HACKING WITH KALI LINUX

MASTER ETHICAL HACKING AND IMPROVE CYBERSECURITY WITH A BEGINNER'S GUIDE. STEP-BY-STEP TOOLS AND METHODS INCLUDING BASIC SECURITY TESTING, PENETRATION TESTING WITH KALI LINUX

MARK CODING

Hacking with Kali Linux

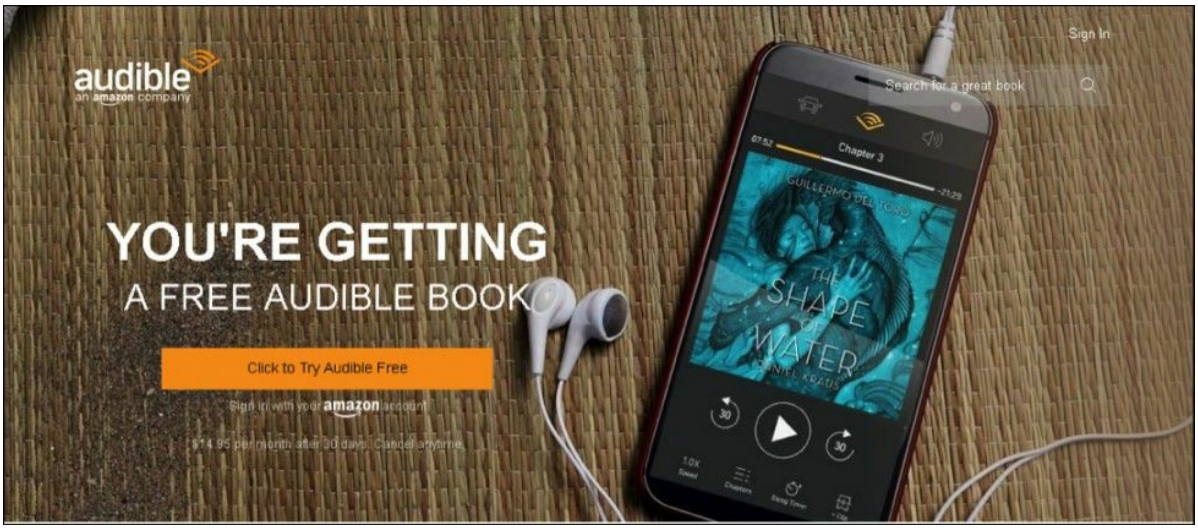
Master Ethical Hacking and Improve Cybersecurity with a Beginner's Guide. Step-By-Step Tools and Methods Including Basic Security Testing, Penetration Testing with Kali Linux

by

Mark Coding

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

TABLE OF CONTENTS

INTRODUCTION

Congratulations on purchasing *Hacking with Kali Linux*, and thank you for doing so.

The following chapters will discuss everything you need to know about hacking with the Kali Linux operating system. There are a lot of issues out there when we think about all of the damage hackers can do. Whether you are an individual trying to protect their financial information against a hacker, or you are a big business responsible for keeping the information of your customers safe, hackers can pose a big risk to your business and how successful you can be. Taking the time to learn how to avoid these attacks, and keep your business and information safe can be a critical part of ensuring your own personal and private information stays safe as well.

That is what we will spend some time talking about in this guidebook. We will look at some of the major hacks an attacker may try to use on your computer or your network, and then learn how you can protect yourself as well. It doesn't matter how big or small your system is; a hacker is interested in getting as much information as possible. But with the help of the Kali Linux operating system, and some of the tools and techniques we will discuss in this guidebook, you will find it is easier than ever to protect your network, whether it is big or small.

In this guidebook, we will start out with some of the information that you need to know about Kali Linux. We will take a look at the history of this operating system, the requirements needed in order to handle this kind of

language, and how to install and download this system before we even try to use it for our own needs. This helps us to get a better understanding of how this whole process is supposed to work and how we can benefit from using this operating system over one of the others.

From there, it is time to get into some information about hacking and how we can keep ourselves safe overall. We will take a look at the importance of cybersecurity, how to recognize a hacker and some of the different types that are out there (not all hackers are the same), and common cyber-attacks that everyone, no matter how big or small their network is, needs to be aware of. These can include options like a man in the middle, dictionary attacks, and more.

Internet traffic is so important to many individuals and businesses, and being able to watch out for what is coming in and out of your network is so important. That is why we will devote some of our studies today on protecting our Internet traffic. We will look at how to deal with a network scan, what a VPN is all about, and more. We will end this guidebook with a look at some of the steps you can take to keep your network safe and to ensure no hacker can get on and steal your information at all.

In our increasingly connected world, there are a lot of times when we have to be worried about all of the threats out there and how they will affect our personal and private information. Being prepared and knowing what is out there, and figuring out the right steps to protect ourselves from all of the threats can make a world of difference overall. When you are ready to learn a bit more about hacking with Kali Linux and how you can keep yourself safe and secure online and, on your network, make sure to check out this

guidebook to get started.

There are plenty of books on this subject on the market, thanks again for choosing this one! Every effort was made to ensure it is full of as much useful information as possible. Please enjoy it!

CHAPTER 1: BRIEF HISTORY OF KALI LINUX

If you have ever tried to go through and test your system for vulnerabilities or crack Wi-Fi passwords on your network, then it is likely you have been familiar with Kali Linux. It is a security-focused version of Linux that will offer us a lot of tools that will help us with hacking our own networks so we can seek out a weakness, and secure the network from other hackers who may try to get onto your system.

In the beginning, this system was made out of necessity for lead Kali developer Mati Aharoni. While doing some professional security work, this developer found out he needed to come up with a lot of security tools without having to go through and install a lot of software and other things onto the systems of his clients. And so, he took to Linux to see what he would be able to do in order to deal with this issue all in one.

The idea of this kind of distribution will contain a bunch of security tools born out of necessity. Aharoni was facing a dilemma when it came to security engagement with their customers. He was not allowed to bring on any kind of hardware to the engagement, and often you would only be able to use the onsite computers as long as you would not get on the hard disks or modify them in any way.

This is a pretty standard procedure. These companies want to get the most security out of their computers and want to make sure there isn’t a way for a hacker to get on. But they do not want a lot of things changed or modified on

their system at all. You have to be careful and still make sure you find all the vulnerabilities.

After Aharoni spent some time thinking about the problem, he could figure out that these conditions for work may seem impossible, but he could meet them simply by going through and adding in a few tools. And all of these can be added to the existing bootable Live Linux CD. This made it easier for everyone to use the system the way they want without issues.

Once this was created, it was possible to bring in the CD, or in our case the bootable USB drive, to the engagement area, boot all of this on the computer you want to work with, no matter where it would, and then work right on the RAM, which is not going to cause any issues to the hard drive or anything else. When it is done, you could either reuse the drive if you want, or you could destroy the bootable drive and then just download it again if you need to use it in another situation.

Over time, this will change, and there are new downloads and updates that have come with Linux. Kali Linux overall was born out of an understanding that it was time to take the previous eight years of experience in building up a Linux Security Distribution and then apply them to a new and clean canvas. The original form of Linux was a great way to deal with hacking and deal with all of the different parts that come with it. But then Kali Linux helped to polish all of this and could spend some time to really work with this and see some great results.

What this means is that with the original hacking with Linux, we need to go through and tear down everything done up to that point and start out with

something fresh. This process was a bit terrifying for the developers who worked on this as well as liberating because it meant they had to let go of some of the distributions overall, and this was hard. But on the other hand, it did allow them a chance to go through and rebuild, and even expand, our current systems in order to create something better.

Once the Kali Linux developers were able to make some of these hard decisions, they figured out that the next step they had to work with was to involve some people in this system who actually knew what they were doing. This was when they brought in a new developer from Debian who could help them to build up a new development infrastructure from the ground up. This assistance was helpful to the project and ensured Kali Linux would be as successful as possible.

One of the goals that came with Kali is that it would provide images of the operating system we can use for a lot of exotic hardware, mainly ones that were based on ARM. This will include everything you need to use, including Android TV devices, tablets, Raspberry Pi, and more. And each piece of hardware we will work with has a unique property.

For example, the MK808 comes with a dual-core CPU with a whopping 1GB of RAM, while still having the form factor of a medium-sized USB dongle. Imagine it! This is a great and powerful hacking computer, battery-powered, in your pocket. Think about how great this is for your whole hacking and security system.

So, we need to then decide which type of this hardware to target. That depends on several things. Availability is the main obstacle. We will try to

identify interesting hardware that is used in an interesting manner when it is time to handle a security assessment, and if such is found, it is possible to build up Kali to work with this. However, right now, there is a wide array of hardware supported by Kali, and this list will keep on growing every month.

One of the biggest concerns with the Kali Linux was the move from BackTrack to Kali, which ended up causing us to rebrand. After so many years of being a major force in the security community, BackTrack was something that was known by all. If we suddenly changed this around, it would be a bit hectic and confusing for some of the users, and they were uncertain about how to handle this and get people on board with it.

The good news is that a lot of different programs rebrand all of the time. This is hard to do, and sometimes it can be done in a poor manner. But they have to do this sometimes. Rebranding is tough in some cases, but the developers who worked on changing their brand over to Kali decided it was worth the time.

There are a lot of different options and benefits of working with the Kali Linux system, and it is worth your time to learn how to work with this for some of your own needs. The first benefit of working with Kali Linux is it is free. Even though you will not have to pay anything to use this system, it will come with an advanced suite of all the tools you need to keep your system safe and sound. Just as the Linux operating system is open-source, Kali is available for you to use for your whole life, free of charge. This is one of the first things that draw a lot of developers over to using this for some of their security needs.

Another benefit is this will adhere to the file-system hierarchy standard. This is important in the world of security. All systems that follow this standard, which is known as FHS, will allow the users to find support files, binaries, and even all of the libraries that they need to succeed. What this will mean for you is you won't have to go through and manually locate any of the tools you need, because you can enter in the command name into your root terminal and the system can find it for you.

There are also hundreds of infiltration tools you can use. We will talk about the infiltration testing you can do with this program later on, but it is helpful to make sure no one else can get onto your system and cause issues. There are more than 600 infiltration testing tools available on Kali Linux, and this is designed to help make things easier for network security teams to check out how safe and secure their network is.

These will include a lot of the basic tools you need to gather up information on your network, analysis tools, and even reporting tools. The reason Kali Linux incorporates so many of these tools is to make sure nothing is left to chance at all.

Using the Meta Packages, you may install the tools you think is the most important to some of the work you want to get done. Each programmer will have a different type of work they want to do and may find some tools a little bit better than the others. This allows you the flexibility to pick out the tools you want to work with, no matter what kind of project is at hand.

You may also like what is known as the Version Tracking feature in this language, which is the part that helps you to compare different versions of

what you are using in the Kali operating system. This makes it easier to know what is going on, if you need updates, and what features are present on your system.

As you work on some of your coding and hacking in Kali Linux, you will find it is actually a really easy operating system and extension to work with for getting some of the results you want. While some other similar tools are available, some of these require a lot of extra work just to learn how to use.

For those who are newer to the ideas of coding and computer languages, this can be hard to work with and can cause some issues overall. This is not a problem when you are working with Kali Linux. You will find that with this distribution, you can get all of your chosen hacking done, without the issues along the way.

And the final benefit that we will take a look at here is the open development tree. The open-source availability that comes with many of the products of Linux is great, and you will find that working with Kali Linux is not going to be any different. as a result, users can access this system well, and it is easy for anyone to come on and view some of the codes. You can monitor some of the codings you are doing at each and every stage you are working with, thanks to this feature of the open development tree.

When it is time to work on protecting your system and ensuring no one else can get on and cause some problems, the Kali Linux system is one of the best. It is an open-sourced free and easy option to use, while providing you with all of the features and more you are looking for to keep your system as safe and sound as possible. When you are ready to learn how to use the Kali

Linux system for some of your needs, make sure to check out the rest of this guidebook to help you get started.

CHAPTER 2: REQUIREMENTS TO UNDERSTAND THE LANGUAGE OF KALI LINUX

Now that we have a better idea of how we are supposed to work with the Kali system and how it is such an important part of the process of working on our own hacks and more, it is time for us to dive into some of the specifics about actually coding with this language compared to some of the others. We have already seen some of the reasons why this is the preferred method to work with when it is time to check your system and keep it safe from hackers, and now it is time for us to learn some of the basics that will help us to make this happen.

One thing to keep in mind with this, though, is when we talk about hacking in this guidebook, we are talking about ethical hacking. Our goal is not to jump onto other computers and start causing issues and stealing information. Instead, our goal is to learn how to use these features in order to understand our own networks and to keep the unethical hackers out of our way.

Of course, you will quickly find that both of these will have the same ideas and techniques that you will work with. This is because we want to use the same processes and techniques as an unethical hacker, but on our own system, or a system we are asked to protect, in order to learn how an unethical hacker will get onto our systems. This will take some work on our part, and it may seem like we are doing things that we should not, but overall, this is the best way to find the potential vulnerabilities of our system and to

ensure that we can keep our system as safe and sound as possible.

With this in mind, it is now time for us to take a look, not only at the basics of the Kali Linux system, but also some of the different codes we can use in the command line. These command-line codes is important because they are what will tell the system how you want it to behave and what work you want it to do. So, let's get started:

Basic Commands for Kali Linux

There are a lot of commands available for this kind of system. They are there to help us to handle or to run any kind of documents, create documents maintain our directories, and write other scripts we need in the Linux platform. There are many of these commands, and we will spend some time looking at the most basic and how we can make them work.

The first basic command we will look at here is the command to bring out the date. This is a common and simple command, but it helps us to see a bit more about how this language works and how we can get all of the parts to work together in the way we want. This one will work because we will use it to display a normal date with time on the screen of the Linux system. It is also possible to get some of the custom dates to show up, which is handled when we use the specific command below:

```
# date-set = '17 Jan 2019 12:16'
```

When we go through and work on this code, we will get the result of January 17 at 12:16 EDT 2019.

Another type of command we can work with to get more familiar with working in Kali Linux is a command to display a calendar for us to use. This is the command of “cal,” which will help when we want to display one of the proper calendars on our terminal screen. Our hope is we can do this in order to get it in a manner so others can see the local date on that calendar.

There are also a number of different packages available in the case of the Kali Linux command, where people can come in and manage the calendar that they create in a different way. Maybe you want to have it go vertically or some other critical features with this additional command. This command package that is added in can call up the ncal package. Make sure to download this on your system in order to get it to work.

The Who and Whoami commands are next. These is really useful, and even popular commands you can use on this platform. The Whoami is a key command that will provide us with an exact effective username right away so you can see who is the one involved when a specific command has been executed. It can also tell you what is the command that gives you all of the logged user detail information, so you know where they were when they did it, and more.

Another command that can be useful in this is PWD. This is a command that stands for Print Working Directory. This is a command that is used for displaying the specific directory where the command executer belongs to right now. Sometimes when we are talking about a user on this platform, it is hard to understand which directory that person is in right at that time. This is when we would use the PWD command to find them. And if your directory is not secure, a hacker would be able to use this to help them get ahold of

someone when they want.

Ls is another common command that beginners need to know. Every user, after they have gone through and applied their logic, will go and use this as one of the very first commands they execute. The command Ls is actually going to provide us with a full list of all the documents available in the directory you are in.

Of course, there is other extended commands of Ls we can use when it is time to manage the display of those files in the right manner. This is used depending on what information and what part of the list, such as which files you are hoping to gather from there.

Cd is another command. This is the command you will use any time you are ready to change up which directory you are in on this platform. This can be useful as you move from one directory to another while doing some of the hacking and the coding you want to accomplish with this kind of coding.

Mkdir: This is another one of the key commands beginners need to know when working on the Kali Linux platform. This is a useful one when it is time to create a brand new directory to work with this platform. It can also be used with the Cat command, which is the one that you can use when it is time to display the entire content of just one file. You may bring up the Cat command in order to create or concatenate single or multiple files on the platform.

Cp is the next command to work with, and it is the one that we will use when we want to be able to copy the image of an existing file or a directory, and

then paste the same thing anywhere else in the platform for Kali Linux, but we want the option to use a new file name when we are saving it.

And finally, out of the basic commands that you can use in this coding platform, and to help you to complete some of the hacks that you are doing, is Mv. This is a command we can use in order to move the directory or the files we want to a new location. When we use this one, we can keep the same content and name for the directory or the files we are using.

Intermediate Commands on Kali Linux

Once you have had some time to work with some of the basic commands that come with the Kali Linux platform, it is time for us to move on to some more commands that will help us with some of the hacking and more that we wish to do. There is a few other commands with this platform that are popular, and that a lot of developers of this platform will use, but they are not going to be as basic as we want for a beginner.

These commands are still going to be really important to learn, even though they do require a lot more work for you to execute and use them. Some of the different types of commands we can use that fit into this kind of category, and will require a bit more intermediate work from Linux is found below:

1. Rm: This is the command we will rely on when it is time to delete or remove the files, or more than one file at a time. If we use this command in a recursive manner, then it is used to help remove the whole of the directory.
2. Uname: This is a command that is useful when you want to display the current system information in a proper manner. It is the one a

programmer will want to use when it is time to display all of the information in the Linux environment so the system is easy to understand and will go through the configuration it should.

3. Uptime: This is the command that will provide us with more information about how long the system is up and running.
4. Users: This is a command that will provide us with more information on the user. This could include the login of that user and even information on who is logged into the Linux system at the time.
5. Less: This command is used to help display the file without having to open it or use the vi or cat commands. This is a very powerful command you can use, and it extends out the capabilities of the “more” command in this environment.

Advanced Commands

As you work with the Kali Linux system, you will find that some of the work you want to complete with this and for hacking is more advanced. This will mean that we need to spend more time and effort figuring out how to make it all work, and how we can use the different parts. Even if you are a beginner with the Kali Linux system and how it is meant to work, it is still important for us to take some time to learn the more complicated parts, and figure out how we can bring it all together.

Some of the more critical tasks needed to make the commands work in Kali Linux is in this section. These tasks will need commands that are more complex in order to get the work done. They are often going to be the ones the management of the company will use in order to sort, identify, or modify a file, some writing in the shell scripting, the job scheduling, and more. Some of the more advanced commands you can use inside of this kind of coding

language will include some of the following:

1. More: This is a command that is used in order to display some of the proper output in one page at a time. This makes it useful for us to read through a long document or file without having to scroll through to get it all done.
2. Sort: This is used when it is time to sort out the content you want into one define file that is specific. This is also going to be useful when it is time to display some of the critical contents that are in a big file in a sorted order, as well. If the user includes a commanding with it, then it will provide us the reverse order of the content.
3. Vi: This is one of the key editors you can use with the Linux or a Unix platform at any time you want. There are two modes that come with this one, normal and insert depending on your needs.
4. Free: This is the command that will provide us with some more detailed information about the free amount of Ram or memory available on that system, so you know what you can do with that space when it is needed.
5. History: This is the command you will use to see what kind of history is being held and executed on the command on this kind of platform when you need it.

Tips to Work on These Commands

Now that we have had a chance to go through and talk about some of the most common commands that work with this language, it is time for us to take a moment and look at some of the things you can remember, and some of the tips and tricks needed to make the Kali Linux system work for you.

Some of those who use this platform on a regular basis and who know how to make these commands work will find there are a number of things that will ensure the work is done the right way, and that these commands are easy enough for them to use and remember. Some of the different commands that work well in this kind of platform, and that you need to remember as we go along will include:

1. How to protect and secure this language: One of the critical processes that are available with this kind of platform, and is really useful for you to use when you when it is time to start some of your own hacking and watching over the network, is the VPN services. These allow you to create your own custom proxy when you want and will make it easier to keep your network and all of your other information secret and hidden from others and safe from those who want to do you some harm.
2. Secure with some good passwords: There is one utility of securing your personal information with a specific password, and then you can lock them onto your target. And then, you can recover that information at any time that you want just by going through and providing the system with your password. This can be one of the best ways to keep the hacker out of your system, but you have to make sure your passwords are strong and powerful, and that the hacker is not able to guess them, or use the dictionary attack against you in order to gain access to your system.

Any time you want to work with the Kali Linux system in order to protect your system and have the tools needed to perform a safe hack on your own system, discovering vulnerabilities and other issues in the system along the

way, is to learn some of the commands that are needed to make this happens. This will help you to see what information is being shown on your system and will give you some of the steps you need to figure out what you can do to keep yourself, your employees, your customers, and others who rely on you as safe as possible.

CHAPTER 3: CYBERSECURITY

Now that we know a bit about the Kali Linux program and what we can do with this, we will take a look at some of the important features that will come with the idea of cybersecurity. To keep things simple, cybersecurity is simply going to be the practice of protecting our networks, programs, and other systems from attacks by hackers. These cyberattacks is aimed, in most cases, at accessing, destroying, or changing information that is sensitive, interrupting some of the normal processes for a business, or extorting money from the user.

Implementing the right and effective measures for cybersecurity is even more challenging in our modern world because there are more devices than people. Plus, most of the hackers out there are becoming more innovative in what they can do.

A successful approach to cybersecurity will have more than one layer of protection that is spread across the programs, data, networks, and computers that you want to keep safe and secure. In an organization, the processes, people, and technology need to all be able to complement one another to help create the most effective kind of defense that is possible against a cyber-attack from any hacker. Whether you are working with a large company or just on your own network, this is really important.

You may find that working with a unified threat management system will help us to automate some of the integrations across the whole system. It is

there to provide us with some acceleration in the key security operations functions, including detecting problems, investigating those problems, and working on remediation.

We have to remember there are several different parts that have to come into play when it is time to work with cybersecurity. We can't focus on just one or the other, and if any of them is missing, then the cybersecurity of your computer or system is not going to be all that great. We have to be careful with the people, the processes, and the technologies found on our system and how they each interact with one another.

First, we have to look at the people. Users need to understand and then be willing to comply with some of the basic principles of data security before they can be on your network. This means they need to pick strong passwords, they must be wary of any attachment that comes in an email to them, and they should do a routine backup of any data they want to work with.

Then we need to take a look at some of the processes that are used in your system. Organizations especially need to have a plan for how they will deal with cyberattacks, whether these are successful or just attempted types of attacks. A plan that does the job will guide you through this. The plan will explain how you will identify the attacks, how you will protect all of your systems, how you can detect and even respond to some of the threats, and finally, how you and the company as a whole can recover if a successful attack does occur.

And finally, we need to take a look at the technology your company is using. Technology is very important when it is time to provide individuals and

organizations with the tools; they need in computer security to protect themselves from some of these attacks.

We have to keep in mind that there are three main entities we need to protect at all times. We need to protect some of the endpoints devices, including the routers, the smart devices, and our computers. We need to also protect the Cloud and our network in the same way. Common technology we may use to protect these entities will include firewalls, malware protection, email security, DNS filtering, and more.

This brings us to our final question about why this cybersecurity is so important. In our connected world today, everyone can benefit when we have programs to defend our systems that are more advanced. When we just take a look at this on a more individualized level, an attack like this will result in a multitude of problems, including extortion attempts, loss of data that is important to you, and identity theft.

And if this is taken to the next level, think about how much you rely on things like financial service companies like banks, hospitals, and power plants to help keep you going in your daily life. Securing these and other types of companies is so essential when it is time to keep our society functioning and working well.

Making sure you have the right kind of cybersecurity in your system, and checking on any of the updates and more that are needed to make this into a reality is so important to helping you get the results you want. This is not something we should push to the side or assume we are not going to need at all. Even individuals have things they want to protect, and being able to keep

your information and your system safe and secure is the first step to getting this done.

This brings us to the point of why cybersecurity is so important and why it is required. At its core, cybersecurity is all about protecting systems and the information on them from cyber threats that are out there. There are a lot of different types and forms of these threats, including malware, phishing, ransomware, and more. And with all of the advancements we have seen when it comes to technology, there are new possibilities showing up all of the time. Making sure the cybersecurity will keep up with this and be able to protect us and our computers and networks is an uphill battle many of us are trying to deal with.

Being able to take advantage of a tool known as automation, hackers can deploy a pretty large scale kind of attack at a low cost overall. In addition, the economy that makes up cybercrime will make it easier than ever to complete a more sophisticated attack, and so many people are willing and able to grab onto this information and use it against us.

This means that the cybersecurity and the tools that come with it need to be even more advanced than what the hackers can send to us. This means that adding in some machine learning, automation, and some shared threat intelligence is the top thing that will ensure that organizations can stay on the cutting edge of this kind of thing, and combat some of the advanced threats out there. and there are a ton of advanced threats we need to deal with, including:

1. DNS-tunneling: Domain Name System is one of the protocols out

there. Please take some of the human-friendly URLs and turn them into IP addresses that are more machine friendly. Most of the time, hackers will use the DNS that is widely used and very trusted, but that it is also not monitored. DNS tunneling will exploit to transfer the malware and some other data through the client-server model.

2. Malicious crypto mining: There are crypto mining attacks possible when an attacker has found a way to take some JavaScript into a website, and then uses this code in order to hijack the processing power of the visitors to this site. This is done in order to mine some of the cryptocurrency that is needed, like Bitcoin. In case of the malware-based type of this, the user's entire device is taken over, and the CPU is used at an even higher level to help mine some of the cryptocurrency that is needed.
3. Ransomware: This is the focus of the criminal business model that will install some malicious software onto our device and then will hold some of the information, data, or files. With its low barrier to the entry and high revenue potential, ransomware is one of the biggest threats that will face an organization today.

In many cases, organizations and governments will take a reactive and point product approach in order to fight off some of the threats that they will get online. This allows them to piece together individual security technologies in order to protect their data and their networks. However, this method is expensive and complex, and it is still hard to fight off all of the different parts that come with it.

We have all heard about how bad the data breaches can be when things don't go the way we would hope with some of the security we are working with.

There are a lot of devastating breaches that hit the headlines on a regular basis, which shows that some of the traditional approaches to data security is ineffective and hard to work with.

With the help of some of the topics we have been able to talk about before, such as shared threat intelligence, machine learning, and more automation in the security architecture of the company, it will help the company to keep pace with some of the growth of more sophisticated cyberattacks that are out there. We will also see that machine learning is there to help us accurately identify some of the variations out there of known threats, predict the steps that will happen next in the attack, recognize patterns, and inform automation tools in order to create and implement protections across the organization.

The neat thing with this is if we do it in the proper manner, we can see all of the things above happen in near real-time. With shared threat intelligence, anything that one user sees identifies, or prevents can benefit all of the other people who are a part of that shared community. The more comprehensive the prevention can be, especially when it is done at a quick rate, the easier it is for us to reduce the overall risk to our security online, and the easier it becomes to manage it all.

Companies need to consider the kind of security they are relying on and decide what they want to do with it. Keeping up to date on this kind of security, rather than just avoiding it or assuming it is not something you need to worry about all that much is important to how much success you can see with this coming together.

While we are here, we need to take a look at some of the challenges that are

likely to come up with cybersecurity and why we need to handle it in a special way to make sure it can protect our information. For an effective amount of cybersecurity, an organization will need to do some coordination of its efforts throughout the whole of the information system. Some of the elements need to come with this security, and some of the unique challenges that come with the cybersecurity we try to put together will include:

1. Education of the end-user
2. Disaster recovery and business continuity planning
3. Mobile security
4. Cloud security
5. Infrastructure and database security
6. Identity management
7. Data security
8. Endpoint security
9. Application security
10. Network security

One of the most difficult things we need to worry about when we are dealing with cybersecurity is the changing nature of these security risks on their own. Traditionally government and organizations have spent their focus on the resources of cybersecurity on perimeter security in order to provide some protection to the parts and components that they find the most crucial to the system and make sure to keep these defended against the known threats that are out there.

Of course, today, we can see that this kind of approach will miss out on what is most important, and it is not going to be enough to protect the system. As

the threats start to advance and they continue to change more quickly than most companies will keep up with, we can find it is really hard to make sure all of the systems are protected and more.

As a result, there are now advisory organizations out there who are more proactive and adaptive to the issues of cybersecurity. In addition, we will find that the NIST, or the National Institute of Standards and Technology, has issued some guidelines in the framework of risk assessment recommend that a company should work on real-time assessments and continuous monitoring of their systems, rather than leaving everything to chance. And it also recommends that these have a more data-focused approach when it comes to their security, rather than a model based on just looking at the perimeter.

There are a lot of different methods that can be used when it is time to keep the security of your company good and strong. In many cases, there is a recommendation that you work with a top-down kind of approach to this security, which will lead for a big change in how this security is focused on across all of the practices of the business.

There are a lot of different types of compliance organizations that we see, and these change based on what kind of industry you are in and more. It is important for us to know a bit more about this process and about the compliance we need to follow, to better understand how we can use those rules to keep our systems not only safe, but compliant for the expectations of our industry at the time.

There are a lot of reasons why a hacker will want to get into your company and look at your data. To start, if you are collecting credit card information

for payments from customers, then this is a gold mine for a hacker. They would love nothing more than to get into that information and use it for their own needs. Think about how far the hacker could go with all of that credit card information, and the chaos they could cause, and the money they would spend before anyone else would even notice what is going on.

This is definitely something you need to be worried about if you are handling any credit card or payment information along the way. and when it happens, your customers could have a long battle ahead of them with dealing with missing money and information, and you will lose your reputation, not only among your customers, but also with some of the potential customers that you want to reach in the future.

It is possible to recover in some situations, but you will find that for many companies, it is easier to go under if you have one of these data breaches. It is always better to be proactive and think ahead about how to handle these cybersecurity issues, rather than letting the hacker take advantage of you.

When you are running a business, and even when you are handling one of your own networks, you need to make sure this cybersecurity is one of your number one priorities. Protecting your information and the information you gather from your customers is really important, and you need to make it something you focus on quite a bit. The good news is that with a lot of the topics we will discuss in this guidebook, you can get started with hacking and keeping your cybersecurity as safe as possible.

CHAPTER 4: HOW TO INSTALL KALI LINUX

With some of the information from before in mind and ready to go, it is time for us to spend our time looking at how we can download the Kali Linux operating system so we can start some of the hacking and other options we want to use. One thing to note with this is that we never want to go through and download a Kali Linux image from anywhere other than the official source. Remember that we are working on keeping our systems as safe and secure as possible, not letting in more issues as well.

Linux is often going to be one of the first operating systems that hackers like to work with because it is easy, and they will have all of the necessary software that will make hacking and finishing some of these projects as easy as possible. It is also an open-sourced and free operating system to work with, so we can go through and make some of the modifications we want, and we don't have to worry about some of the added costs with other operating systems out there.

There are a number of ways we can install the Kali Linux option, but we will work with one of the most common options, where we will have Dual bootup with another operating system. This allows you to still use your computer with the regular operating system on it, but will bring up Kali Linux any time that you want, without taking more too much memory and space on your system.

For some of those who are beginners in the world of programming and

hacking, the installation process of this system will seem a bit complicated. But that is why we will spend our time working at how to complete the dual boot of Kali Linux, the different things that you need to get started, and then the steps that will help you to get this done. We will look at how to do this dual boot, so it works with either the Mac OS or Windows operating systems based on what your preference is here.

The first option we will need to look at when it is time to work with a dual boot of our Kali Linux is how to handle our dual boot, as we said earlier. This will help us ensure we can pull up this operating system any time we want, but we would still be able to use our regular operating system.

We will start by using this with our Windows operating system. Windows 7, 8, or 8.1 are the best for these. It can work with the newer versions, but these are a bit harder to download and install the Kali Linux on, so we will start with something that is a little bit easier to handle. Before we are ready to begin on doing our own dual boost, we first need to make sure we have some of the right materials set up and ready to go here. Some of these will include the following:

1. A laptop or PC that can handle some of the different hacking processes that we want to do.
2. A minimum of 4 GB Pen drive
3. 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.
4. Windows 10 or any of the other versions of Windows that are already installed on your computer.
5. The latest version of Kali Linux
6. Rufus

7. And patience to get it all done.

Once we are sure we have all of these supplies, it is time to learn how to start up our Dual Boot of Kali Linux with the help of the Windows 10 program. The first step we need to do is make sure we download the latest ISO file of this operating system. The best place to get it is www.kali.org because you know this is the official site, and you will not need to worry about having viruses or other things attached.

You can choose which version of the download you want to work with, and then move on to creating a bootable USB that will contain this image on it. For this, we need to bring in the extension, and in particular, we will work with the Rufus extension. This is a utility that is really useful here because it allows us to create a USB flash drive that is bootable. You can download this extension from www.rufus.ie and then install it on your system.

When you have both of these items above on your computer, it is time to get started with some of the fun of creating your own bootable USB drive. First, take out the USB drive that you want to use and then connect it to your computer. As we said above, make sure this has a minimum of 4 GB of memory to work with and enough space that you can handle the operating system of Kali Linux and the Rufus extension as well.

When you have had time to plug in the USB drive you want to use, we are ten going to run Rufus, and use the steps we have following here to help us create our very own bootable USB drive:

1. First, you will get a screen image to show up about the Rufus program

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 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, it is also possible to use this USB to do a live boot of Kali. This means we can run Kali without having to install it on our system. Keep in mind it does limit the functions and the features a little bit when you work in this matter.

From this point, we are then able to create our own separate partition for the installation of this operating system. To help us do this part, we will open up the settings that are needed for Disk management. Another method that works well here is to open up the command line in Windows and type in "diskmgmt.msc." Creating a partition of the size that is somewhere near 15 to 20 GB can help make sure it will fit into the system you want.

At this point, we will find that the initial processes are done. We have gone through and downloaded the ISO needed for Kali Linux, created a USB drive that is bootable and has this ISO on it, and we even went through and created a different partition for the installation of Kali Linux. Before going on from here, keep in mind we will need to work with the Fast Boot and the Disable Secure Boot option that is available from the BIOS if we want to use these in

our own program.

We are now ready to move on to the next step. We can do this by restarting our laptops or PCs because we want to change up which operating system shows up. When we restart the computer, make sure to go straight to the boot manager. Select the option you want the computer to boot from the USB. The options will look a bit different based on the brand of computer you are working with, so take some time to look for this option.

If you did this in the proper manner, you should see that your computer will show you the installation window that comes with Kali Linux. There are a few options that will come up when we get to this point about how we can install Kali Linux. You will want to work with the option that says "Graphical Install" to help you get this operating system to start up with ease. We are even able to take this further and add in a few features and settings we think will work nicely. For example, you can choose which language you want to have when this installs, and the country that should be there as well.

After we have had a chance to go through and add in some of our own preferences from above, and all of the other options that come up with the system, it is then time for us to work on our hostname. Your installation at this time will ask for this hostname. You get the option of choosing any name you want to work with, and you can just think of this as a username. Then make sure to enter in the password you want to have present for the root user. After entering both of these things, you can click on the button to continue.

Now we want to take some time to choose the partitioning method we want to see in use for this, and for our projects here, we will work with Manual.

The next step needs to be taken with caution to ensure we can get it to work the way we want. We want to only choose the partition that we took the time to create and add to the USB drive earlier for the installation of Kali and then press on the Continue button. When you are sure you have the right option in place, you can select “Delete the partition” before we continue.

If you picked the right option and you did this in the proper manner, you will see that the partition for Kali Linux will tell us it has FREE SPACE. We will want to choose to work on this free space partition before we decide to continue on with this process.

This is the part where the installation will ask us the way we want to use all of the free space we have. What we want to do here is click on the part for “Automatically partition the free space” and then click on the continue button. Next, choose the option that says, “All files in one partition.” This is usually the recommended option for new users in case this is worded in a slightly different manner when you get online. And then we want to finish this out by clicking on the option that says, “Finish partitioning and writes changes to disk.” Here it will grant the right permissions to write these changes onto the disk. You want to click on Yes and then on Continue.

This is the part where we will see some of the installation processes with Kali Linux happen. This can take us a bit of time to complete, so wait about 15 minutes or so to ensure the process has enough time to complete itself. When your process gets to the halfway point, you will see that it will pop up and ask you about a network mirror. Select the one you want to work with. This setting is about the kinds of update options you want to work with, so it is usually best if you choose no for now and then make some changes to these

settings at a later time if you want.

Next, the installation will ask for installing the GRUB boot loader. You want to click on Yes before continuing. Next, it will ask you where you want to install the Kali GRUB boot loader. The hard disk with the second option is the best. We want the GRUB to happen on your hard disk, or the installation of Kali Linux will not display the option to choose the operating systems 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 will see a screen that will 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 can see the Kali Linux through our GRUB Loader. Here you can choose the Kali GNU/Linux to boot the computer with the Kali Linux. Or, if you want 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 this process. You just need to go through a few of the different steps that we have above, and then you can have the whole thing set up with the Kali Linux distribution ready to go and handle. Each time you are ready to restart your computer, you can choose, as long as you have it all set up, whether you want to work with the Kali operating system or if you want to use your Windows system in this case. You can easily switch back and forth between the two depending on your needs.

CHAPTER 5: USE OF KALI LINUX

We can now spend some time looking at how we can perform a penetration test. This is basically an in-depth process that we can use in order to figure out where some of the vulnerabilities in our code is. These are the best to work with when it is time to check where a hacker may try to get us and figure out the best way to handle this overall.

The first thing we need to understand this process is what infiltration testing is all about. Infiltration testing is the art of finding vulnerabilities and digging deep in order to figure out how much our system can be compromised. This is done ahead of time so you can be prepared and protect yourself before a legitimate attack happens against your system.

An infiltration test will involve a number of different steps in order to check out the system and make sure that it will work the way we want. For example, this type of test will involve exploiting the network, servers, computers, firewalls, and more, in order to find the vulnerabilities there, and then highlight some of the practical risks that will show up with using this system.

There are a lot of steps we can take when it comes to performing this kind of infiltration test, and we have to make sure we have it set up in a manner so we actually fund the vulnerabilities and can figure out the right steps to take next in order to keep things safe on your network. Let’s take a closer look at some of the different parts that come with an infiltration test, and how you

can use your Kali Linux system in order to perform this kind of testing procedure at the right times.

The Stages of Penetration Testing

Infiltration testing is a more in-depth process than many programmers may think, and it will come with a number of phases to see success. The number of phases you try to accomplish through will depend on your situation and what needs to happen for each part, as well. Let's take a look at all of the different phases you can work with when it is time to focus on an infiltration test.

The first phase is known as the agreement phase. During this phase, there is some kind of mutual agreement between the parties. This agreement will cover all of the high-level details and methods we need to follow and the number of exploitation levels you will go through. The attacker is not going to be able to bring down the production server, even if the testing has been done at non-peak hours.

There are a number of things that you and the client need to discuss when it is time to perform this penetration test. You will most likely need to sign a non-disclosure agreement to tell that you will only share the details of the test with the company you are working with, and no one else, and this is often going to tell us what else has to happen. There may be some rules about what you can access, what techniques you can use, and even when you can perform the testing so it does not interfere with some of the work the business needs to focus on.

If this is your own computer system, then this is not going to be a big deal.

You will not need to go through all of this process in order to see results. But you will find that if you are working with another company or client, there are often safety concerns you need to work in order to see the results you want and to make sure everyone is on the same page the whole time.

Once you are both on the same page and have discussed the rules you will follow, it is time to work on the planning and the reconnaissance. In this phase, you will go through and gather up as much information about your target as you can find. This is the client in this situation, but you need to make sure you can get as much information as possible and to see what information is out there and available to the public.

This is the first step a hacker will undertake when they are trying to gain access to your client, so you need to take this step as well. You want to take a look at the domain details, network topology, mail servers, and IP addresses and any other information found online for your client. Hopefully, they have been doing a good job with some of their work already, and you will not have to worry about this. But most of the time, your client is surprised at the amount of information that is already out there and available to a hacker to use against them.

An expert hacker is already going to spend quite a bit of their time on this phase. This helps them to make a map of the network and will ensure that they will find more potential places for the vulnerabilities. As an ethical hacker, you want to be able to take a look through this as well and see what you can learn about the system as well.

Now we are ready to move on to the third section or phase of this. This is the

phase where the attacker can interact with the target, and they will try to identify some of the vulnerabilities there. An attacker will send off some probes to the target and then can record the response to the target to the different inputs.

This is a helpful phase because it will tell the hacker how much security is on the system or not. If the hacker can send in a lot of information and a lot of input without issues, then this may be a sign there is a lot of availability for them to get into the system. If it is a bit harder to do this, you will find that a lot of the ports during this phase are blocked off.

This phase will include a few steps, including scanning the network with a lot of scanning tools, identification of some of the share drives that are open, open portals of FTP, services that are running, and so much more. When we are working with the web application, the scanning part could be either static or dynamic. In a static form of scanning, the application code is scanned by an expert application vulnerability analyst.

The aim of working through this part is to identify some of the vulnerable functions, the libraries that are there, and some of the logic that is being implemented in the process. When you are working with a dynamic type of analysis, the tester will pass through a lot of different inputs to the application, and then will work to record some of the responses. The various vulnerabilities like injection, cross-site scripting, and the execution of the remote code can all be things we will identify in this phase.

At this point, the hacker has spent a lot of time taking a look at this system and trying to figure out what information is found inside of it. They should

have a good idea of where they can exploit and what areas they want to try and attack first. And that is why the next phase is gaining access to the system.

Once the vulnerabilities have been found by the hacker, the next thing that they need to work with is a way to exploit the vulnerabilities with an aim to gain some access to the target. The target can be a lot of different things, including the server, a secured zone, firewall, or a system depending on where the hacker could find the vulnerability in the first place.

While we are in this phase, be aware that not all of the vulnerabilities you find will lead you over to this phase at all. You need to not only find these vulnerabilities, but you also need to find the ones that are exploitable enough that you can use them in order to gain the access you want from the target.

Next on the list is maintaining access. If you were successful at finding a good vulnerability that allowed you to get on the system, then it is time to make sure you can maintain the access you have gained. And you need to be able to do this in a manner that you will not be found. This is a challenge in some cases because you want to be able to stay on the system and see the results you want, without someone else noticing you are there. once you are found, then the system will make sure you are kicked off, and you will not be able to go any farther.

That is why this step is all about ensuring the access we were able to gain is maintained. This is important to make sure we can keep our access to the system, even if that system is reset, modified, or rebooted. This kind of persistence is used by hackers who want to live in the system and gain some

knowledge about what is on it, what information is inside, and more, over a period of time. Then, when they are certain the environment is suitable and ready to use, the hacker will go through and exploit what they have found in there.

This is the part where the hacker will get some of the information that they want and cause some of the chaos that they want. This is also going to be the part where a lot of businesses need to be careful about what is going on around them because when the hacker can get to this part, they will end up with some issues as well. It is best if the hacker can be stopped before this point, and that is part of why we will work with the infiltration testing.

This is the phase where most of the actual damage of a hacker is done. The attacker will try and get ahold of the data, compromise the system or the network in some manner, launch their attack, and more. This is the phase we will control in infiltration testing to ensure the mayhem you cause is kept to a minimum. But it is still a good idea to gather an idea of what the hacker would be able to do if they were able to get on the system.

This is the phase that is modified a bit. A dummy flag is placed in the zone that is critical to know about later. The aim of the exploitation phase is to go and get the flag. Revealing the contents of this flag is often going to be enough in order to ensure the network could be exploited if nothing is done about this process.

Once the infiltration test is all done, the final aim or goal that will happen here is for the hacker or the penetration test to collect the evidence of the exploited vulnerabilities, and then report this back to those in charge for the

client. Often this allows them to figure out how to review and what actions to take. Now, it is the management's decision here to figure out how to address the risk. Whether they want to accept the risk, transfer it, ignore it, or do something to keep the information safer, they can take the right actions at this time.

The Methods of Penetration Testing

There are a few different types of penetration testing you can work with. These can be categorized on the basis of the position of the infiltration tester, and the knowledge that the tester has about the target. There are a few other types of parameters that can fall into the categorization of the infiltration that is happening:

Black Box, Gray Box, and White Box

This is the first type of penetration method we can work with. When the tester is given all of the knowledge about the target, this is known as an infiltration test that is a white box. The attacker will know everything they need in order to get things taken care of, including code samples, controls that are in place, the IP address, and more.

There can also be times when the attacker is not going to have any knowledge of their target. They are going in with no information and seeing where they will see where they can get with some work. This is known as the infiltration test that is a black box. Please note that the tester can still have all of the information that is available publicly to others about the target.

And then, when the tester can have some partial information about the target,

then they are working with a penetration type known as a gray box. In this case, the attacker has a bit more information about the target than what the public could find, like IP addresses and URLs, but they are not going to have complete knowledge or access to the system at all.

An External and Internal Penetration Test

If the penetration test is one conducted from outside of the network, then we are working with a type of penetration testing that is external. But if the hacker is someone who is inside the network, such as an employee or someone the company hires to be on the network, then this is a good example of an infiltration method that is internal.

When the attacker or the hacker is an internal person who is getting onto the network, the knowledge about the system and the target is very high, which is why these are more effective than other methods. Those who conduct the attack from outside of the network can be successful in some cases, but they will find it more difficult because they do not have the same information as others.

Third-Party or In-House

When the test is done by the security team that is in-house, it will basically be a type of penetration testing that is internal. Companies who will hire an organization that is the third party to do these tests for it, then this is known as infiltration testing that is third-party.

A Double-Blind and Blind Penetration Test

When we are working with a blind penetration test, we will see that the hacker, or another person who is working with infiltration testing, will not receive any information about the company or the client besides their name. The tester will have to do all of the work here, just like a real hacker would try to do. This one will take up more time, but the results we will see are more closely related to some of the practical attacks we see.

Then we can work with a type of penetration test known as a double-blind test. This is similar to a blind test, but the security professionals will have no idea when the testing will start. Only senior management will have this kind of information. This is done because it will test the controls, the awareness, and the processes of the security team, and see if things will happen when people act the same way that they do on a day to day basis, rather than how they behave when they know an attack is about to happen.

How Important are Penetration Tests?

While we are here, we can take some time to see how important a penetration test can be to your business. For a company, the most important thing they can do for their business is continuity. The second thing they need to work on is supporting services that will ensure the business can run as smoothly as possible.

Thus, to make sure the senior management of the company is involved and can pay the right amount of attention, the infiltration testing can highlight the risks that any business can face due to some of the findings that are done in this process. Let’s discuss a few of the things that a penetration test will allow your business to do.

First, it will ensure that any of the weaknesses that show up in the architecture of your coding language are fixed and identified before a hacker can find and then exploit them. When this happens by a hacker rather than you finding them and preventing them, it will cause a lot of loss to your business, and can even make it, so you are unavailable to provide services to your customers.

Organizations in our modern world will need to comply with a lot of different compliance procedures and standards. A penetration test is one of the best ways to ensure the gaps in the security of the company are fixed so this company can meet with the compliance the way they are supposed to. One example of this is with PCI-DSS. This is a company that will deal with the information for credit cards and helps other companies who take this kind of information. And one of the ways these companies because PCI-DSS certified is to make sure they do their penetration testing on a regular basis.

Infiltration tests are a big eye-opener or a check on the internal security team of an organization. How much time does it take for the team to identify attacks and take responsive steps? Does the team realize one of these breaches happened, and how long did it take them to notice what was happening? If yes, what did the team do, and when they did it, was that sufficient to get things done and keep the information safe and secure?

In addition, this will help us figure out what the real effect is on the company if one of these attacks does occur. We can use this kind of testing to see what damage can be done and then calculate the potential loss to the company from this kind of attack and nothing is done. Of course, these is some

theoretical kinds of numbers, and it is hard to know for sure, but we can often take a look at what would happen if they broke into the credit card system, for example, and how much that would cost the business.

It is important to do this kind of infiltration testing because it will allow us to see where the vulnerabilities of the system are, and how we can fix them in order to keep our customers' information as safe as possible. You do not want to leave it all to chance because once a hacker can get onto the system, it could not only cost you a lot of money, but it could cost your customers a lot of money and time, can ruin your reputation, and if you are found to be in violation of the compliance rules, it could get a lot worse.

Many companies will hire out some of this work because they want to make sure that someone on the outside to see if they can get onto the system and cause some of the issues. The tester can go through and figure out where the issues are, and then will make some of the necessary reports and suggested changes the company can choose to follow.

Often this is something that is a big eye-opener to a lot of companies. They may have not realized there were so many problems with their system. And sometimes, these issues show up, even when you go through and deal with a security team that is supposed to protect your system. But even with the recommendations from the penetration tester, it is still up to the business to determine what they want to do with the information, what steps they want to take, and how they will deal with the vulnerabilities and make it all better.

It is not the job of the penetration tester to fix the issues in the computer system unless this is your own personal computer that you are trying to work

with. This is the work of the top management of the company you are working with to determine how they want to handle some of these issues, and what steps they will take to make it a bit better. However, the infiltration tester can provide the top management with the suggestions and recommendations they can follow.

CHAPTER 6: HACKERS: HOW TO FIGHT THEM

Another topic we need to spend some time learning about in this process is the different types of hackers that we will encounter throughout our time in cybersecurity. You will find that there are actually quite a few different types of hackers, but we will spend some time looking at the three main types of hackers that we can work with.

In this chapter, we will focus on black hat hackers, grey hat hackers, and white hat hackers. While all of these individuals will employ some of the same ideas and techniques in order to get the work done with hacking and getting onto a system, they are all going to have different motivations behind the work they are doing. With this in mind, let's take a look at some of the different things we need to know about hackers and how each of these main types is similar and different.

Black Hat Hacker

The first type of hacker we will take a look at is a black hat hacker. This is the type of hacker we will hear about when we hear anything about hacking. This is the type of hacker we will hear about from television, movies, shows, and even from the local media. This is what has given all of the hacking that we ever hear about a bad reputation overall, but it is important to take a look at all of the different types of hackers so we can understand how this world works.

To start, a black hat hacker is someone who works to find the vulnerabilities of a computer security system and then will exploit these vulnerabilities for personal financial gain or for some other malicious reasons. This will differ a bit from the white hat hackers that we will take a look at later. The black hat hackers will try and use the system for their own personal gain while the white hat hacker is someone who works to find and patch up the security flaws that a black hat hacker may try to use for their own gains

It is possible, if you are not using the proper security measures, that a black hat hacker will inflict a lot of damage on your system, whether it is an individual system or a large company, but stealing some of the personal information that is there, compromising some of the security that is found with major systems, or even shutting down and altering up some of the functions that happen with networks and websites.

There are a lot of different options the black hat hacker will work on in order to gather the information they want. They could use keystroke-monitoring programs to get your username and passwords, and even launching an attack in order to disable some of the access that we have to websites that we are using. Malicious hackers, in some cases, will work with methods that don't need a computer to get the data they want, such as calling into a system and assuming another identity to get the password of that user.

Grey Hat Hacker

Now it is time for us to move on to what the grey hat hacker is all about. This hacker is kind of the middle ground. They are not really hired by the company they are trying to get into and gain access to, but they don't

necessarily have malicious intent for doing this kind of hacking either. This is kind of a grey area between the two, and that is why we are working with the grey hat hacker in this section.

A grey hat hacker is a professional who may violate some of the ethical principles and standards of the computer security world, but they do that without some of the malicious intents we will see with the black hat hackers we talked about above. These hackers are often going to engage in some practices that are technically not legal, and are not going to seem like they are above board, but they are often doing it to operate for the common good in the process.

We can think about these grey hat hackers as more of the middle ground. They are not really allowed to be on the system, so what they are doing is illegal. But they are doing this in order to figure out the vulnerabilities and keep the users and safer and informed, rather than stealing the information and using it how they want, before alerting other black hat hackers about these vulnerabilities too.

Many times, when we are talking about hacking, people will see this and IT security as a world that is more black and white. This kind of hacking through will have an important role when we are looking at the environment of security. One of the biggest examples of this kind of hacker that we will see is when someone will exploit a vulnerability of a network in order to spread out some awareness to customers and others that there is this kind of vulnerability.

In this case, experts will say that the difference between the grey hat hacker

and a white hat hacker is that the grey hat hacker will exploit the vulnerability in a more public manner. This can still allow other hackers to take advantage of what is going on and cause issues. But on the other hand, when we are working with a white hat hacker, we may see that they are doing this in a privately and then will alert this to the company without these results going public.

White Hat Hacker

And last, but not least, we need to take a look at what the white hat hacker is all about. This is an individual who is often ignored, or at least not thought about when compared to the other types of hackers. But they are still able to do a lot of the same kinds of processes and hacks that the other two categories can do as well. These individuals will focus more on helping others and making sure businesses and others stay safe, rather than working to steal information and cause trouble.

A white-hat hacker then is a specialist in computer security who can break into a system or a network that is protected, and then test and assess the security that is on that kind of network. These hackers can use some of their own skills in order to improve security for a company by exposing vulnerabilities before some of the malicious hackers, or some of the black hat hackers we talked about above, can find those vulnerabilities and use them for themselves.

Although the methods the white hat hacker will use is similar to what we see with the black hat hackers, the first group actually has permission to use some of their tactics against the organization that has gone through and hired them in the first place. These individuals may work on a freelance kind of

basis, or, in the case with some of the larger corporations who are under attack all of the time, they may employ a team of these specialists at all times.

These kinds of hackers are seen as the ones who will use their skills in a way that can benefit society and others around them. They are sometimes even reformed black hat hackers, although, for the most part, they are individuals who have gone to school and are more versed in some of the techniques and methods that a hacker will use. It is possible for any company to hire these individuals to help them get their network secure and ready to stay as safe as possible.

There are a lot of ways a white hat hacker can help a business they are employed for. Depending on the issue going on, these individuals or specialists can help out with tests, while also implementing some of the best practices that will help companies and organizations be less vulnerable to malicious attempts of hacking them and their information in the future.

Other Types of Hackers

In addition to some of the hackers that we have listed above, there are a few other types, and we will spend a few moments talking about these and what they can do, and how they are different from some of the other three we already looked at.

The first option is a Script Kiddies. This is more of a derogatory term that is used by amateur hackers who are not going to care as much about learning the right coding skills to get the work done. These hackers are the ones who will download tools or use codes that were already available and written by someone else to do the hacking. The primary purpose of doing this is to

impress their friends or even to gain a bit of attention along the way.

However, these individuals will have no want or interest in learning about how hacking works. By using these codes that someone else has taken the time to write and work on, these hackers can launch an attack, without taking the time to look at the quality of the attack they are doing. The most common cyber-attacks by these individuals will include options like DDoS and DoS.

We will also see that there can be a green hat hacker. These are the amateur hackers of the online world. They can be similar to the script kiddies from before, but they have a key difference in that they are willing to learn how to become a full-blown hacker, they just don't have the skills yet. This is what you may be when you start out with this guidebook, ready to learn how to get started by not quite sure how to do it all yet. You may find that these individuals is very involved in their hacking communities and asking a ton of questions along the way.

The way that you can identify these individuals from the script kiddies is by their spark and interest in learning more about the world of coding. Once you answer one question for them, they will listen and then ask a lot of other questions with an intense desire to learn and figure out what will work for the next.

Blue hat hackers. These is another form of novice hacker that will have the main agenda that is to take revenge on those who have made them angry. They want to hack because they see it as a way to have revenge on them. They have no desire for learning and may use simple cyberattacks like flooding your IP with a lot of packets, which will result in DoS attacks.

Red hat hackers are the next on the list. These individuals will have a similar agenda to what we see with a white hat hacker, which is a simple way to say they will try to halt the acts of the black hat hackers. However, the way that they operate these individuals are ruthless when it is time to fight off the black hat hackers.

Instead of just reporting one of the malicious attacks that they see, these individuals believe it is better that they take down that black hat hacker completely. They are more than happy to use revenge against these black hat hackers with a series of aggressive cyberattacks and malware on that hacker. In some cases, this can get so bad the black hat hacker will need to go through and replace their whole system because they can't fix what has happened.

Hacktivist is the next type of hacker that we need to take a look at if you have ever spent some time and seen a social activist propagandizing a social, religious, or political agenda, then you may at some point meet a hacktivist as well. This is basically the online version of what you will see with an activist, even though there are some key differences that show up.

A hacktivist is a hacker or even a group of hackers who remain anonymous, who think that they can bring about some kind of social change based on their actions. And often, they will hack into organizations or the government to gain attention. Sometimes this is just done in order to share how displeased they are over the other line of thought that may oppose their own as well.

And finally, we will take a look at the idea of a malicious insider or a

whistleblower. This will often be some kind of employee who has a grudge against the company or a strategic employee who was compromised or hired by the rivals in order to garner some big trade secrets of their opponents in order to help them stay on top of their game.

Often this kind of hacker will take privilege from their easy access to information, and the kind of role that they have inside of that company, to hack through the system and cause the problems that they want. This makes it easier for them to garner that information because they are already seen as being on the inside of the company, and it is possible that they already have a lot of the needed access rights that are needed to get into this kind of system.

Because there are so many different types of hackers, you can work with on a regular basis. You will find that it is always best to err on the side of caution and watch out for some of the potential hackers who may try to get on your system. Whether you are worried about your own individual system or you are in charge of a large system that needs some care and attention, make sure to be on the lookout for those who want to do you harm along the way.

For the most part, even though the goals and the objectives of each kind of hacker is slightly different, they will rely on a lot of the same techniques and more to get the work done. This is important in order to ensure we can see some good results in the process and that we can actually use the same techniques as the bad guys in order to keep our systems safe and secure.

CHAPTER 7: MORE CYBER ATTACKS: KNOWING THEM TO DEFEAT THEM

We also need to take some time to look at the different types of attacks the hacker can use against us. There are many different ways a hacker can get ahold of our information and get into the system we are using, and if we are not careful with what we are doing, we will end up with a system that is compromised and with a lot of information that is stolen and used against us.

Because there are just so many ways that a hacker can go against us and get on our systems, it can be a difficult task for us to keep the hackers out and to know where they will come from next. The more we can learn about these attacks and work to prevent them from our knowledge, the better off we is. With this in mind, you will find that there are many attacks, and some of the most common ones will include:

Man in the Middle

The first type of attack that we will spend some time exploring is known as a man in the middle attack. This is where a malicious hacker will work and take the right steps in order to insert themselves between two parties, without being seen, in a communication. The goal is to do this without being detected, and for the hacker to impersonate both sides that are going on in this exchange. The hacker can intercept, send, and receive the data meant for either user. Sometimes depending on the information that is being sent, the information handed to the hacker cold be passwords and account numbers.

A typical kind of communication flow will happen between the server and

the client. To access your bank account, for example, you would need to get on the bank website. Your computer, which is the client here, will send in the necessary login information over to the bank's servers. If the servers find the information is correct, then the bank will send back a verification that you were able to sign in properly, and you will then be able to access the account.

This all works well until the hacker can get onto the account and cause some issues. The malicious hacker will work to get onto the network and establish a relay for communication between the real server and the client. This allows the hacker a chance to modify all of the communication between the server and the client.

Instead of the information heading from the client over to the server as it should, the information will get to the relay point, which is the hacker. The hacker is then able to either alter the information sent to the server, alter the information that is sent to the client, or even just read the information and get the passwords and usernames.

For example, maybe the client communicates that they want to send out some money to another bank account. They go through and say that the other bank account should be 222333444. But then the hacker will use a man in the middle attack and will intercept that communication. They may choose to change up the account number.

In this case, the bank is then going to get notified about the transfer requests, and they will get the account number the hacker sends over. They will not be aware any foul play has happened, and is happy to send out the money to the account they assume that you specify. And it is too late before either party

realizes that the theft happened.

Dictionary Attack

The next kind of attack we will take a look at is known as a dictionary attack. This is a method or a technique used to breach the security of a computer, or a password-protected server or machine. A dictionary attack will try to defeat some of the authentication mechanisms because it will go through the process of entering each word in a dictionary as the password. It may also try to use this in order to determine the decryption key of the message or document that the target computer has been able to encrypt before sending it.

The reason that these are so successful is that businesses and individuals will choose ordinary words for their passwords, rather than making it something hard to guess. These ordinary words can often be found in any dictionary you want, and the hacker will exploit this for their own needs.

If you have not gone through and picked out a good and secure password for any of the systems or websites you like to visit, then you will run into some trouble because the hacker will try and gather that information with one of these attacks. They may take some time since all of the words in the dictionary have to be used, but it is very effective for a hacker.

The most common method of a user being authenticated through their system is with a password. This method will continue for a bit more because it is seen as the most practical and most convenient way to authenticate the user who wants to be on the system. Even though it is easy to use, this is often going to be one of the weakest forms of authentication because the users are not good at picking out strong passwords.

Spammers and hackers are more than happy to take advantage of this kind of weakness by working with the dictionary attack that we are talking about now. These individuals will try to get onto your system simply by trying out all of the different passwords that they can think about until they find the one that lets them on.

The good news here is that there are a few countermeasures you can take against this kind of attack. These will include:

1. Delayed response: Having a slightly delayed response from your server is helpful because it will prevent the hacker from checking out more than just a few passwords in a shorter period of time.
2. Account locking: This is where the account is locked out after a few attempts of the password that are not successful. This will make it impossible for the spammer or the hacker to check more than a few passwords at a time.

These attacks is the most effective when the user is not careful with the kinds of passwords that they are choosing. If you go with a really strong password or you go with a system that needs more than one passwords, then this will make it harder for this kind of attack to work the way that the hacker wants.

DOS and DDOS

Denial of Service, or DOS, the attack is used in order to deny some of the legitimate users any access to a website or a resource. They may have trouble getting onto a network, an email, or a website, or they will make use of it really slow. This attack type is done by a hacker who can hit the target

resource, such as the webserver, with way too many requests all coming in at the same time. Because of this rush of traffic all at once, the server is not going to be able to keep up and will fail. This can either have the server slowing down, or the servers will crash down all at once.

Cutting off some business from being online can cost the business a loss of customers and money. The computer networks and internet that we have all come to rely on so much will power many companies in our modern world. Some of the organizations, such as sites of e-commerce and payment gateways, will rely only on the Internet to do business. If they are not able to get online in order to do their work, they will lose a lot of customers and money in the process.

There are five common techniques you will find when we are talking about the DOS attack. First on the list is the Ping of Death. This ping command is usually going to be done in order to test out whether the resource of that network is available or not. It will work because it can send out a small packet of data to the network. The ping of death is then going to take advantage of this and sends the packets above the maximum limit that the IP or the TCP allows.

The TCP/IP fragmentation will break up the packets into smaller chunks that we are then able to send over to the server. Since the sent packages is larger than what our server can handle, it will reboot, freeze, or crash.

Another attack to worry about is the Smurf. This is a type of attack that will use a very large amount of ICMP or Internet Control Message Protocol, ping traffic to the target address. The reply IP address is spoofed to look like that

of the intended victim. All of the replies are then going to be sent over to the victim rather than the IP used for pings. Since a single of these addresses can support at most 255 hosts, a Smurf attack will amplify just one of these pings by 255 times. The effect is the network will slow down so much that it is almost impossible for us to use it.

Then there is the bugger overflow. A buffer is a temporal storage location found in the RAM of our computer that is used to hold onto some of the data that we need, allowing the CPU time to manipulate it before we write it back into a disc. Buffers will come with a size limit. This attack can load up the buffer with more data than it can hold. This will cause the buffer to end up overflowing and will basically corrupt any of the data it is holding onto.

The Teardrop is the next type of data attack that can happen. This attack will work with very large packets of data. The TCP/IP will break them into fragments that are then assembled on the host that is receiving the information. The attacker is then able to manipulate the packets are they are being sent so they can overlap one another. What this will do is cause the target system to crash because it is busy trying to get those packets back in order.

And finally, there is the SYN attack. This is short for Synchronize. We will find that this kind of attack will take advantage of a kind of three-way handshake used to help establish communication between different systems with TCP. This one will work because it will flood the victim with SYN messages that are incomplete. This will cause the target machine to take resources from the memory it never uses and then will end up causing it to deny legitimate users to the system instead.

Ransomware

There are also several types of malware we need to worry about when it is time to protect our data from a hacker. And the first type of malware we will watch out for here is ransomware. This is a type of malicious software that can encrypt some of the files on your computer, or it can be used in order to completely lock you out of that system. It is spread by hackers who will try to lock you out from your files, who will then demand some ransom or money from you. They often claim that if you pay them the fee, they will give you the key to decrypt the information so you can get your files back.

Often the hackers will not let go of the system all the way through. You may or may not be able to get onto your files again, but even if you do, the hacker will usually leave something behind on your system, so they can gain access and do what they want at a later time. There are also a few different options that we will see when it is time to learn more about ransomware, and this will include:

1. Crypto malware: These is some of the most common types of malware that we see, and it is surprising how much damage they can cause. Besides being able to get more than $50,000 from its victims, one of these types of malware options known as WannaCry actually could put thousands of lives at risk when it could hit hospitals throughout the world and made it impossible to access the files of patients in the process.
2. Lockers: These will infect your whole operating system so you are locked out of your computer, and you will not be able to access any of the files or apps you want.

3. Scareware: This is a fake type of software that will come on your computer and claim there is some issue on the PC. These will often demand some money to fix the issue. Some variants will lock the computer, and others can flood your screen with a lot of pop-ups and alerts.
4. Doxware: This one is often called leaks as well, and it is one that will threaten to publish some of your stolen information online if you are not able to pay up. Everyone has some sensitive kinds of files on their computers, so it is easy to see why this can cause some panic and issues for a lot of people.
5. RaaS: This one is known as Ransomware as a Service, and it is some malware that is hosted anonymously by a hacker who can handle everything in exchange for a cut of the ransom that shows up.

Viruses

A computer virus is designed so it can spread from one host to another, and it is even capable of going through and replicating itself. Similar to a way that a flu virus is not able to reproduce without a host cell, this kind of virus on the computer is not able to reproduce or do any of the spreading without programming, such as a file or a document.

In a more technical idea, a computer virus is just going to be a type of malicious program or code that is written in order to alter the way that our computers can operate, and it is designed in a manner that it spreads from one computer to another. A virus can operate because it will insert, or even attach, itself to a program or document that is legitimate, and then can execute its code when the time happens.

Once a virus has had a chance to attack a document, file, or program, the virus will sit there and be dormant until there are some circumstances that cause the system to execute its code. For the virus to actually infect your computer, you need to first run the program that is infected so the virus can see its code executed.

This means it is possible for that virus to remain dormant and doing nothing on your computer for a long time without any symptoms or signs on your computer. But, once the virus can infect your computer, any of the other systems on that network are infected as well. These viruses can do many things such as take over your machine, spam others in your email list, corrupt files, log keystrokes, and steal data and passwords based on how the hacker wrote that program.

In a world that is connected all of the time, you can contract a computer virus in a variety of manners, some of which are more obvious than others. Viruses are spread through so many different areas such as social media, Internet file downloads, text messages, email, and more. It is even possible for this to happen through your smartphones and mobile devices. This is why it is often a smart idea for us to be careful about our attachments or content we share online because it is possible the virus is hidden inside it as well.

Trojan Horses

While we are here, we need to take a look at the idea of the Trojan horse. These Trojans are a kind of umbrella term for the delivery of malware, but there are several different types of these that we can work with. Depending on the intent of the programmer, a Trojan can be like the Swiss Army knife when it comes to hacking. It can work as a tool for some of the other

activities you want to do, as a standalone, and so much more.

To put it in a more simple manner, a Trojan is a strategy of delivering by hackers that will help the black hat hackers to deliver any number of threats from ransomware that will demand money right away to spyware that can conceal itself while it steals a lot of information from the system it is on.

Trojans will look like other things that you are likely to trust. Sometimes they will look like legitimate apps, advertisements about your browser, and free music and software. Any number of behaviors that are unwise from the user can lead to an infection of a Trojan. Some of the most common ways your computer can become infected with one of these Trojans is through the following means:

1. Downloading applications that are cracked. This could be something like a promise of an illegal free copy of a piece of software you want. This can sound enticing, but often these will have a Trojan attack that you need to worry about.
2. Downloading free programs that you are not certain are from reputable companies. What may look like a great screensaver or a free game could easily have a Trojan behind it, especially if you are not certain about the website it is from.
3. Opening an attachment that is infected. You may see this in an email that looks a bit strange but has an attachment that looks important, like a delivery receipt or an invoice. But when you click on the attachment, you will find that it will launch a Trojan when you click on it.
4. Visiting websites that are a bit shady. Some sites only need a moment before they can infect your whole system. Others will trick you like

pretending to stream a movie that is popular, but only if you go through and download a video code, that is a Trojan in reality.

5. We can also see this with any of the other techniques of social engineering that can disguise itself by taking advantage of some of the newest trends that are out there. For example, in December of 2017, there was an extensive installed base of Intel processors that were vulnerable to an attack, thanks to a hardware issue. Hackers were able to leverage some of the panic by faking a patch, and when people agreed to work with this, they would install a Trojan.

Spoofing

And the final type of malware we will take a look at is known as spoofing. In general, we will find that spoofing is the fraudulent practice in which communication is sent from an unknown source, and it is disguised as a source that is known to our receiver. Spoofing is seen when there are mechanisms of communication that will lack a higher level of security that it should have.

Email spoofing is one of the best known of all these spoofs. Since the core SMTP will fail to offer us with some authentication in the process, it is fairly easy for hackers to go through and forge, as well as impersonate, emails. Spoofed emails may request a lot of personal information from the target, and sometimes they can do a good job of looking like they come from a sender you know.

These emails will ask the recipient to provide some personal information, such as an account number, to be used for verifying themselves. The email spoof can use this number to take the identity of the target, can access the

bank account, and change the contact details, and so on.

The hacker will know if the recipient receives a spoofed email that looks like it is from a source they know and trust. This means that they are more likely to at least open the email and even act upon it. So, a spoofed email is also going to contain additional threats to the user, including viruses and Trojan horses, as well. These programs will cause a significant amount of damage to the computer by triggering remote access, activities that are not expected, and deletion of files as well.

As we can see, there are a lot of ways that a hacker can get on your system and cause some troubles. When you are not careful about the security of your system or protecting some of the information there, you will end up with a bit of trouble in the process as well. Taking the right precautions, watching the way you share information online, and more can be important to ensure that you can keep the hacker off and keep your system safe all the time.

CHAPTER 8: PROTECTING OUR INTERNET TRAFFIC

Very few people have a computer without at least some Internet access allowed on it. And most of us will spend the majority of our time online when we are using our computers. This can vary from doing work, checking social media, looking for stuff online, shopping, and even sending and receiving emails. With all of the different things that we can do with our computers over the Internet, it is no wonder that we will try so hard to find ways we can keep our Internet safe. Let's take a look at some of the things you can do to maintain the safety of your Internet traffic so you can use your computer how you want, without running into any risks.

What Is a Network Scan?

One process that we can work on in order to protect the internet traffic that we are working with is to complete a network scan. Network scanning is when we use our computer network in order to gather up information that relates to computing systems. Network scanning is mainly going to be used for system maintenance, security assessment, and also to help a hacker perform the attack they want. There are a number of things that will happen during our network scanning, and some of the most common purposes will include the following:

1. Recognizing all of the available TCP and UDP network services that are running on the hosts that we wish to target.

2. Recognizing what kind of filtering system is there between the user and the hosts that we want to target.
3. Determine the operating systems that are in use by our target system simply by being able to assess the IP responses.
4. Evaluate the target host's TCP sequence number predictability in order to determine the sequence prediction attack and the TCP spoofing.

Network scanning will consist of a network port scanning as well as some vulnerability scanning. This port language is important because it is a method where we will send the packets of data through the network over to the specified numbers of the service port. This is done in order to help us figure out which network services are available for that system. This procedure is the most effective when we are trying to troubleshoot system issues and to help keep the security of your system as strong as possible.

Vulnerability scanning is another method that we can use in order to discover some of the known vulnerabilities of the computing systems that are available on our network. It is there to help us detect the weak spots found in our operating system or application software, which is something that a hacker can crash or compromise for their purposes if we are not careful.

Doing a combination of network port scanning and vulnerability scanning is a good technique to help us gather up information on our network. But when it is carried out by someone who doesn't belong on your system and someone who chooses to remain anonymous, these are seen as a prelude to an attack.

The processes of network scanning, like ping sweeps and port scans, will return a lot of details about which IP addresses will map straight to the active

live hosts, and the different services that these all provide. Another method for doing this, which is known as inverse mapping, will gather up some details about IP addresses that are not going to map a live host, which will help an attacker to focus more on their feasible addresses that are the best to attack.

What Is a VPN?

One way you can keep your network as safe and secure as possible is to work with a VPN or a Virtual Private Network. This is a great thing to work with because it will ensure you can create your own secure connection over to a trusted network while using the internet. You can use these VPNs in order to access some of the region-restricted websites that you want to visit, help to shield some of your browsing activity from others when you are online, and so much more.

It is common for these VPNs to be really popular right now, but sometimes not for the reasons that programmers originally developed them. Originally, these networks were just a way for a business network to connect to another one over the Internet, or to allow you to access your business network when you were traveling or at home.

VPNs will essentially forward all of the traffic of your network over to the VPN, which is where the benefits, like accessing the local network resources in a remote manner and bypassing internet censorship, all come from. The good news is most of the major operating systems will have some VPN support integrated into them.

The VPN will connect to your tablet, smartphone, or PC somewhere on the

Internet, and will allow you to do some browsing using that computer's internet connection. So, if you have a connection to a server that is in another country, then you would be able to access a lot of things you would not be able to do in other situations. So, how will that help you out? There are a number of ways this VPN can help you out, including:

1. Bypass some of the geographic restrictions that are on websites or when it is time to stream video and audio.
2. Watch some of the streaming media that are out there like Hulu and Netflix.
3. Protect yourself from being logged in when you are doing torrenting.
4. Gain at least a bit of anonymity online by hiding the location where you truly are
5. Protect yourself from snooping that happens with some of the Wi-Fi hotspots that are not trustworthy.

The vast majority of people who want to stay safe and keep their information away from prying eyes and hackers will turn to VPNs to help them. One of the popular ways of using this is to bypass many of the geographic restrictions to watch content in a different country. Either way, it can help to hide your location and makes it easier for you to get the things done online that you want in a safe and secure manner.

When it is time to connect to your computer, or one of the other devices that you want to use, and get it hooked up to the VPN< the computer will act as if it can hook up to the same local network that the VPN is on. All of your network traffic is sent over a connection that is secure until it can reach the VPN you choose.

Because the computer behaves as if it belongs to that network, this will make it easier for you to securely access local network resources, no matter where you are located in the world. This means you can use the Internet in the same manner you would if you were in the same location as the VPN. This will have some benefits if you want to work with a Wi-Fi that is public or you want to access websites that are blocked based on where you are located throughout the world.

When you take the time to browse the Web while you are connected to one of these VPNs, your computer can contact the website through our encrypted VPN connection. The VPN is then able to forward that request for you, and then forwards the response that it receives from the website back to the secure connection. If you are using the USA-based VPN to help you get onto Netflix, for example, Netflix will notice the connection is coming from the United States and will provide you with the content that is available there.

There are a lot of good reasons to work with these VPNs. They are a great way to hide the information you are sending online and will make it a lot harder for a hacker to find you and figure out what you are doing online. For those individuals and companies who want to be able to do their work and have fewer worries about how a hacker would be able to get in the middle and cause some issues, working with the VPN may be the best option to choose.

CHAPTER 9: METHODS AND APPLICATIONS

This guidebook has taken some time to look over all of the different parts that come with hacking, especially when it comes to working with the Kali Linux system. Being able to use this system and understand some of the different ways that a hacker can get onto the system and cause some problems is important. But we also need to know some of the steps we can take in order to prevent them from attacking us, and how we can stay safe and secure online.

That is where this chapter will come into play. You will find that with the help of this chapter, we will take some time to figure out how to test out the security of your current network. And then we will move on to some of the tips and tricks that will ensure you can in order to keep your network safe.

How to Test the Security of Your Network

There are a few different techniques that you can try out in order to make sure that you are checking out the security of your network in the proper manner. Using these and ensuring that you add in the right software and tools and pick good passwords can all come into play. However, some of the best approaches and techniques you can use in order to test out the security of your network will include:

1. Network scanning: This is a technique where we work with the port scanner in order to figure out all of the hosts connected to the network.

Network services are also going to be scanned in this. This will help us to ensure whether or not our ports are configured to allow only the right secured network services.

2. Vulnerability scanning: Working with a vulnerability scanner will help us to figure out if there are some weaknesses in that network. It can also help us to learn some more about the security loopholes, which can be improved as well.
3. Ethical hacking: This is a type of hacking that is done in order to identify potential threats to our network. This will help us to identify if there are any possible malicious attacks or access that are not authorized on the system.
4. Password cracking: This is a method that hackers can use in order to crack through some of the weaker passwords on your system. This is a good thing to use because it enforces the policy of your network about minimum criteria for passwords, making sure that everyone has a password that is safe and secure.
5. Infiltration testing: An Infiltration Test is an attack that is done on the system or network in order to figure out what flaws are there. under these techniques, we will compromise all of the parts of the network in order to figure out the vulnerability that might be found in the system and then learn how to fix it.

Simple Tips to Keep Your System Safe

Now that we have spent some time in this guidebook talking about all of the different ways that a hacker can get onto your system and cause issues, it is time to take a look at a few of the steps that you can take in order to make sure that your computer and network are as safe as possible. No one is completely safe in terms of these attacks, and no matter how small or

unimportant you may think you are, you can still become a victim of the attack as well.

The first step that we can take is to make sure your system and all of the software on it is updated on a regular basis. This is a hard thing to work with because these updates seem like an annoyance. But it is really important for us to stay on top of them. Besides being able to offer us new features, they are there to cover up any security holes that can happen on our computer. In most cases, when your operating system or another major software as an update, you will get a notification about it. You can choose to go with updating later or right away.

While it is easy to just forget about the update and assume that you will get to it at a later time, this is not a good thing to do for the safety of your system. In fact, you is much better off to do this right away and get it over with, because it helps to prevent issues with a hacker getting on the system.

The next thing on the list we need to focus on is making sure you always have your wits around you and that you think things through. It is something that should just go without saying, but being suspicious about everything is one of the best things that you can do to make sure that your computer is secure all of the time. while a lot of techniques of hacking are becoming more sophisticated as time goes on, so it is harder to figure out if you are under attack or not, it can also be something simple that takes over as well.

Make sure that you are always stopping and thinking twice before you click or open anything that doesn’t really look legitimate to work with. Do not rely on just the spam filters in order to catch some of the sketchy emails or other

issues that may come through. Remember that criminals are always looking for ways to outsmart some of these settings, and if you are not careful, they will get through.

Enabling a good firewall is the next thing that you need to focus on. A firewall will act as the barrier that you need between your network and the internet. If you have a good firewall in place, you will find that it is effectively going to close up the ports of the computer so that it prevents communication from the outside world with your device. This is a good thing because it provides you with some protection by stopping threats from being able to enter the system and spreading between the other devices that are there. it can also be a good way for us to prevent any data from heading out of the computer.

If you find that there are open computer ports, then anything that comes into them could be processed. This is a bad thing if you are talking about a malicious program that a hacker sent to you. While it is possible to go through and manually close these ports, a firewall is a great defense to help close up these ports. The firewall will open the ports on occasion, but only to external devices on a needed basis and trusted applications it already knows about.

The good news is that most operating systems will come with a firewall, so you just need to make sure that you enable this so that it works. But you can always go through and download and install one if your operating system does not have this feature. It is an extra bit of security for your system that can really do wonders for keeping those hackers out of the way.

We can also work with some adjustments to our browser settings. Most browsers will have some options in place to help us adjust how much privacy and security is present while we are browsing online. These can help us to lower some of the risks of a malware infection reaching the computer and hackers getting on and attacking the device. Some of the browsers out there will even enable you to tell a website that you would not like it to track your movements, simply by going through and blocking the cookies.

We have to keep in mind though that while we have these options, a lot of them is disabled by default, so it is possible that you are exposed or show off more information than is needed each time you get online. The good news is you are easily able to go to your chosen browser settings and make the adjustments needed on most of the common Internet options you want to use.

While we are on the topic of computer safety, we need to make sure that the system has anti-spyware and antivirus software on it. This is because any system or machine that is connected back to the internet will have some kind of vulnerability when it comes to threats from a hacker. Antivirus software can help, even though we must remember that it is not going to catch everything. And while it is possible to find some free options to work with out there, the paid programs are not that much more expensive and can often be a much better option to work with.

Spyware is another option that the hacker can use against us if we are not careful. It is a malware designed to secretly infect some of the computers it touches, and then it will just sit in the system, gathering up information and sending it back on to the hacker. The information is pretty sensitive in nature most of the time and can lead to a lot of problems for the target. Having some

anti-spyware software on your system will help prevent this kind of attack, and will keep your system safe and sound.

And finally, we need to take a look at how we can password protect any of the software that we are using and lock up the devices as well. Most of the software that is web-connected and then you can install on your system will require some login credentials. You need to pick out a good and strong password to use here and remember to not use the same password you have on another account or application.

To take this further, make sure that you have a strong computer password that you want to work with, as well. There are times when someone may be able to gain access physically to your computer, and if you do not have a strong password in place, then you will end up in trouble. a simple line of defense to make sure that you are protected on all sides with your system, no matter what is on it, is to come up with a strong password for the computer, so it is harder for the hacker to enter.

Protecting your system is an important part of making sure that hackers are not able to get ahold of your information and use it in any manner that they choose. Having this setup, and following some of the security tips we talked about in this chapter, and in some of the rest of the guidebook, can be important to keep your system as safe and secure as possible.

CONCLUSION

Thank you for making it through to the end of *Hacking with Kali Linux,* let's hope it was informative and able to provide you with all of the tools you need to achieve your goals whatever they may be.

The next step is to get started with some of the different ways that you can protect your own system and network that we were able to discuss in this guidebook. There are a lot of potential issues that can come up in our ever-connected world. We will find that there are hackers everywhere who would love nothing more than to get onto our systems and steal as much information and cause as much chaos as possible. But with some of the techniques we talked about in this guidebook, you will find that it is possible to handle the issues with hacking and you can keep your system safe and sound.

When you are working with the Kali Linux operating system, it is easier than ever to learn not only how to ethically perform a hack on your own system, but how to keep that system as safe and sound as possible. Most networks and systems are under attack all of the time, and being able to take the right steps to keep your information safe form others is a big issue as well.

That is what we will spend our time on in this guidebook. Learning how to work with the Kali Linux operating system and using it for some of our own needs along the way can make a big difference in how secure and safe our own systems can be overall as well. We will take a look at the processes of network scanning and penetration testing, and look at some of the different

ways a hacker will try and trick you and get information off your system. But with the help of the topics we will discuss in this guidebook, you can take control and ensure no one can get on your network.

There are a lot of things you can do with the Kali Linux system in order to prevent hacking and ensure that no one can steal your information or cause other problems. When you are ready to learn a bit more about Kali Linux and what you can do with this kind of operating system to keep your information safe and protected, make sure to read this guidebook to learn more.

Finally, if you found this book useful in any way, a review on Amazon is always appreciated!