, then they can do whatever they want on your system.

The term zero-day refers to a newly discovered vulnerability in the software. Because the developer has already learned about the flaw, it also means that an official patch or an update to fix the issues hasn't had time to be released. So, the idea of zero-day is going to refer to the fact that the developers have zero days to fix the problem that they have just been exposed, and that hackers are already exploiting it. Once the vulnerability is known by the public, it is the job of the vendor to work as quickly as possible to fix this issue and make sure that the users are protected.

Keep in mind that because the vulnerability is already found, it is likely that the software vendor is not going to release a patch before the hackers are able to exploit the hole in security. This turns it into a zero-day attack, and many users of that software could be at risk. The best thing that you can do here is to make sure that you stay protected against these zero-day vulnerabilities. These can present a big security risk that would leave you susceptible to a lot of things, including damage to your personal data and your personal information.

To make sure that your data and your computer are safe, it is best to take reactive and proactive security measures. The first line of defense that you can rely on is going to be being proactive by using comprehensive security software any time that you can. This can help make sure that you are protected against known and unknown threats all of the time. Then the second line of defense is known as reactive, and it is going to be when we immediately install some new updates for new software whenever they

become available form the manufacturer. This helps us to reduce the risk that we will be harmed by a malware infection.

The right software update is going to help us install all of the necessary revisions to the operating system or software. These could include things like adding in some new features, removing any features that are outdated, updating the drivers, delivering fixes to some bugs in the system, and even fixing some of the security holes that we have discovered.

However, there are a few other steps that we are able to take to make sure we don't become caught with one of these zero-day attacks. These steps are going to include:

1. Keep your security patches and all of your software up to date as much as possible. You can do this by downloading the software releases and updates. When you add in the security patches as they come up, it helps to fix any bugs that an older version of the software may have missed at some time.
2. Establish some safe and effective personal online security habits at any time that you get online.
3. Configure the settings for security on your operating system, your security software, and your internet browser.
4. Make sure that you install comprehensive and proactive security software that is going to help us block the known and unknown threats and vulnerabilities on your system.

As we can see here, a hacker has a lot of tools in their arsenal when it is time for them to get online and try to take your personal information, or even when they would like to hijack your system and your network for their own personal gain. Recognizing some of these attacks and looking at some of the steps that you can take in order to avoid these attacks and keep your data and personal information safe can make a big difference in the results that you will get.

Chapter 7: How to Scan the Servers and the Network

One thing that we need to spend some time on while we are here is how we can scan our servers and the network that we are on. This may seem like a waste of time, shouldn't we already know all the ports and systems and devices that are on our network? But surprisingly, a lot of professionals have no idea what is all on their network. Even if you do, this also means that you can take the time to ensure that no unauthorized users are on the system, and allows you a chance to kick them off if they are there. Let's take a look at some of the steps that we can take to help us scan the servers and the network, and make sure that everything is safe and sound as it should be:

Getting Started

We need to make sure that we take the time to look through our system, and think like a hacker. Where would they be most likely to come onto the network and try to cause trouble? What information would the hacker be the most interested in the gathering if they would like to get ahold of if they could? Some of the other questions that you can answer when it is time to get started with your own network scan to help you direct your activities include:

- If someone tried to make an attack on the system, which part would end up causing the most trouble or which part would end up being really hard if you lost the information on it?
- If you had a system attack, which part of the system is the most vulnerable; therefore, the one that your hacker is most likely to use.
- Are there any parts of the system that are not documented that well or which are barely checked? Are there even some that are there that aren't familiar to you (or you haven't even seen in the past)?

With these questions answered and a good idea of where you would like to take this process, and a good list started on some of the applications and

systems that you are most interested in running, it is time to go through the steps to make sure that all the parts of your system are covered. We want to run these tests on all of the parts inside of our computer, double-checking that it is all safe. Some of the different parts of this process that we need to remember will include the following:

- Your routers and your switches
- Anything that is connected to the system. This would include things like tablets, workstations, and laptops.
- All of the operating systems, including the server and the client ones.
- The web servers, the applications, and the database.
- Make sure that the firewalls are all in place.
- The email, file, and print servers.

You are going to run a lot of different tests during this process, but this is going to ensure that you check through everything on the system and find the vulnerabilities that are there. The more devices and systems that you need to check, the more time it is going to take to organize the project. You are able to make some changes to the list and just pick the options that you think are the most important in order to save some time and keep your system safe.

What Can Others See With my System?

One thing that we need to consider when going through this whole process is what others can see when they look into the company. Hopefully, your security is pretty good at this point, and they are only going to see some of the basics, like your website and the financial information that is required. But you want to make sure that there is nothing else about your system or network that is showing that others can easily reach.

Any hacker who tries to get onto your system is going to spend time researching your network and system and seeing where the vulnerabilities may be. If you are the owner of this system, you may miss out on some of these more obvious parts, so it is important to take a look at these with a brand new angle. There are a few options that we are able to use when we

want to gather up information on our own network, but the first place to go here is an online search.

To do this, we just need to do an online search about the business or the individual and see what information is out there that relates back to us. You can then work on completing a probe to find out what someone else will be able to see with your system. Sometimes, a local port scanner can help out as well. Keep in mind that this internet search doesn't have to be that complex, but you can delve in and actually look so that you don't miss out on some of the things that are getting sent out to the world through your computer. Some of the things that you need to focus on the finding of your system include the following:

- Any contact information that will let someone else see who is connected with the business. Some of the good places to check out include USSearch, ZabaSearch, and ChoicePoint.
- Look through any press releases that talk about major changes in the company.
- Any of the acquisitions or mergers that have come around for the company.
- SEC documents that are available.
- Any of the patents or trademarks that are owned by the company.
- The incorporation filings that are often with the SEC, but in some cases, they can be in other locations as well.

This is a lot of information to look for, but it can be valuable to a hacker, and you need to be able to determine how much is available out there for the hacker to use. A keyword search will not cut it; you need to go even deeper and do some advanced searches in order to find this information. Take the time to write out some of this information so that you have a better idea of how big the network is, what information is being let out to the public, and other vulnerabilities that may harm your network.

How to Map Out the Network

Once we have been able to complete all of the information from before, and we can start a bit of our research as well, it is time to start the actual process of an ethical hack. Your system or network is going to have a lot of

information and devices on it, and we need to make sure that it is protected, even when there are a ton of users on the system as well. The devices must be secure, and all employees have to be held to higher standards to ensure they don't use the network and any devices in an improper manner.

For this point, we need to be able to create a map of the network that we control. The reason for this is to see what all is included in the network and better see, usually in a visual form, where all of the issues could end up being in the system. This is also a good way for us to see what footprint our network or system is leaving behind it online for others, including hackers, to take a look at and exploit for their own needs as well.

A good place to help us get started with this is the Whois option. This was actually a site that was originally designed to help us figure out whether a domain name was open to using, but it is also a great place to start if you want to see what information is on the registration of any domain name. If you go through here and do a search, and you see that your own domain name shows up, it shows that personal information about you and the company, including names of individuals who run the company and email addresses, are being broadcasted at least through this site, if nowhere else.

Whois is able to provide information about all the DNS servers found on a particular domain as well as a bit of the information about your tech support that the service provider uses. One place that you really need to look is in the DNSstuf so that you can find out a lot of the information that is shown about your domain name including:

- The information about how the host is able to handle all the emails for this particular name.
- Where all of the hosts are located
- Some of the general information that can be useful to a hacker about the registration for the domain.
- Information about whether this has a spam host with it.

This is just one of the sites that you can visit to find out some of this information, and it is a good idea to check out a few of these. This helps to give a good start on the information that may be out online for your domain and your company, but there are a few other places that you should check out including:

In addition to working with the Whois option above, it is possible to take a look through Google Forums and Groups, and some other similar options. These are going to be helpful for hackers because there is a ton of information that can be posted about your business or network on these forums and more, even though you were not the one who went through and posted the information.

Depending on the kind of information that someone else went and posted on here for others to see, there could be issues of security that you need to focus on and learn more about. Sometimes, if a hacker has already been on your network and wants to sell the information to others, it is possible that things like your IP address, domain name, and usernames will be on the site. A simple search of your own domain name or company name is often enough to figure out whether there are any security issues present on the site .

The good news with this one is that if you are in one of these forums and you find that your security information is there, it is possible to go through and remove that information before more people find out about it and use it to their advantage. You have to show how the domain or business is yours, with the right credentials, but this shouldn't be a problem if you are doing this kind of scan. You can then go into the area for the support personnel on these sites and file your own report to get that information removed as quickly as possible.

Completing the Scan

As we are working through some of the steps that have been listed above, we have to remember that the main goal with that is to find out how much of our system or network is already available online in order to get a better picture on where the hacker could look in order to start up with one of their own attacks. Of course, this is a process that is not easy and can take some time to accomplish. Hackers do not give up easily, and they are determined to get on the system. Your job is to catch them and get to the vulnerabilities before they do to stop any of the chaos that they may try.

Now that we have gone through some of the other steps and we have the necessary information, it is time for us as ethical hackers to complete a few more steps to ensure the network is closed off and that the vulnerabilities

are handled. And we are able to do all of that with the help of a scan over the whole network ahead of time.

These scans are useful because they are going to show us a few of the vulnerabilities that are in our system, which makes it easier to know where to start when we want to protect the network. Some of the different scans that ethical hackers can consider doing to keep their information safe and sound includes the following:

1. Visit Whois like we talked about above and then look at the hostnames and the IP addresses. See how they are laid out on this site, and you can also take the time to verify the information that is on there.
2. Now, it is time to scan some of your internal hosts so that you can see what users are able to access the system. It is possible that the hacker could come from within the network, or they can get some of the credentials to get on from an employee who is not careful, so make sure that everyone has the right credentials based on where they are in the company.
3. The next thing that you will need to do is check out the ping utility of the system. Sometimes, a third-party utility will help with this so that you can get more than one address to ping at a time. SuperScan is a great option to use. You can also visit the site www.whatismyip.com if you are unsure about the name of your gateway IP address.
4. And finally, you need to do an outside scan of your system with the help of all the ports that are open. You can open up the SuperScan again and then check out what someone else may be able to see on the network with the help of Wireshark.

These scans are all great to help you to find out what your IP address is sending out online and what hackers may be seeing when they try to get onto your system. A hacker can basically do some of the same steps that you just did on the system to get in and see what is going on to see the emails that are being passed back and forth, and even learn how to get the right information to have remote access. The point of these scans is to find

out where the hacker can get in so you can close them up and keeping the system safe.

Once we have taken the time to get a good idea of how a hacker is able to get into our network, it is often much easier to learn the exact way that any hacker is going to try and target that network or the computer. Keep in mind that the hacker does not want to work any harder than they have to, so they are going to stick with the easiest method available, while still keeping themselves hidden on the system. Sometimes, it is the first thing that you try, and sometimes, you have to try a few things to keep the hacker out.

These scans are important, and they are something that we need to keep doing on a regular basis. It is not enough for us to just do the scan ones and then call it good forever. As you start to use the network and maybe even grow it out a bit more over time, the information that is sent out is going to change, and hackers are always going to find some of those vulnerabilities. Performing these scans regularly, based on the schedule that is good for your business and IT professionals, can help to keep out all of the hackers who do not belong there.

Chapter 8: The Basics of Web Security

The next topic that we need to take a look at is our web security. If we are not careful when we work online and visit a variety of websites, then we are setting ourselves up for a big attack. Hackers have a lot of different methods that they can utilize when it comes to being online and on a variety of websites. And if the unsuspecting user is not careful with what is going on around them, it is likely that they will invite the hacker right into your system.

Websites are going to be prone to a lot of security risks, As are any networks that are connected to a web server. Setting aside some of the risks that come about because of employee use or because the network resources are being misused, your web server, and the site it hosts presents your most serious sources of security risk.

Web servers are going to, by design, open up a window that links between your network and the world. The care that is taken with the maintenance of the server, web application updates, and your web site coding will define the size that we see with this window and can limit the amount and kind of information that is able to pass through the window. If it is coded the proper manner and is set up the way that you would like, then it is going to help us have some web security that you will have when going online .

Web security is going to be more relative and has two components to it, including one that is public and one that is internal. Your relative security is going to be high if you already have a few network resources that are higher in financial value, your company and site do not present anything controversial in any manner, and your network has had some tight permissions put on it. Add in that the webserver is all patched up to date with all of the settings done in the right manner, your applications on the webserver are all patched and updated, and the web site code is done to high standards, and you have a secure network.

You can imagine that keeping up with all of this is going to be a bit tough, and it may not prove to give you all of the results that you are looking for. If one of these fails a little bit, or you end up with someone in the system who is not careful with the way that they behave online, then your security is going to end up being a little bit lower.

In addition, you will see that there are a few factors that are going to show us that web security is relatively lower for your company. Some of the issues that we need to take a look at here when it comes to seeing our web security lower than normal include:

1. The company has a lot of important financial assets that it holds onto. This could include lots of information on credit card numbers or information on the identity of customers.
2. If the content on your website or with your network is more controversial.
3. If your servers, applications, and site code are more complex or if it is older and if these are maintained by an outsourced IT department or one that is not getting the funding that it needs.

Keep in mind that all IT departments are going to be challenged when it comes to the budget department, so this can be hard to handle for a lot of companies. Tight staffing can sometimes cause us to have deferred maintenance issues that play into the hands of the hacker who would like to challenge the web security that you are working with.

If you have any assets that are valuable, or if there is anything about your business or site that could put you into the spotlight with the public, then it is likely that hackers are going to work with testing your web security. We hope that the information provided here is going to prevent you and your company from having one of these hackers get onto the system and can prevent your business from becoming embarrassed in the process.

One of the things that can cause a big security issue is software that has been written poorly. The number of bugs that are able to create issues with web security is going to be directly proportional to the size and the complexity of the webserver and applications that you have on your network. What this means is that all of the complex programs that are written are going to come either bugs in them, or they will have some other kind of weakness in the process.

On top of all of this, web servers are already seen as complex programs in the way that they are used. Websites, on their own, are complex, and they can often intentionally invite more interaction with the public just by how they are designed. Because of the way that these things work, and how the

company wants their network to be used, it is leaving a lot of security holes in the process, and the opportunities for a hacker can be many.

The issue that technically comes up here is that the same programming that is going to work to increase the value of our website, which is namely that we want it to interact with visitors, is also going to allow SQL commands and scripts to be executed on the database and the web servers in response to the requests of the visitors. Any web-based form or script that is installed on the site could potentially have some weaknesses or even bugs, and each of these, which could be many in a complex system, can present us with a big risk to our web security overall .

Contrary to some of the common knowledge about the balance between allowing visitors to the website, some access to your corporate resources, and keeping visitors out of the network proves to be a really delicate task. There is no one setting or even one single switch that will help to get the security at the right level automatically to handle all of this. There are dozens, and even hundreds, of these settings in a web server on their own, and then each of these services, applications, and open ports can add in a new layer as well. And then we can add in the code to the website, and before long, we see where the complexity is going to come into play.

Some companies are even going to add in some of the different permissions that they want to add into the system to grant employees, partners, customers, prospects, visitors to the system, and the variables that come with this web security goes through the roof.

As you can see right here, there are a lot of potential problems where there could be a lot of web security issues. And the more layers that you add on, the more interaction that you want, and the more permissions that you try to add to the system, the worse this whole thing can get. These add in the potential for bugs and more security holes, and if you do not have a good IT department on top of it, it becomes easier for the hackers to gain access and do whatever they want on the system .

Now, one of the best defenses that you can use when it is time to protect against the various attacks that a hacker can use against your website is to make sure that you do a regular scan to the setup domain. This needs to occur on a regular basis to make sure any bugs, holes, and vulnerabilities

are found, and to ensure that a hacker has not been able to sneak past things and figure out how to get on your website.

Testing the website, which can also be known as the process of auditing or scanning, is going to be a hosted service that a lot of companies can offer. There are many that will not provide us with any installation of the hardware and software, and businesses are able to use this in order to check out the security of the process and the web site, without interrupting the use of the web site for other users.

Being careful with how you manage your web page and all of the different parts that come with it can be important as well. When you make sure that a regular scan is done and ensure that you are not releasing any information that is potentially incriminating against your company, you will find that it is so much harder for a hacker to gain the access that they want to your system and it makes things so much easier for you to keep your information and the information of your customers as safe and secure as possible .

With so much of our world happening online and the fact that a lot of companies are reaching their customers through web sites and other online means, it is not surprising that hackers are moving to this realm as well. If you are not providing your customers with the security that they desire, and you don’t cover up some of the holes and other issues that can be present in your system, then it is likely customers are going to get taken advantage of and harmed in the process.

For example, maybe you have an online retail store that you sell your products through. When a customer makes a purchase, they have to provide you with their name, address, credit card information, and sometimes, some other important information along the way. This is done so that you can finish up the transaction and get the results that you want of selling the product, and they can get the product.

But what happens to that information from the customer when the transaction is done? Your company is likely storing it on a database, but if there is not the right kind of security present, then a hacker is definitely going to want to gather all of that information and use it for their own needs. If you just leave it alone and do not take care of it, and your business

starts to grow, it won’t take long for a hacker to find that information and use it .

When customers find out that their information has been stolen, usually because the hacker tried to steal their money and commit other types of fraud, then what will happen to your business? There will be a lot of backlashes, it is not going to end well at all for you, and your reputation will be shot in no time. As we can see here, it is much better for you to take a step back and make sure that your web security is as organized and high class as possible, ensuring that the hackers are not able to steal that information.

As more of our information goes online, and we get more familiar with talking to our customers and others online, the idea of web security is just going to grow and become more important. Taking care of the web security that you have and ensuring that you are able to keep all of the information on your network safe, whether it is your own personal information or the customer's information, prevent the hackers from getting what they want.

Chapter 9: Understanding your Firewall

During this guidebook, we have spent a bit of time talking about security and how important it is to the overall process of protecting your system and your network. We also took a bit of time to talk about a firewall and how it is so important for helping you to protect against some of the big hacks and attacks that could come at you. Now, it is time for us to take this a bit further and try to see a bit more about what this firewall is and how we can use it, whether on a big network or on our own individual network, to really make sure that we are protected against all kinds of hackers.

To start with, a firewall is going to be a security-conscious router that is going to be there, sitting between the internet and your network with a single-minded task in mind. And this task is to prevent hackers and others from getting in. The firewall is going to act kind of like a great security guard between the internet and your LAN, or local area network. All of the traffic that goes into and then out of this LAN needs to pass through the firewall that you install, which is one of the best ways to help us prevent some unauthorized access to the network that we don’t want there.

One thing to remember here is that some of the types of firewalls that are out there are considered must-haves if your network has a connection to the internet. This matters whether the connection is considered broadband or some other high-speed connection. Without this firewall, you are putting yourself up for a lot of risks because, at some point, whether it is now or at a later time, a hacker is going to discover you. They will see that your network is not protected, will get in and do what they want, and even tell their friends about this. If you want to see a network get toasted in just a few hours, then go ahead and work online without a good firewall in place.

The good news here is that there are two methods that we can use when it is time to set up a firewall. The easiest way that we can use is to purchase a firewall appliance. This is basically going to be a self-contained router that has some built-in features of the firewall. Most of the appliances that include this are going to also have an interface that is web-based. This means that we are able to connect this particular firewall from any of the computers on our network, with the help of a browser. You can then go through all of the settings and customize them for the needs that you have.

That is the first method, but there is also another method that can come in handy when you want to set up your own firewall. For example, you are able to set up your own server computer in order to function just like a firewall computer. You are able to run the server on just about any of the operating systems in the network, but keep in mind that one of the most dedicated firewall systems will run with the Linux operating system.

Whether you choose to protect your network with a firewall computer or a firewall appliance or a firewall computer, the firewall has to be located at a point between the network you are using, and the internet if you would like it to be successful at all.

Types of Firewalls to Use

The next thing that we need to take a look at here is the different types of firewalls that are available. There are a few options, but the three basic types that we are going to focus on are known as the application layer, stateful, and packet filtering, or stateless.

First is the packet filtering or the stateless type of firewall. These firewalls are going to work because they can stop and inspect the individual packets all in isolation. Because of this, they are unaware of the connection state, and they have the ability to deny or allow packets based on the packet headers that they receive, regardless of the origin of that packet.

Then we have the stateful firewalls that we can work with. These are a bit different because they can show us the connection state of our packets, which is going to add in a bit more flexibility than what we can see with the stateless firewalls. These firewalls are going to work by collecting the related packets until it is able to determine the connection state. Then, when it figures this out, it is able to apply all of the rules that the firewall has to that kind of traffic.

And finally, the third type of firewall that we can work with is the application firewall. These are going to take us another step on the journey by analyzing any of the data that we are seeing transmitted. This allows us to match up the traffic of the network against the rules of the firewall that are specific to individual applications or services. These are also going to be known as proxy-based firewalls.

In addition to some of the software that we just talked about with firewalls, which are available on all of the operating systems that are used right now, the functionality of the firewall can also be provided with a few hardware devices. We can see this with firewall appliances and even some routers. We are going to spend a lot of time here talking about the stateful software firewalls that are available, and that run on any server that they intend to protect, but realize that some of the others are important as well.

Firewall Rules

As we mentioned a bit above, the traffic on a network that gets to a firewall is going to be matched against some of the rules of that firewall in order to determine whether or not that traffic can be let through or not. An easy way to explain what these rules look like is to show a few examples, and we are going to do that below.

For this first one, let's suppose that we have a server with a list of rules for the firewall that applies to all of the incoming traffic. Some examples of the rules that we could have present include:

1. It can accept new and established incoming traffic to the public network interface on port 80 and 443. These are going to include options like HTTPS and HTTP web traffic.
2. It can drop all of the incoming traffic that is coming from any IP address that is a non-technical employee to the office, and it can do this through the port 22 or the SSH port.
3. It can accept any of the new and established traffic from the office range of IP to the private interface network on port 22 or the SSH port.

Note that the first words of all of these rules will have something like accept, reject, or drop associated with them. This is going to specify the action that we want the firewall should do when an event happens. When some kind of traffic happens and matches one of the rules, then the firewall is going to know what it needs to do .

For example, when we set up a rule to Accept, it means that the firewall needs to let the traffic through. When we set up a rule for Reject, it means that the firewall is going to block the traffic but will reply to that traffic with an error about being unreachable. And when we work with a Drop rule, then it means that the firewall needs to block the traffic without sending any reply at all. The rest of each rule is going to be responsible for consisting of the condition that each packet is going to be matched against.

As it turns out, the network traffic is going to be matched against the list of rules that have been set up with your firewall in a chain or a sequence, from the first to last. To be more specific with this, once a rule has been matched on this process, the associated action is going to be applied to the network traffic that is trying to come through, and then the firewall will be able to determine, based on the different rules that you set up with it, whether to allow the information or the traffic to come through at all.

When we look at an example, if we have an accounting employee that has attempted to establish an SSH connection to our server, then the firewall would reject them because of the second rule that we have. And since the second rule is able to reject it, the connection or the traffic is not going to be checked at all. But the system administrator would be accepted because they are only going to match the third rule .

One thing to keep in mind here is that for the typical chain of firewall rules to not be able to cover all of the possible conditions that are out there. There are a ton of different changes that are going to come up over time, and often, the results that your firewall has to sort through are going to be ever-changing as well. For this reason, the chains in your firewall must have a default policy that is specified from the beginning, which is just going to consist of a single action.

So, let’s say that you set up a firewall, and the default policy on it for the example chain that we have above was set for it to drop the traffic. So, if there is any kind of computer that tries to get into your office and establish an SSH connection to the server, but that computer is outside of your office, then the traffic would be dropped. That outside computer is not going to match any of the three rules that we had above, so it is going to be dropped right away.

Now, we can also choose to set up our default policy so that it is at Accept. This means that anyone, except your own non-technical employees, would be able to get onto the connection and establish themselves there to any of the open services that are on the server. This would be an example of a firewall that is not configured well because it is only going to keep out some of your employees, and anyone else who wanted to be there, even a hacker, could easily find their own way onto the server .

Watching the Incoming and the Outgoing Traffic

As network traffic, when we look at it from the perspective of the server, can either be incoming or outgoing, the firewall is going to maintain a set of rules that will be distinct for either case. Traffic that is able to originate from elsewhere, incoming traffic, is going to be treated in a different manner than what we see with outgoing traffic that your server, or your own system, is sending out. You are not in harm from sending out your own information. But you could be in danger when there is something new coming into the system, so the firewall is going to handle each of these in a different manner.

It is pretty common for a server to allow most of the outgoing traffic that you try to send to other locations, mainly because it tends to find itself trustworthy. Still, we still want to make sure that there are some outgoing rules in place in order to prevent unwanted communication in the case that a server is compromised by a malicious executable or an attacker in that manner as well.

To help us to get the maximum out of our security benefits with the help of a firewall, we need to identify all of the ways that you would like to have other systems interact with yourself. How to create rules that explicitly allow them, then drop all of the other traffic. We must keep in mind with this one that some of the appropriate outgoing rules have to be in place to make sure that the server is able to allow itself to send any outgoing acknowledgments to the incoming connections as you choose.

Another thing to remember here is that since the server is typically going to need to be the one to initiate its own outgoing traffic for a lot of different reasons, including downloading updates or connecting back to the database,

it is important that we can include those cases in the outgoing rule set as well.

From here, we are able to write some of our own outgoing rules. Let's say that we are going to set up a firewall that is going to drop the outgoing traffic, and this is our default. This means that the incoming accept rules would be useless without having the right outgoing rules in place. To help complement the incoming firewall rules (which were 1 and 3 from above), from the Firewall Rules section above, and to make sure that there is an adequate and proper amount of communication on those addresses and for the ports to work correctly, some of the outgoing rules that we may want to set up for the firewall could include the following:

1. Accept the established outgoing traffic that comes to the public network interface using port 90 and 443.
2. Accept established outgoing traffic to the private network on port 22.

Note, with this one, that we are not required and it is not needed for us to write out a rule for incoming traffic that needs to be dropped (this was the rule 2 in the previous section) because the server isn't going to need to establish or even acknowledge this kind of connection.

Having a good firewall in place is going to be very important when it comes to keeping your network and your system as safe as possible. It can set up the rules about what is allowed on the system, and what needs to be kept out of the system from the beginning. Without the right firewall protection in place, it is possible that anyone, and any hacker, is going to be able to get into your system and cause the chaos and havoc that they would like. Pick out a good firewall and ensure that you can set up the rules that work the best for your system and the security that you would like to have overall.

Chapter 10: Understanding Cryptography

The final chapter that we are going to talk about when working in this guidebook is the idea of cryptography. If we want to make sure that the messages we send and the ones we receive are kept secure and safe from others, then we need to make sure that we can add in some level of cryptography to the mix as much as possible. Cryptography is going to be the method of protecting information and communications through the use of codes. The point of doing this is so that only those who are intended to see the message are the ones that can read it in the end.

The point of this is that we want to make sure that the information is kept secret. Whether this is just an email that you want to send to someone else, or it is secure information that you want to keep hidden from others, this cryptography can make sure that hackers and others who may be performing man-in-the-middle attacks and more are kept out of your system and will not cause some issues along the way.

When we are looking at it through the lens of computer science, this cryptography is going to refer to secure information and communication techniques that are going to be derived from a variety of mathematical concepts and a set of rule-based calculations

Techniques of Cryptography

We need to start off with some of the different techniques that we are able to use when it comes to adding some cryptography to our system and the messages that we try to send. Cryptography is going to be related pretty closely to the ideas of cryptanalysis and cryptology. It is going to include techniques like microdots, merging words with images, and other methods that are meant to help us hide our information in storage, or in transit, so that no one else without the right authorization is able to get ahold of that message.

However, when we look at the world and how it is today, and all of the computers and digital stuff that is going on with it right now, cryptography is more likely to be associated with scrambling plaintext (which is going to be ordinary text) into ciphertext in a process that is known as encryption.

Then, when the messages get to the right person, then it is going to go back into regular or plaintext again in a process known as decryption. Individuals who are able to practice this field are known as cryptographers .

Now, there are going to be four main objectives or concerns that come with the process of cryptography, and these will include the following:

1. Confidentiality: This is where we try to make sure that the information isn't understood by anyone for whom it was not intended. When we work with cryptography, we are relying on codes and other processes to keep our messages and our information safe until it reaches the intended person.
2. Integrity: Cryptography worries about whether the information is altered during the storage or the transit. The goal here is to not allow the information to be altered in either of these two processes between the sender and the person who is supposed to receive the message, and if this alteration does happen, it is detected right away.
3. Non-repudiation: This is where the creator or the sender of the information is not able to deny, at a later stage, what their intentions are in the creation of the transmission of the information when things are all done.
4. Authentication: This is where the sender and the receiver are able to confirm the identity of one another, and the origin or the destination of the message or the information.

When we have a protocol or a procedure that is able to meet at least some, but hopefully all, of the criteria above, then we have something that is known as a cryptosystem. These are often thought to refer just to mathematical procedures and some of the programs that we can make on our computer. However, they are also going to include some regulation of human behavior, such as choosing passwords that are hard to guess, logging off when the system is not in use, and not discussing any procedure that may be sensitive to the business with someone who doesn't need to know the information.

Algorithms with Cryptography

As we are working with cryptography, it is important that we take a moment to talk about some of the algorithms that come with this kind of process. Cryptosystems are going to use a set of procedures, which are the algorithms, to help us to encrypt and decrypt messages that are sent between a few systems. The point here is to make sure that the communication that is shared among the computer systems are going to be as secure as possible. This works not only on computer systems but also on applications and other devices like tablets and smartphones.

A cipher suite, or the algorithm, is going to use one algorithm to help us with the encryption part of the process, another for helping to message the authentication, and then the final key to finish up the exchange that is happening. This process, which is going to be embedded in protocols and then written in the software that runs on the operating systems and the networked computer systems, needs to have two keys generated in order to be successful.

With this, we have to make sure that there are a private key and a public key that is generated to do all of the work that you would like in this process. Some of the ways that we are able to use these two keys for include data decryption and encryption, digital signing, and verification for authentication of the message can all be important, as is the exchange of the key.

Types of Cryptography

While we are here, we need to spend some time taking a look at the different types of cryptography that are available. To start, the single-key or the symmetric key algorithms of encryption are going to create for us a fixed length of bits known as a block cipher. This one is going to contain a special key that the creator or the sender will use to help them encipher or encrypt the data. Then the receiver will get this key and can use that to help them decipher the information they have.

There are a lot of different types of symmetric-key cryptography, and one of these is going to include the AES or Advanced Encryption Standard. AES because a specification established in 2001 by the National Institute of Standards and Technology as the Federal Information Processing Standard, and it was used to help protect any information that was considered

sensitive. The standard is mandated for use with the US government, and many of those in the private sector will use it as well to help them get things done and stay safe.

In addition, a few years later, in 2003, the AES was approved to be used in the information that was classified by the US government. Right now, it is a specification that is free of royalties and is implemented in software and hardware throughout the world. This is actually the successor to the DES or the Data Encryption Standard that would work with longer key lengths and could prevent things like brute force attacks.

Then there are also options for asymmetric or public-key encryption algorithms. These are a bit different because they are going to use a pair of keys instead of just one. There is going to be a key that is the public one, and this is associated with the sender or the creator for encrypting messages. Then there is also the private key, the one that only the originator is going to know (unless a hacker can get in and expose this key or the originator decides to share the information), for helping them to decrypt their information.

There are a number of public-key cryptography options including RSA, which is used often on the internet to keep things safe, Elliptic Curve Digital Signature Algorithm which is used with Bitcoin and other cryptocurrencies, Digital Signature Algorithm which was used as a standard for digital signatures, and the Diffie-Hellman key exchange.

To help make sure that the integrity of the data is maintained in cryptography, functions, which are able to return to us a deterministic output from the input value, are going to be used to help us map up all of the data to fixed data size. This is going to make sure that your information is able to stay as safe and sound as possible, and makes it easier for you to send and receive messages, without a hacker being able to get in the middle and cause a mess.

How did Cryptography Start?

The next thing that we need to take a look at here is the history of cryptography and how it got started. The word “cryptography” is actually from a Greek word known as kryptos, meaning hidden. The origin of this is dated from about 2000 B.C. with the Egyptian practice of the hieroglyphics.

These were consistent with complex pictograms, the full meaning of which was really only known by a few people.

In more recent times, cryptography has turned into a kind of battleground of some of the world's best mathematicians and computer scientists working to come up with the best code. The ability to store and transfer, in a secure manner, any sensitive information that is needed has been such a critical factor in business, and sometimes, in war as well .

Because governments do not wish for certain entities in and out of their countries to have access to the different methods of receiving and sending information that could be secret and could hold a threat to national interests, it is no wonder that cryptography has been a big subject to restrictions in different countries. This can include some limitations of the export and usage of the software to the public and more.

Of course, the way that cryptography is being used is different now than what it has been in the past. Many times, we are going to see this kind of cryptography in any transaction where the information needs to be kept secure. While it is used in government quite a bit, it can show up with the banks that we use and many of the transactions that occur online when we make purchases. The point is to allow us to send some personal and confidential information to another person or business, without the risk of having someone take it over and use the data for their own needs.

Concerns with Cryptography

Attackers are able to circumvent some of the cryptography on occasion. And when they are able to do this, it allows them to hack into computers that are responsible for doing the encryption and the decryption of the data to start with. The hacker, once they are there, is able to exploit some of the weaker implementations that are there, such as using the default keys to help them out .

It is true, though, that this cryptography is going to make it harder for an attacker to access the messages and any data that is protected by the algorithms of encryption. This is why it is so important to add this to your system. It may not be able to keep everything out all of the time, especially with a really skilled hacker. But it can make things more difficult and can solve a lot of problems for you in the process.

Growing concerns come with the processing power of quantum computing to break through some of the current encryption standards for cryptography led by the National Institute of Standards and Technology. This is meant to pull out a call for papers about the community for science and mathematical for new standards on cryptography. If some standards were decided ahead of time, it would make life easier for most companies and would ensure that they know the minimum that they could expect when using one of these services.

Unlike today's systems for computers, quantum computing is going to use what is known as quantum bits that are able to represent both the 1s and the 0s. Because of this, it is able to get two calculations completed in one. While a large-scale version of this kind of computer is not something that will likely be done in the next decade, the infrastructure requires standardization of publicly known and understood algorithms that can offer us a secure approach .

If you want to make sure that your messages and your information are as safe and as secure as possible, it is important for us to make sure that some form of cryptography is in place early on. The Kali Linux system will be able to help us out with this and will ensure that we can really see how safe and secure our own messages can be, even when we have to send things off the network in the first place.

Without this cryptography being in place, it is possible for a hacker to come into your system and steal the messages that are there. With the proper type of cryptography and the help of the Linux system, it is easier for individuals and companies to hide their information and to send secure messages back and forth with less chance of someone being able to intercept the information and read what is there.

Conclusion

Hacking is a term that many people are not that familiar with. They may have heard about hacking when it happened to a big corporation, and maybe, they have an antivirus on their computer to keep out those who may try to cause harm to their systems, but they are uncertain about all of the different types of hacking available, or even that there are different types of hackers. This guidebook attempted to go through all of the different aspects that we needed to know about hacking so that we can keep our own networks and systems safe from those with malicious intentions.

This guidebook spent a lot of time talking about the different types of hacking, how to prepare for an attack, and some tips on how to keep your computer and networks safe. We took a look at this from a more ethical standpoint, but realize that the techniques and skills that an ethical hacker will use are similar to identical to the ones that a malicious hacker would rely on too. This is good news for the ethical hacker because it allows them to go through the system, find some of the biggest vulnerabilities, and make sure that no one tries to hack into the system.

No matter what kind of system you are trying to protect, whether it is a bit database for a corporation or your own personal computer, having a good idea of how to protect yourself from hackers and all the trouble they can cause is always a good thing. It can save a lot of time, money, and hassle and can keep you, along with countless others safe. When you are ready to learn more about how the Kali operating system can help us with all of our hacking needs, make sure to check out this guidebook to get started.

Description

Are you interested in learning more about hacking and how you can use these techniques to keep yourself and your network as safe as possible? Would you like to work with Kali Linux to protect the network and to make sure that hackers are not able to get onto your computer and cause trouble or steal your personal information? Have you ever been interested in learning more about the process of hacking, how to avoid being taken advantage of, and how you can use some of the techniques for your own needs?

This guidebook is going to provide us with all of the information that we need to know about Hacking with Linux. Many people worry that hacking is a bad process and that it is not the right option for them. The good news here is that hacking can work well for not only taking information and harming others but also for helping you keep your own network and personal information as safe as possible.

Inside this guidebook, we are going to take some time to explore the world of hacking, and why the Kali Linux system is one o f the best to help you get this done. We explore the different types of hacking, and why it is beneficial to learn some of the techniques that are needed to perform your own hacks and to see the results that we want with our own networks.

In this guidebook, we will take a look at a lot of the different topics and techniques that we need to know when it comes to working with hacking on the Linux system. Some of the topics that we are going to take a look at here include:

1. The different types of hackers that we may encounter and how they are similar and different.
2. How to install the Kali Linux onto your operating system to get started.
3. The basics of cybersecurity, web security, and cyberattacks and how these can affect your computer system and how a hacker will try to use you.
4. The different types of malware that hackers can use against you.
5. How a man in the middle, DoS, Trojans, viruses, and phishing can all be tools of the hacker.

6. And so much more.

Hacking is often an option that most people will not consider because they worry that it is going to be evil, or that it is only used to harm others. But as we will discuss in this guidebook, there is so much more to the process than this. When you are ready to learn more about hacking with Kali Linux and how this can benefit your own network and computer, make sure to check out this guidebook to get started!