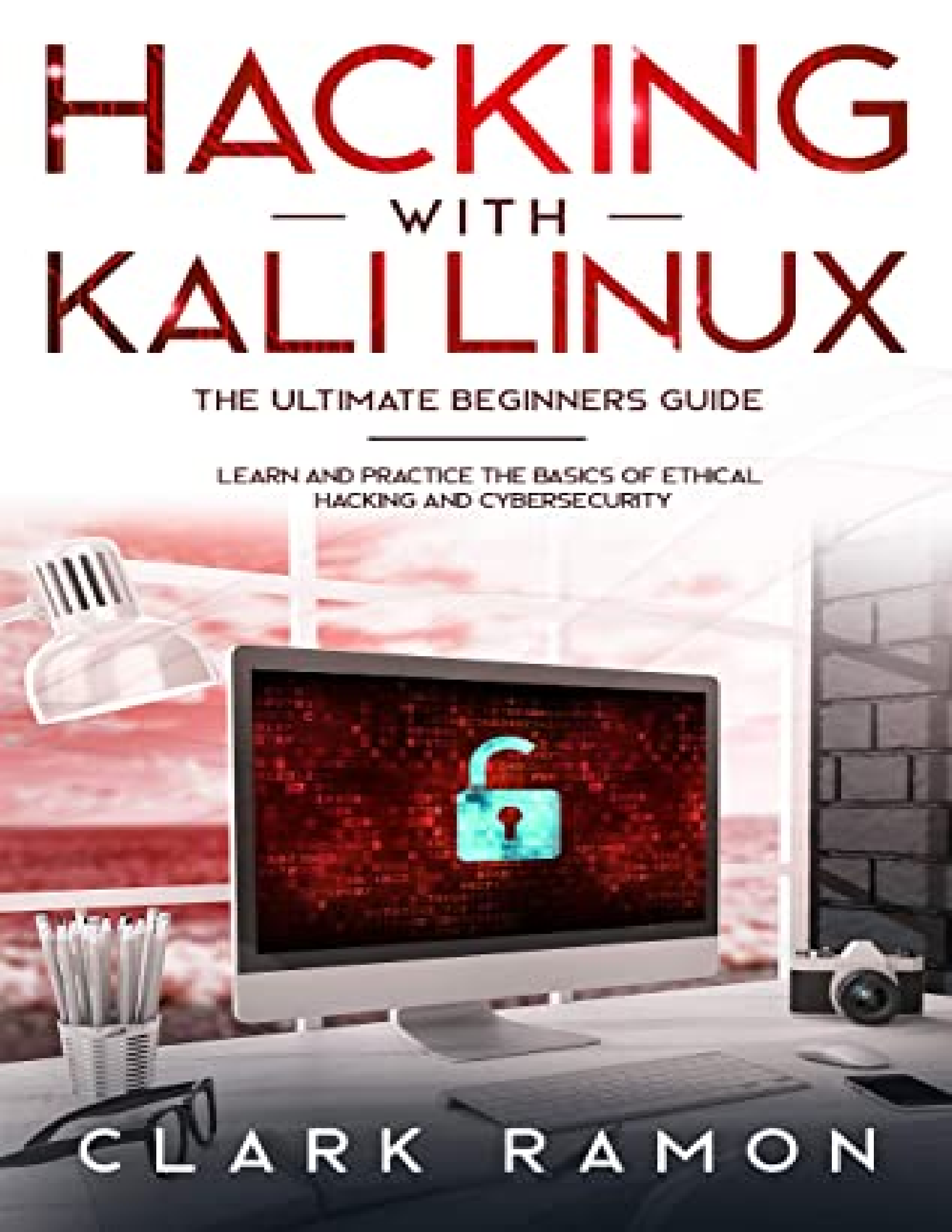
HACKING
— WITH —
KALI LINUX

THE ULTIMATE BEGINNERS GUIDE

LEARN AND PRACTICE THE BASICS OF ETHICAL HACKING AND CYBERSECURITY



CLARK RAMON

HACKING WITH KALI LINUX

THE ULTIMATE BEGINNERS GUIDE

LEARN AND PRACTICE THE BASICS OF ETHICAL HACKING AND CYBERSECURITY

CLARK RAMON

Legal & Disclaimer

The information contained in this book and its contents is not designed to replace or take the place of any form of medical or professional advice; and is not meant to replace the need for independent medical, financial, legal or other professional advice or services, as may be required. The content and information in this book has been provided for educational and entertainment purposes only.

The content and information contained in this book has been compiled from sources deemed reliable, and it is accurate to the best of the Author's knowledge, information and belief. However, the Author cannot guarantee its accuracy and validity and cannot be held liable for any errors and/or omissions. Further, changes are periodically made to this book as and when needed. Where appropriate and/or necessary, you must consult a professional (including but not limited to your doctor, attorney, financial advisor or such other professional advisor) before using any of the suggested remedies, techniques, or information in this book.

Upon using the contents and information contained in this book, you agree to hold harmless the Author from and against any damages, costs, and expenses, including any legal fees potentially resulting from the application of any of the information provided by this book. This disclaimer applies to any loss, damages or injury caused by the use and application, whether directly or indirectly, of any advice or information presented, whether for breach of contract, tort, negligence, personal injury, criminal intent, or under any other cause of action.

You agree to accept all risks of using the information presented inside this book.

You agree that by continuing to read this book, where appropriate and/or necessary, you shall consult a professional (including but not limited to your doctor, attorney, or financial advisor or such other advisor as needed) before using any of the suggested remedies, techniques, or information in this book.

Table of Contents

Introduction:

Given the prevalence of hacking, and the importance of being able to find these vulnerabilities in order to shore them up to protect the network and the data contained within, and prevent unauthorized access, tools have been developed with this in mind, tools which allow hackers to be able to better carry out their tasks with regard to network security such as activities like penetration testing, security auditing, and even computer forensics and reverse – engineering cyber – attacks.

Kali is one such tool, being a Linux distribution structured on Debian that is designed specifically to aid “white hats” in carrying out their assigned tasks, featuring multiple specialized tools and other features that make it much easier for a “white hat” to do their job.

What is a Linux Distribution?

A Linux distribution, often shortened to “distro”, is a type of operating system built from a collection of software based upon the classic Linux operating system kernel, and usually includes a package management system. “Linux” as it is popularly known usually serves as a base for variants, which are often developed specifically for the particular device that the user wishes to use, ranging from embedded devices, to personal computer solutions, and even to massive supercomputers, with the Linux system of packages differing depending on what type of platform they will be run on.

Most Linux distributions are composed of a Linux kernel, GNU tools and software libraries, other third – party software, a window manager, and a specialized desktop environment. Due to the nature of Linux, this often includes free and open – source software that can be found either as a

compiled library or in raw source code, which may allow for various modifications, though most Linux distributions also include proprietary software in their core package, which cannot be modified by the user.

Debian is a type of Linux kernel which Kali is built on, meaning that Debian is a particular build of Linux, and Kali is a build based on Debian, but is not Debian itself. It was developed by programmers Aharoni and Kearns of Offensive Security, basing it on a previous Linux – based incarnation of a security testing Linux Distribution known as “Backtrack”.

The main reason for this rebuild was that though Backtrack was effective, the programmers wanted to build an updated Linux distribution, choosing Debian as their base due to Debian’s reputation as a reliable and stable Linux kernel, as well as due to the expansive software library that Debian had access and compatibility with. It was eventually developed and expanded to what it is today, and it has hundreds of tools designed specifically for security testing and network security purposes, and can be run natively directly from a hard drive, or even booted from a USB or CD, and can also be run on a virtual machine.

Kali Linux was developed with multi – platform support, with both 32 – bit and 64 – bit host formats, developed for compatibility with devices running x86 ARM processing chips, and which can run on other operating platforms such as Android and Windows 10, the former on certain compatible hardware, such as the Nexus line of Samsung phones, and the latter on Windows Subsystem for Linux – capable Windows 10 operating systems, and this is even available from the official Windows Store for download.

Features of Kali Linux

Given the short background of Kali Linux as discussed earlier, it would be beneficial for the reader to have a short overview of the features and specific capabilities of Kali Linux, which should give a clearer idea of what Kali Linux really is and how it is used.

Expansive library of network security and penetration testing tools: Kali Linux found its origins from Backtrack, as previously discussed, and thanks to this, there have been a huge amount of tools developed over time for the Backtrack distribution. However, due to the passage of time, a lot of these tools have been rendered redundant or outdated, and the Kali developers have been able to cut these down, removing the tools that no longer serve the intended purpose, while integrating and adding new and updated tools. Currently, Kali has over 600 penetration testing tools available for its user, and some of the more important and / or notable tools will be discussed later on.

Free – use software: Much like the predecessor, BackTrack, Kali Linux is available for use free of charge, and according to the developers, they intend to keep it that way, making this tool available for download and use without need for any paywall, with all users receiving full functionality of the Kali Linux distribution.

Open Source Git Tree: Kali Linux is freeware, and much like other freeware and many Linux distributions, it is also open source. The developers of Kali Linux are committed to using the open source development model, allowing their development tree to be made public. In addition, all the source code used in Kali Linux is also consistently made available by the developers, for any user that wants to tweak or modify Kali Linux for a specific need.

File System Hierarchy – standard – compliant: The Kali Linux software is adherent to the FHS, or the “Filesystem Hierarchy Standard”, making it

much easier for Linux users to navigate and locate specific files such as binary codes, support files, software libraries, and the like. The use of this standard allows for convenience and ease of use, one advantage that Kali Linux has over a lot of other similar software.

Support for a wide variety of devices: As earlier discussed, the developers of Kali Linux have tried their best to make Kali Linux as user – friendly and versatile as possible, making it compatible with a large range of platforms. Kali Linux is supported by multiple operating systems, and one of the biggest things is that Kali Linux itself supports the use of wireless devices. Not only is Kali Linux compatible with multiple software setups, but also a large range of hardware setups, and the developers are trying their best to include as many hardware configurations as possible. This is quite notable, especially due to the wireless device support, as one of the regular criticisms against most Linux distributions is that they tend to lack support for wireless hardware, which Kali Linux provides.

Custom Kernel: Kali Linux's development team are, first and foremost, penetration testers, meaning that they are often required to do assessments wirelessly, and as such, the kernel of Kali Linux has injection patches constantly included, keeping it up to date.

Secure Development Environment: The Kali Linux team is made up of "white hat" hackers and penetration testers, and as such, they are acutely aware of the need of security, especially when it comes to software that "white hats" often use, as a vulnerability or bug in the software itself can have disastrous and wide – ranging results. As such, the development team is restricted, and they are the only ones who commit packages and interact with Kali Linux's repositories, all of this being done under multiple secure protocols to ensure fidelity and security. In addition, Kali Linux's packages

and repositories are GPG signed, with all packages contained by Kali Linux signed by the individual developer responsible for building and committing it, and each repository also signs the package, allowing for a secure set of software packages and repositories.

Multi – lingual support: Though much of coding and a lot of penetration tools are built on the English language, Kali Linux attempts to include multi – lingual support, allowing non – native English speakers to operate in their native language, making it easier for them to make use of Kali Linux and its features, enabling them to be more effective in carrying out their tasks.

Customization – enabled: As earlier mentioned, Kali Linux is a piece of open – source software, meaning that its source code is open to all. Much like most open source software, and in fact, a lot of Linux distributions as well, Kali Linux can be modified to suit the individual user's needs and tastes, in case they have a differing opinion when it comes to design. Kali Linux is customizable on multiple levels, up until the kernel level, offering advanced users almost total control over their Kali Linux instance.

ARMEL and ARMHF support: ARM – based single – board systems are becoming very popular and widespread, such as the well – known Raspberry Pi microcomputer or the BeagleBone Black, and true to the design philosophy of the Kali Linux team, they did their best to make Kali Linux run on as many platforms and configurations as possible. As such, Kali Linux has robust ARM support, allowing it to work on both ARMEL and ARMHF embedded systems, and are compatible with a very wide range of ARM devices. In addition, Kali Linux's ARM repositories are integrated with the mainline update distribution, meaning that ARM tools are updated along with the rest of the distribution, keeping them up to date and on par with the main tools of Kali Linux.

Why use Kali Linux

Kali Linux was specifically designed for “white hats” and for penetration testing and security testing, among other activities that “white hat” hackers usually do. In accordance to these specialized needs, the Kali Linux distribution has been modified in order to address these requirements, specifically these core changes:

Single – user with root access: Kali Linux is, first and foremost, a Linux distribution centered around security auditing and penetration testing, and it has been tweaked to reflect the needs of that particular setup. A single user setup is there for security purposes, and this allows the user to consistently have root access. The general practice is that root access is only given when necessary, but the nature of penetration testing requires that Kali Linux be given root access thanks to the escalated user access requirements needed by penetration testing and security auditing tools. If Kali Linux were to follow the standard root access only upon demand, this would be quite inconvenient and a burden to the user, hence this particular design choice.

Disabled network services: Kali Linux, in the interest of security, has its network services and capabilities disabled by default, with system hooks that make sure that the network services are disabled, while still allowing services to be installed as needed. Network services are not the only services disabled for security purposes, but even other connectivity options such as Bluetooth are disabled by default, though depending on the user’s needs and preferences, network services can be switched on as required.

Custom Linux kernel: The Kali Linux distribution’s kernel is an upstream kernel specially patched for wireless injection, which allows the kernel to send out information packages on a network connection while making it seem like they are part of the normal communications and information flow,

a key component of a lot of hacking activities. This enables security testers and “white hats” to properly duplicate one of the common avenues of gaining unauthorized access and exploiting weaknesses.

Trusted and curated repositories: Given its nature as a security – focused Linux distribution, one of the developers’ main priorities is keeping Kali Linux secure and safe for use, as a weakness in the distribution or an available exploit would defeat the purpose of Kali Linux. As such, the developers know that system integrity is of utmost importance, and they vet and verify every upstream software source that Kali Linux makes use of, making sure that only the extremely necessary ones are kept in order to minimize risks. Note that a lot of Kali Linux users are often tempted to expand their sources.list resource, but note that doing so has a high chance of breaking the Kali Linux Installation.

Chapter 1. Types of Hackers

All lines of work in society today have different forms. You are either blue collar, white collar, no collar…whatever. Hacking is no different. Just as there is different kinds of jobs associated with different kinds of collar colors, the same goes for hacking.

Hackers have been classified into many different categories, black hat, white hat, grey hat, newbies, hacktivists, elites, and more. Now, to help you gain a better understanding as to what grey hacking is, let's first take a look at these other kinds of hacking, so you can get a feel for what it is hackers do, or can do, when they are online.

Newbies

The best place to start anything is at the beginning, which is why we are starting with the newbie hackers.

The problem with a lot of newbie hackers is that they think they have it all figured out when they really don't. The idea of hacking is really only scratching the surface when it comes to everything that is involved, and it is not at all uncommon for people who want to get into it to get overwhelmed when they see what really needs to be learned.

Don't let that discourage you, however, you are able to learn it all, it just takes time and effort on your part. Borrow books and get online. Look up what needs to be and remember it. Don't rush yourself. You need to learn, and really learn. Anything that you don't remember can end up costing you later.

There are immediate reactions when it comes to the real world of hacking, and sitting there trying to look up what you should have already known is

not going to get you far as a hacker. If you want to be good at what you do, then take the time required to be good at it.

Don’t waste your time if you don’t think you really want to learn it, because it is going to take a lot of your concentration to get to the heart of the matter. Don’t get me wrong, it is more than worth it, but if you are only looking into it for curiosity sake, don’t do it unless knowing really means that much to you.

Sure there are those that kind of know what they are doing, or they can get into their friend’s email account, but that is not the hacking I am talking about here.

I want you to become a real life, capable hacker, and that isn’t going to happen unless you are willing to take the time needed to learn it, and put forth the effort to learn it.

You have to remember that any hacker that is in existence had to start as a newbie hacker, and build up their skills from there. Now, as fast they built those skills depended greatly on how much time and effort they put into working on it, but don’t worry, you will get the hang of things, and while you have to start as a newbie, you will have Grey Hat status soon enough.

Elites

As with the newbie hackers, elite hackers can be any kind of hacker, whether that be good or bad. What makes them elite is the fact they are good at what they do, and they know it.

There is a lot of respect for elite hackers online. Just like with elite anything, they know what they are doing, and they know that others can’t challenge them unless they too know how to handle themselves.

There is a level of arrogance that goes with the status, but it is well deserved. Anyone can stop at second best, but it takes true dedication to reach the top.

An elite hacker can use their powers for good or bad, but they are a force to be reckoned with either way. They know the way systems work, how to work around them, and how to get them to do what they want them to do.

If you have a goal of becoming an elite hacker, you do have your work cut out for you, but don't worry, you will get there. It only takes time and effort to get this top dog status, and it comes to those who want it.

No one'accidently'achieves elite status, it is something that they had to work for, but it is definitely worth all of the time and effort that is put into it.

As an elite hacker, you won't have to worry about whatever system you run into, you will know what is coming, and how you can work around it, it just comes with the line of work.

Hacktivists

Hacktivist hackers use their skills to promote a social or political agenda. Sometimes they are hired by specific groups to get into places online and gather information, sometimes they work all on their own.

The point of this kind of hacking is to make one political party look bad, and the one that the hacker promotes to look good.

Then, they either publish it elsewhere online, or they pass it along so others can see what the person has done or what they are accused of doing. It is a way for politicians to make jabs at each other, and it isn't really playing the game fairly.

The hacker then is either payed by the party that hired them, or, if they are working for themselves, they get to see the results of what they posted about the politician.

The list of hackers and what they do is one that goes on and on, but they all can ultimately fit into three categories, being the black hat, white hat, and grey hats. No matter what kind of hacker they are on top of it, these are the three realms that are really all encompassing.

This is because these are not only hackers in and of themselves, but they are also characteristics of every king of hacker out there. Whether they are doing things for good, for bad, or doing good things without permission, these are really what hacking comes down to.

a. Black hat

The black hat hacker is likely the most famous of the hacking world, or rather, infamous. This is the line of hacking that movies tend to focus on, and it is the line of hacking that has given all hacking a bad name.

A black hat hacker is a hacker that is getting into a system or network to cause harm. They always have malicious intent, and they are there to hurt and destroy. They do this by either stealing things, whether it be the person's information, the network's codes, or anything else they find that is valuable to them, or they can do it by planting worms and viruses into the system. There have been viruses planted into various systems throughout history, causing hundreds of thousands of dollars'worth of damage, and putting systems down for days.

Viruses are programs that hackers create, then distribute, that cause havoc on whatever they can get a grip on. They often times disguise themselves to

look like one thing, and they prompt you to open them in whatever way they can.

Then, once you do open the link, they get into the hard drive of your system and do whatever they want while they are in there. Many viruses behave like they have a mind of their own, and you would be surprised at the harm they can cause.

There is a certain kind of virus, known as a‘backdoor’virus, which allows its sender to then have access to and control of whatever system it has planted itself into. It is as though the person who owns the system is nothing more than a bystander who can do nothing but watch as the virus takes its toll on the system.

Hackers will use these viruses for a number of reasons, and none of them are very good for you. When a hacker has access to your computer, they can then do whatever they like on there.

They can get into your personal information, and use that for their own gain. They can steal your identity, they can do things that are illegal while they are on your computer, and thus make it look like you were the one who did it, and get out of the suspicion by passing all the blame onto you.

These are really hard viruses to get rid of, and it is of utmost importance that you do whatever you can to protect yourself on the outset to make sure you don’t get one of these viruses. However, if you do happen to get one, there is hope. You may have to get rid of a lot of your system, or close it down and restart it entirely, but it is always better to do that then to let a hacker have access to anything you are doing.

Black hat hackers are malicious. They only do what they do to harm others and cause mischief. It is unfortunate that they do what they do, as this is

what made hacking fall under a bad light, but there is hope, because wherever there is a bad thing, there is also some good to be found, and that good comes in the form of the white and grey hat hackers.

b. White hat

The white hat hacker and the grey hat hacker are really similar, but there are key differences that make them separate categories. The white hat hacker is a person who is hired by a network or company to get into the system and intentionally try to hack it.

The purpose of this is to test the system or network for weakness. Once they are able to see where hackers can get in, they can fix it and make it more difficult for the black hat hackers to break in.

They often do this through a form of testing known as Penetration Testing, but we will look more on that later. White hat hackers always have permission to be in the system they are in, and they are there for the sole purpose of looking for vulnerabilities.

There is a high enough demand for this line of work that there are white hat hackers that do it for a full time job. The more systems go up, and more hackers are going to try to break into them. The more hackers that try to do that, the more companies are going to need white hat hackers to keep them out.

Companies aren’t too picky on who they hire to work for them, either, so it is remarkable that so many hackers will choose to go down the black hat path. They could be making decent wages by working for people and getting paid for what they do, but unfortunately not many people see it this way, and they would rather hack for their own selfish gain than to do what would help others.

To put it simply, however, it can be broken down to a very basic relationship. Black hackers try to get in, white hackers try to keep them out. Sometimes the black hats have the upper hand, then there are times when it goes to the whites.

It is like a codependent relationship of villain and super hero, where you are rooting for one but the other still manages to get what they want every once in a while.

It is a big circle that works out in the end. Of course it would be a lot easier if black hat hackers would stop breaking into the systems in the first place, but unfortunately that isn't going to happen.

c. Grey hat

The world is often portrayed as being full of choices that are either right or wrong. You can do it one way, or you can do it any way but that one right way…thus making you wrong.

Right and wrong, black and white. Yet…what about those exceptions to the rule? There is an exception to pretty much every rule in existence, and hacking is no exception. Grey hat hackers fall into this realm.

Whether they are right to do what they do or wrong to do what they do is up to the individual to decide, because it is a grey area.

To clarify what I mean, think about it this way. Black hat hackers get into networks without permission to cause harm. That is bad. Very bad. White hat hackers get into systems with permission to cause protection. That is good. Very good.

But then you have the grey hat hackers. Grey hat hackers get into a system without permission…which is bad, but they get into that system to help the

company or network…which is good.

So, in a nutshell, grey hat hackers use bad methods to do good things. Which, in turn, should make the whole event a good thing. Many people feel that it is the grey hat hackers that do the best job of keeping the black hat hackers at bay, but there are still those that argue the grey hats should not do what they do because they have no permission to do it.

What is important and universal is the fact that a grey hat hacker never does anything malicious or bad to a system, in fact, they do every bit as good as the white hat hackers for those who are in charge of the network, but they do it for free.

In a way, the grey hat hackers can be considered the robin hoods of hacking, doing what they can to help people, unasked, and unpaid, and largely without a‘thank you’even.

In the chapters to come we are going to look at how you can become a grey hat hacker, and how you can get into whatever network you please, as well as how you can help the people who run the network.

Chapter 2. Hacking process

By now, we should have a good idea of what Kali Linux is used for, and what “white hats” are, and ethical hacking. In addition, we have already gone over how to make sure that the Kali Linux that the user is downloading is verified and safe, with no malware or any other modification that would compromise its security. We now also know how to build our own installer image and package of Kali Linux, customizing it to our needs. We’ve already gone over how to install Kali Linux, and even dual – boot it, in case we need such a feature. Now we can go on to some of the basics, how to actually use this program that we’ve learned about, downloaded, and installed.

Step by step, gaining remote access

WiFi hacking is one of the most basic forms of hacking, and is usually taught to beginner white hats to get them familiar with the process. The first step is to find a wireless network to hack: remember that “just trying” or “I’m learning” is not an excuse, and any unauthorized access or attempt to access without authorization may be punishable, so best that you ask permission, or better yet, simply create your own wireless network for convenience.

Now that we have a wireless network to work with, the next step is to find out the name of your own device’s wireless adapter. Note that there are a couple of terms that we should be familiar with: “eth – ethernet”, and “wlan – wireless local area network”. The “wlan” is what we’re looking for, so keep an eye out for that. Boot up your Kali Linux terminal and type in ifconfig, which should show us a lsit of all the terminals of our computer.

Take note of the “wlan” adapter, along with the suffix, which is usually 0 / 1 / 2.

Now that we have our wireless adapter, we now have to enable monitor mode. The user can employ a tool called airmon – ng to create a “mon” virtual interface. This can easily be done by typing

Airmon – ng start wlan0

This should create a monitoring interface, which would be named by default as - mon0 if using an earlier version of Kali Linux, but if using the Kali Linux 2.x onwards, the name would be wlan0mon.

Once the monitoring interface is up, we can begin to attempt to capture data packets that are being transmitted by the wireless network that we are trying to crack into. The following tool should help us gather data:

Airodump – ng wlan0mon

That should allow us to access a few data packets. If we want to save the data in a file, which we do, we add another command to the end, “write *filename*”, so it should look like the following:

Airodump – ng wlan0mon - - write *filename*

That will store any captured packets in *filename*.cap. Once we have about ten thousand data packets minimum stored, we can proceed with the wifi cracking process.

Now that we have our data packets, we can open another terminal and type in:

Aircrack – ng *filename*-01.cap

This should begin the cracking process, or, if there are multiple wireless networks, the program will ask which wireless network will be the target of the crack. Note that if there are multiple wireless networks, the amount of captured data packets needed may be even higher. If the password is fairly weak, then the password should appear in the following format:

Xx :: xx :: xx :: xx :: xx :: xx :: xx …

Remove the colons (so it will be “xxxxxxxxx”), and that should be the password of the wireless network. If the data packets captured aren’t enough, then the program will tell you so, and you have to gather more data packets to have enough to crack into the wifi.

One of the more common attacks, as earlier discussed, is SQL injection in order to gain access to a website or a database. Though the reader should know this by now, just for review: SQL is a structured query language that allows the computer to manage data, in order to store, manipulate, and retrieve data from the server or system database. The database is the repository of all the data, often containing passwords and other sensitive information.

So what is SQL injection? SQL injection is a way of injecting queries into the database. Now the database is specifically meant to answer queries, but only from authorized sources. SQL injection is a method wherein external queries, from unauthorized sources are granted access to the database. This is done through “inserting” them into the normal flow of data queries in order to disguise them as authorized requests for information. This allows the hacker to retrieve the information in the database, whether it be passwords, encryption keys, or even raw data. There are also some SQL injection methods that not only allow for retrieval of information, but even insertion of malware or other files, which may allow the hacker in question

to control the database, either locking out the owner or even deleting some or all the files within. Needless to say, SQL injection is one of the preferred methods of attack by many hackers.

Now, “white hats” can duplicate some types of methods of SQL injection by trying to find vulnerabilities. One of the tools available to a white hat running the Kali Linux distribution is “metasploitable”, a virtual linux machine that will allow a person to practice gaining access and looking for vulnerabilities using the SQL injection method.

The “metasploitable” virtual machine is available online, or may even be contained in the bundle or installation of your Kali Linux. It should include various duplicates of web applications that have vulnerabilities, something that will help the “white hat” learn how to find vulnerabilities and how access to them is gained, which in turn can help the network security professionals find a way to shore up those vulnerabilities by patching them out or developing workarounds.

After installing or opening the “metasploitable” virtual Linux machine, the user can login, with the default username and password of the application being set to “msfadmin”. Once logged in, the user should change the application’s network settings to “bridge”, and restart the machine in order to make sure that the changes have properly taken effect.

How to remove hacking traces

This the climax of the penetration attack. The hacker now has access to the resources available on the database of the organization. The hacker is then free to either extract the information that he sees of value or he is able to take control of the network and use it as a base to launch further attacks against other targeted networks in how we described a DoS attack. By

gaining access to the network, the hacker now has control over one or more devices.

As was the case in the preventative measures of scanning, there are some precautions that administrators and security personnel are able to take to ensure that devices and services are more challenging to access by legitimate users such as black hat hackers. This can involve restricting access of users such who have no legitimate day to day requirement to be accessing the devices. Furthermore, security managers should be closely monitoring the domains and those who are accessing services such as local administrators. Using physical security controls will allow managers to detect attacks that are occurring in real time and can deny access while also alerting the proper authorities to ensure the intruder is exposed.

Another approach which can be taken to ensure that access is denied is to encrypt highly sensitive and confidential information using protection keys. This would mean that any attacker attempting to access the system regardless of how well the system is protected, will gain access only to find that the information is scrambled and with the keys protected, the attacker would have no reliable method for using the data that has been encrypted. Encryption is a good final line of defence for particularly valuable data however it cannot be relied upon entirely in itself. Even if the attacker was to access the system and discover that the data is encrypted, they can still wreak havoc on the network and even disable it, causing significant damage as a means of sabotage. Even more alarming, the attacker could have control over the system and use it for further crimes which could be traced back to the organization's network.

Once the attack has gained access to the system, they are still far from being in the clear. Access is for a limited time, the longer the hacker is operating

from the system, the greater the chances of being caught. The hacker must then shift to the next phase, maintaining access to ensure they are able to collect as much data as possible.

Maintaining Access

The hacker is working against the clock at this point and they must ensure they are able to maintain access long enough to succeed in what they had set out to do whether this was to steal critical data and information or to launch a further attack from the encumbered server. The hacker has been able to avoid detection up until this point, however they are still at risk of being caught and the longer they have access to the system, the higher the risk they could be detected.

Covering Tracks

You are aware that there are a number of attacks launched using the network, which means that hackers do consider access points to be among the most vulnerable aspects of any information technology fortress. If you remember the Heartbleed incident, you would realize that even top corporations can be easily exploited over the network, even causing their more advanced systems to suddenly spit out confidential and encrypted information about their clients. If they are vulnerable, then so are you.

If you suspect that your system has been attacked over your network, or that someone has made an announcement that they are going to hack you, then you have all the right reasons to monitor what is going on in your network and try to find out who your attacker might be. In this chapter, you would also learn what a forensic investigator may gather about an attacker during a network investigation exploitation.

Example Problem Scenario

Your browser is behaving badly and your homepage keeps on redirecting to a page that tells you that your computer is infected with a virus, and then prompts you that you need to purchase a specific antivirus program. In addition, your computer also starts lagging and you see that there are too many ads that are popping up. Not only does this disrupt your work, but it also eats up the resources of your computer.

At this point, you are certain that your computer has been infected. You want to know what it is, and where the infection came from.

Get Wireshark

If you already have Kali Linux (yes, the tool suite that can also be used to launch a network attack), then you already have this tool. You can find it in the Network Traffic Analysis dropdown menu. This interface is capable of creating a live capture on your network's traffic and then analyze the information that is being sent and received on your access points.

Launch Wireshark and do a live capture. You can do that by clicking Capture (found at the menu at the top), and then selecting the active interface.

You will see that there are three windows on your screen. The windows on the upper portion will tell you about the packets that you are receiving, and you will also be given some information about them. The middle window will show you all the bits in your traffic and the packet header's bytes. The lower windows will show you the packet contents both in ASCII and hexadecimal.

If you look at the contents of the packets, you would probably see that there is a messenger packet coming from a device somewhere in the World Wide

Web. You can have a closer look at this packet when you click on it, and then inspecting the details that will appear in the white middle window.

If you are aware that messenger services on your network are disabled, you would see that there would be no other activity should be happening. However, you may notice that there is an ICMP packet in the list that says that it is unreachable by your request. This is most likely a suspicious activity.

Scan the Traffic then Filter It

If you are online, you would see that your computer is receiving a lot of traffic. However, with a device like Wireshark, you would be able to select traffic that you are interested in to verify the data that you are receiving. At the same time, you can also check packets and filter the safe from the suspicious ones. For example, you may see that you are receiving traffic from your reliable antivirus program. When that happens, you can remove that from all the other packets that you see in the window since you are already aware that that specific traffic is coming from a reliable device. To filter the ones that you have already inspected and remove them from view, use this syntax:

!ip.addr == (IP address of traffic)

After doing that, you can focus your attention to other traffic that can be potentially harmful to your computer.

Start Looking at DNS Queries

Check the other traffic that you see on the window. You would probably see that your computer (check for your IP address) is doing standard queries using a DNS protocol to a site that you do not remember accessing while you were using your computer. If you are aware that you are not currently

viewing a site and your computer behaves this way, then you can rule that as a suspicious activity.

Now check the other packets. If your computer's host appears to be requesting downloads from an unknown site, then it is very likely that your computer has a rootkit and the malware is reporting back to its source! The good thing is that you already know where the rootkit is coming from, and you can run a malware scan to remove it from your system. Should you think that you are incurring serious damage because of the rootkit, you can save the results to serve as evidence against the culprit once you report them to authorities.

Detecting Possible DoS Flood Signatures

Since you read about DoS attacks in an earlier chapter, you might also be very interested on how you can possibly see if your ports are being flooded by a hacker with the attempt to deny your service. If you have Wireshark, you can detect the signs of possible waves of packets that are possibly being sent to you by a criminal hacker.

Here's a typical scenario for packet floods such as DoS attacks – if a criminal hacker wants to flood you, he would want to conceal his identity by spoofing IP addresses for each type of packet that he wants to send you. The reason why criminal hackers do this is because they are very aware that it is very easy for many commercial firewalls to detect flooding from a single source and then proceed to blacklisting that IP. Of course, if the huge wave of traffic looks like it is coming from a single source in a small amount of time, then you can just stop the connection coming from that address.

When detecting a DoS attack, you can run a Wireshark capture and look at the ports that are receiving traffic. If you see that there are too many IPs that

are sending traffic to a single port, and that the packets that they are sending are coming to you in suspiciously small intervals, then you know that someone is trying to destroy (or at the very least, bog down) your network.

Making Sure that Your Network is Safe

By making sure that you are aware whenever someone is trying to send you a port scan, you would be able to secure your network and prevent any network-related attack. The only proven way to do this is to have a person monitoring the traffic that is coming in to your system, and then making sure that all data requests coming online are legitimate. Once there is a suspicious activity going on, then it is time for you, the ethical hacker, to carry out the next step in thwarting a possible attack.

What could you possibly do during a possible attack? You can simply try to find all the suspicious incoming connections and then ban them from connecting to you. This way, you would not have to deny service to anyone who should really be accessing your network – and this is of importance if your business depends on being able to offer access. In other words, you should always consider the possible repercussions of every step you take against possible attacks.

Chapter 3. Kali Linux

Now that we have our downloaded Kali Linux file, presumably using the official ISO download to ensure it is free from malware, and with the proper ISO build in order to match the user's hardware and software set – up, the next step is to actually begin the installation process. Of course, the installation is necessary in order to use Kali Linux, and there are multiple ways we can install Kali Linux, from the most basic method: placing it on the system's hard disk drive; to more advanced methods, such as dual – booting Kali Linux with other operating systems. Let's get started!

Installing Kali Linux on your machine

Let's start with the most basic method of installation of the Kali Linux distribution: placing it on our system's hard disk drive. By now, the user should have already ensured that their system hardware is compatible (as a reminder, Kali Linux supports i386 / 32 – bit systems, amd64 / 64 – bit systems, and ARM / armel / armhf systems). The next step is ensuring that the system hardware, in addition to having compatible system architecture, should also meet the minimum hardware requirements, which are as follows:

Installing Kali Linux on your hard disk drive

Minimum of 20 gigabytes of free hard disk drive space for Kali Linux's installation

Minimum of 1 gigabyte of random access memory (RAM) for i386 and amd64 – based architecture (The more RAM the system has, the better the performance)

Native CD – DVD drive support, or USB boot support

Note as well that the i386 default images have PAE kernels enabled by default, so they can be run on systems that have above 4 gigabytes of RAM. Once the system hardware matches the Kali Linux compatibility and performance requirements, the ISO that was downloaded or rebuilt should be burned to a DVD, or a USB stick with the Kali Linux Live installation media should be readied. Note that in case there is no CD – DVD drive support, nor USB boot support, another option exists, being the Kali Linux Network Install, which will be discussed in a following section.

Installation Procedure

Once everything is ready, i.e all the requirements are met, and the Kali Linux software has been prepared and is ready to be installed, the first step would be to insert the installation media and boot it / run it (through the USB boot or the CD – DVD drive). Booting the medium should result in a window appearing with multiple options, such as “Live (amd64)”, “Graphical Install”, or simply “Install”. The “graphical install” enables a GUI install, and the “install” initiates a text – mode installation process.

Once the installation method is selected, the window will then request the user to select their preferred system / software language, as well as place their country’s location. In addition, a prompt may come out to request the user to configure their keyboard for the appropriate key – mapping. Once the language – country combination has been selected, and the keyboard properly mapped, the next step will be to input the geographical location of the user. Pressing “continue” after this step will instruct the installer to begin the process of installing the image by copying it to the hard disk drive, as well as probing the network interfaces of the device.

Once these steps are complete, the installer will request the user to input the host name of the system. The purpose of the host name is to identify the

system to the network that it is connected to. The host name can be selected by the user, and can be changed in the future. The next step is to choose a domain name, which forms part of the computer's address, found on the right side of the host name. This domain name is usually seen as the ".com", ".edu", ".net" suffixes. Note that this step is entirely optional, but if used, it would be prudent to ensure all the computers on the network share the same domain name to avoid errors or confusion.

Once the host and domain name have been selected, the system will then prompt the user to provide a name for the user account. Note that this account will NOT have root access, and is meant to enable the system to have an account that can carry out non-administrative activities without admin – access for safety purposes. Upon providing a name, a user – ID will be created based on the given account name, but this ID can be edited to match the user's preference.

Once all the naming conventions have been set up, the system will check and configure the clock, by requesting for the time zone wherein the user is located. Note that this step still occurs even after having chosen the geographical location, and in fact it notes that in case the time zone the user is in is not listed, they can simply go back and choose the country they are currently located in.

After choosing the partition, the system installer will prompt the user one more time to check whether or not their chosen configuration is what they really want, allowing the user to double – check their configuration options, as installing the Kali Linux software makes numerous disk changes, and making an error in installation may cost a lot of time and effort to reverse and / or remedy. Once the configuration is confirmed, the installer will begin installation on the partitioned drive, and the result will be a near –

complete installation. After this, the network mirrors can be configured by the user, and as Kali makes use of a central repository for the distribution of applications, it is necessary to set the network mirrors. Note that it may be possible that the installer will require the user to enter proxy information in case their network makes use of a proxy.

Once the network has been set up, one of the final steps is to install the “GRUB” boot loader in order to be able to boot Kali Linux. Note that in case there are no other operating systems currently installed, the user may choose to have GRUB as the master boot loader. In case of other operating systems, selecting GRUB as the master boot loader may render the other operating systems temporarily unbootable, but this may be fixed by manually changing the configuration later on in order to reset it. Once this is done, the user only has to reboot their system by clicking “continue”, and this should reboot and load the newly – installed Kali Linux operating system.

Installing Kali Linux over a network (Preboot Execution Environment)

As earlier mentioned, the conventional method of installing Kali Linux requires either a USB boot capability or a CD – DVD drive that can be used for the installation media to be loaded on the system. A lot of the time, this method is used for business or enterprise Kali Linux deployments, where multiple devices need to have the Kali Linux distribution pre – loaded onto them in order for use. This pre – seeding can be done over the network, which is something useful especially when the devices have their USB and CD – DVD ports and drives disabled, as is common practice for business laptops and computers.

The first step in getting the Kali Linux distribution installed over a network, through a PXE (pre – boot execution environment), is to install the “ **dnsmasq”** , which provides the DCHP / TFTP server. Once the **dnsmasq** is installed, the next step would then be to edit the **“dnsmasq.conf”** file.

The previous code installs the **dnsmasq** . The following snippet of code will then allow the user to enable the boot – up of the DHCP, TFTP, and PXE, as well as allow the user to set the dhcp – range to match the environment. In addition, the gateway as well as the DNS servers can be re – defined using the dhcp – option directive as needed.

After all the necessary changes have been made, the **dnsmasq** must be restarted in order for these changes to properly take effect.

Once the **dnsmasq** has been restarted and the changes have taken effect, the next step is to make sure that the directory that will be holding the image of the Kali Linux netboot has been created, and that the proper image has been downloaded from the proper Kali Linux repositories.

That should create the requisite directory and initiate the needed download. The user can then simply boot the system that they intend to install Kali Linux on and configure it to boot from the connected network. The connected device should automatically retrieve an IP address from the PXE server and begin the Kali Linux installation process.

Installing Kali Linux as an encrypted disk install

Preliminary Requirements

Ensure that the device that they want to run Kali Linux on is properly protected, and in those cases, they may wish to create an installation that is encrypted with a secure password. By now, the user should have already

ensured that their system hardware is compatible (as a reminder, Kali Linux supports i386 / 32 – bit systems, amd64 / 64 – bit systems, and ARM / armel / armhf systems). The next step is ensuring that the system hardware, in addition to having compatible system architecture, should also meet the minimum hardware requirements, which are as follows:

Minimum of 20 gigabytes of free hard disk drive space for Kali Linux's installation
Minimum of 1 gigabyte of random access memory (RAM) for i386 and amd64 – based architecture (The more RAM the system has, the better the performance)
Native CD – DVD drive support, or USB boot support

Note as well that the i386 default images have PAE kernels enabled by default, so they can be run on systems that have above 4 gigabytes of RAM. Once the system hardware matches the Kali Linux compatibility and performance requirements, the ISO that was downloaded or rebuilt should be burned to a DVD, or a USB stick with the Kali Linux Live installation media should be readied. Note that in case there is no CD – DVD drive support, nor USB boot support, another option exists, being the Kali Linux Network Install, which will be discussed in a following section.

Installation Procedure

Once everything is ready, i.e all the requirements are met, and the Kali Linux software has been prepared and is ready to be installed, the first step would be to insert the installation media and boot it / run it (through the USB boot or the CD – DVD drive). Booting the medium should result in a window appearing with multiple options, such as "Live (amd64)", "Graphical Install", or simply "Install". The "graphical install" enables a GUI install, and the "install" initiates a text – mode installation process.

Once the installation method is selected, the window will then request the user to select their preferred system / software language, as well as place their country's location. In addition, a prompt may come out to request the user to configure their keyboard for the appropriate key – mapping. Once the language – country combination has been selected, and the keyboard properly mapped, the next step will be to input the geographical location of the user. Pressing "continue" after this step will instruct the installer to begin the process of installing the image by copying it to the hard disk drive, as well as probing the network interfaces of the device.

Once these steps are complete, the installer will request the user to input the host name of the system. The purpose of the host name is to identify the system to the network that it is connected to. The host name can be selected by the user, and can be changed in the future. The next step is to choose a domain name, which forms part of the computer's address, found on the right side of the host name. This domain name is usually seen as the ".com", ".edu", ".net" suffixes. Note that this step is entirely optional, but if used, it would be prudent to ensure all the computers on the network share the same domain name to avoid errors or confusion.

Once the host and domain name have been selected, the system will then prompt the user to provide a name for the user account. Note that this account will NOT have root access, and is meant to enable the system to have an account that can carry out non-administrative activities without admin – access for safety purposes. Upon providing a name, a user – ID will be created based on the given account name, but this ID can be edited to match the user's preference.

Once all the naming conventions have been set up, the system will check and configure the clock, by requesting for the time zone wherein the user is

located. Note that this step still occurs even after having chosen the geographical location, and in fact it notes that in case the time zone the user is in is not listed, they can simply go back and choose the country they are currently located in.

After choosing the partition, the system installer will prompt the user one more time to check whether or not their chosen configuration is what they really want, allowing the user to double – check their configuration options, as installing the Kali Linux software makes numerous disk changes, and making an error in installation may cost a lot of time and effort to reverse and / or remedy. After the confirmation, the Kali Linux installer will require the user to set a password, which will be required every time that the Kali Linux instance is booted up. Once the password is verified, the user can simply click “continue”.

Once the configuration is confirmed and the password selected, the installer will begin on the partitioned drive, and the result will be a near – complete installation. After this, the network mirrors can be configured by the user, and as Kali makes use of a central repository for the distribution of applications, it is necessary to set the network mirrors. Note that it may be possible that the installer will require the user to enter proxy information in case their network makes use of a proxy.

Once the network has been set up, one of the final steps is to install the “GRUB” boot loader in order to be able to boot Kali Linux. Note that in case there are no other operating systems currently installed, the user may choose to have GRUB as the master boot loader. In case of other operating systems, selecting GRUB as the master boot loader may render the other operating systems temporarily unbootable, but this may be fixed by manually changing the configuration later on in order to reset it. Once this

is done, the user only has to reboot their system by clicking “continue”, and this should reboot and load the newly – installed Kali Linux operating system.

Dual Booting Kali Linux and the Windows Operating System

Some users may have a need of having two operating systems on one device – for example, budget constraints may mean that they can only really afford to have one device, so they need their laptop to be able to multi – task, or perhaps the user simply prefers to have the option of using Kali Linux on their Windows – loaded device. Whatever the reason, Kali Linux can be dual – booted alongside the Windows operating system.

For the purposes of this particular tutorial, we will be assuming that the Windows operating system will be taking up the full capacity of the hard disk drive’s space, and as such, we will teach the reader how to partition the hard disk drive in order to lessen the dedicated size for Windows, enough that the user will be able to boot Kali Linux.

Much like any other Kali Linux installation, the user has to ensure that the system hardware, in addition to having compatible system architecture, should also meet the minimum hardware requirements, which are as follows:

Minimum of 20 gigabytes of free hard disk drive space for Kali Linux’s installation (after re – partition)
Native CD – DVD drive support, or USB boot support

Note that the creation of a dual – boot is not possible using the PXE system, meaning that native CD – DVD drive support or USB boot support is indispensable when creating the dual – boot setup.

Creating a Partition

In order to create a partition, the installation media should be booted – this means loading the downloaded Kali Linux ISO or booting the Kali Linux Live, whichever is applicable. Booting the medium should result in a window appearing with multiple options, such as “Live (amd64)”, “Graphical Install”, or simply “Install”. The “graphical install” enables a GUI install, and the “install” initiates a text – mode installation process. Once this is loaded and the menu has opened, the “Live” option should be selected. This “Live” option will boot up the Kali Linux desktop and allow the user to access some of the applications and tools.

The tool that we are looking for here is the **GParted** program. The user should look for and launch the **GParted** program. Linux distribution.

Once the **GParted** program has launched, there will be options available to the user. There will be a list of partitions, and the user has to select the partition that has Windows loaded on it. Where it is situated on the list will depend on the user’s configuration, but most configurations have it as the second and larger – sized hard disk drive partition. Once the partition containing the Windows boot is selected, simply right – click the partition and select “resize / move” in order to resize the partition in question. Resize it in such a way that there will be at least twenty gigabytes (20 GB) in the “unallocated” portion, as this will be used for the Kali Linux installation further on.

Upon resizing, there should be a button on the application dashboard shaped like a green check – mark, which is an “Apply All Operations” button. Simply click this in order to finalize the partition. Once the partition

has been finalized, simply exit the **GParted** application and reboot the system. This should re – size the hard disk drive and free up enough space for the user to install a fresh version of Kali Linux.

Installation Procedure

Once the hard disk has already been properly partitioned, simply run / boot the installation media once again and select the install option. Follow the same steps as provided in the section of “Installing Kali Linux on your hard drive” with one key difference, notably the selection of the partition option, which will be shown in the next paragraph.

Upon completion of the preliminary steps, i.e language, location, time zone, and keyboard mapping, the installer will now probe the system’s disks and offer five possible choices for installation. These choices are: guided – use the largest continuous free space (note that this is a non – default option that only shows up once a partition is created using the **GParted** application). Upon selection (in this case, “guided – use the largest continuous free space” option should be used), the system installer will now install the Kali Linux distribution on the previously “unallocated” space that we previously freed up by making use of the **GParted** application. The system installer will give the user the option to have “all files in one partitioned” as the default recommended option, but also allows for a separate / home partition as well as a separate / home, / usr, / var, and / tmp partition setup.

How to work with Kali Linux

Before a hacker can hack into a system, he or she must complete certain processes. Some of these are:

1. RECONNAISSANCE

To avoid being hacked, you should keep your private information very secure. The word “reconnaissance” in this context is a means by which the hacker tries to gather all information regarding you (the target) and any weak spots in your system. The hacker uses this step to find as much information as possible about the target.

2. SCANNING AND ENUMERATION

Scanning involves the use of intelligent system port scanning to examine your system’s open ports and vulnerable spots. The attacker can use numerous automated tools to check and test your system’s vulnerabilities.

3. GAINING ACCESS

If the hacker was able to complete the two phases above, his/her next stage is to gain access to your system. This stage is where all of the hacker’s fun will begin. He or she will use the weaknesses discovered during the reconnaissance and scanning of your system to break into your connection. The hacker could exploit your local area network, your internet (both online or offline) or your local access to a PC. In the real sense, the moment a hacker breaks into your system or network, the hacker is considered to be the owner of that system. The security breach refers to the stage in which the hacker can use evil techniques to damage your system.

4. MAINTAINING ACCESS

In the previous phase, we said that once a black hat hacker hacks your system, it is no longer yours. In this phase, after the hacker has breached your security access and hacked your system completely, he or she can gain future access to your computer by creating a backdoor. So even if you get access to that computer system or network again, you still can’t be sure you

are in total control. The hacker could install some scripts that would allow access to your system even when you think the threat is gone.

5. CLEARING TRACKS

The hacker gained access to your system and at the same time maintained access to that system. What do you think the hacker will do next? The hacker will then clear all of his or her tracks to avoid detection by security personnel or agencies so that he or she can continue using the system. In other cases, the hacker may do this just to prevent legal action against him or her. Today, many security breaches go undetected. There have been cases in which firewalls were circumvented even when vigilant log checking was in place.

By now, you should have some insight into what hacking is all about. Now we will outline the fundamental security guidelines that will protect you, your system and your information from external threats. All of the information we will provide is based on practical methodologies that have been used successfully. These methodologies will help prevent a computer system from being attacked and ravaged by malicious users.

Update Your OS (Operating System)

Operating systems are open to different types of attacks. On a daily basis, new viruses are released; this alone should make you cautious because your operating system might be vulnerable to a new set of threats. This is why the vendors of these operating systems release new updates on a regular basis, so that they can stay ahead of new threats. his will help you improve your security and reduce the risk of your system becoming a host to viruses.

Update Your Software

In the previous section, we talked about the importance of an update. Updated software is equipped with more efficiency and convenience, and even has better built-in security features. Thus, it is imperative that you frequently update your applications, browsers and other programs.

Antivirus

Based on our research, we have seen that some operating systems are open to a lot of attacks, especially Microsoft or Windows platforms. One way you can protect your system from viruses is through an antivirus program. An antivirus program can save you in many ways. There are many antivirus programs (free or paid) that you can install on your system to protect against threats. A malicious hacker can plant a virus on your system through the internet, but with a good antivirus scan, you can see the threat and eliminate it. As with any other software or program, your antivirus software needs frequent updates to be 100 percent effective.

Anti-Spyware

This program is also important, as you don’t want trojan programs on your system. You can get many anti-spyware programs on the internet; just make sure you go for one that has received good ratings.

Go for Macintosh

The Windows operating system is very popular and therefore many hackers and crackers target it. You may have read articles and blogs saying that Macintosh operating systems are less secure; however, Macintosh is immune to many threats that affect Windows. Thus, we urge you to try the Macintosh platform. However, as we have explained in other chapters, no system in the world is completely hack-proof, so don’t let your guard down.

Avoid Shady Sites

When you are browsing Facebook, you may come across unknown people who send you messages with links, some in the form of clickbait. Avoid clicking on such links. Also, you must avoid porn sites, or sites that promise you things that are too good to be true. Some of these sites promise you free music when you click on a link, while others offer free money or a movie. These sites are run by malicious hackers who are looking for ways to harm your computer with their malware links. Take note that on some malicious sites, you don't even have to click on anything to be hacked. A good browser will always inform you of a bad site before it takes you there. Always listen to your browser's warnings and head back to safety if necessary.

Firewall

If you are a computer specialist working in an organization, you might come across cases in which more than one computer system's OS is under one network. In situations like these, you must install software that provides a security firewall. The Windows operating system has an inbuilt firewall that you can activate and use directly. This firewall feature comes in different versions of Windows, including Windows XP, Windows Professional, Windows 10 and the other versions.

Spam

You can be hacked from spamming too. Email providers have taken the initiative to classify emails according to a set of parameters. Some emails will be sent directly into the inbox and some will be sent to the spam folder. To be safe, avoid opening emails that look suspicious. Some of them will have attachments that you should not open. Regardless of the security measures taken by email providers, some spam emails will still pass their

filters and come straight into your inbox. Avoid opening such emails and do not download the attachments that come with them.

Back-Up Options

Some files will contain confidential information, such as personal files, financial data and work-related documents you cannot afford to lose. You should register with Google Drive, Onedrive and other cloud drive companies so that you can upload your files as a form of backup. You can also purchase an external hard disk and transfer all of your important files to it. Take all these security measures because a single malicious software can scramble your data regardless of the antivirus you have installed. You can’t reverse some actions once they’ve been taken, so always have a backup.

Password

This is the most important aspect of security. The importance of a strong password can never be overstated. Starting from your e-mail, your documents or even a secure server, a good password is the first and last line of defense against external threats. There are two categories of passwords: weak and strong. A weak password is made by using your mobile phone number, your name, a family member’s name or something that can be guessed easily. Avoid using this kind of password, as even an amateur hacker can guess it.

Some people use dates such as their birthday or a special anniversary; however, that is still not safe. When creating a password, take your time and do some basic math because your password must contain both letters and numbers. You can even combine it with special characters. For instance, if your initial password is “jack,” you can make it “J@ck007.” A password like this will be almost impossible to guess even though it’s simple.

Furthermore, avoid writing down your passwords. Your password isn’t a file that needs backup; it must be personal to you. Make sure you use a simple password that is very strong. However, keep in mind that a strong password still doesn’t make you completely safe.

GENERAL SAFETY TIPS

At this point, you should have an in-depth idea of what hacking is all about and some guidelines for ensuring the safety of your computer system or network. Following are general tips to follow to avoid becoming a victim of hackers.

· When you log into your email, you should avoid opening emails from unknown sources. Most importantly, do not download any attachments that come with such emails.

· Do not visit unsafe websites. Always visit websites that are secured, such as sites with “https”. Try to only engage in safe browsing.

· Before you install a new program, make sure the program is scanned to ensure it is free of viruses. Then, you want to delete any old installation files because you now have the new installation files. This can save you if a hacker uses those old files as a backdoor.

· Scan your files from time to time. Also make sure that all of the applications on your system are updated frequently to the latest version.

· If you work at home, make sure you are in contact with security professionals or firms that can help you check network loopholes and rectify them as soon as possible.

· Always back up your files. You can use safe cloud drives such as Google Drive or Dropbox. You can also purchase an external drive to keep your

important files safe and intact.

· Are you on a social network? Avoid clicking on links sent by people you don’t know. Such tempting messages can be invitations to private chat rooms or promises of money if you click on the links. Avoid them and stay safe.

· As technology is improving, so are software developers. Always make sure you are surfing the internet with a good browser. For instance, some browsers have inbuilt virus or danger detection bots, which will alert you if you are trying to access a web page that is not safe. When you want to download a browser, go for one with better inbuilt security features. The following browsers are recommended:

a) Google Chrome

b) Mozilla Firefox

c) Safari

· Use the features that matter to you when you are connected to the internet with your browser. For instance, if you are not using Java or Active X while you are connected, deactivate them in your browser. Having them connected all the time is not safe.

· Research has shown that the most secure operating systems are Linux and Macintosh. If the these two systems meet your needs, it is recommended that you switch to them. They are more secure, as they have had fewer incidences of hacking compared to the popular Windows systems.

· When you sleep, you can still be attacked if your computer system is on and idle or in sleep mode. To prevent this, make sure your computer is completely switched off when you are not using it.

Hacking with KAli Linux

Given all these features and modifications made to the Linux Debian system in order to make it useable for security testers and “white hats”, the question now is, what makes Kali Linux the proper tool for a “white hat” hacker? One would think that due to its thorough security features and wide range of capabilities, that anyone would want to use Kali Linux. However, its specialized nature means exactly that; Kali Linux is designed specifically for professionals, for security specialists, penetration testers, and other types of “white hats”. As such, Kali Linux offers little to no utility if the user wishes to have a Linux distribution that is for general – purpose use, or a specialized distribution for development, design, gaming, and Kali Linux is especially not recommended for beginner users of Linux.

Note as well that while Kali Linux is a type of open – source software, it’s not entirely widely open – source, mainly for security reasons. Thus, the development team is kept small, with packages and repositories signed by each team member that uploaded it as well as the team as a whole for verification and security purposes, and the amount of upstream repositories used are kept to a minimum, with as few updates and packages drawn from them as possible, again all in the interest of security. This configuration means that adding new repositories or packages that have not been fully vetted by the Kali Linux team is wont to cause problems, and may just break the installation of Kali Linux. Though as discussed earlier, Kali Linux was designed and intended to allow for a very high degree of user customization, the user still has to know what packages and repositories are compatible with Kali Linux, as adding unrelated or unvetted packages or software repositories will still most likely lead to bugs. For example, while Kali Linux has a lot of features, it does not support the apt – add –

repository command, PPAs, or Launchpad, showing exactly the intent of the developers. Other unrelated programs such as Steam will also most likely not end well, and the Kali Linux distribution will most likely not work out well if that is the user's intent.

Even the insertion of some mainstream software packages such as NodeJS can take a bit of effort and know – how, but then, what Linux distribution doesn't? However, due to the advanced nature of Kali Linux, it would require more than just a basic level of sys – ad competence in order to make proper use of and unlock the full potential of the Kali Linux distribution. This is also another reason why Kali Linux is not recommended for beginners, as the specialized nature means that it is difficult to learn from scratch, and as it is highly specialized, the knowledge that one may pick up from learning Kali Linux may not be applicable to other Linux distributions as a whole.

Last but not least is that due to the fact that Kali Linux was developed as a "white hat" tool, and contains numerous security and penetration testing tools, it may be possible that these tools may be used improperly if the user is not quite familiar with what they are doing. Misuse of these tools, especially on a network where the user was not given express authorization, may result in damage, either to the system or the network, and may also result in numerous consequences, be it personal or legal. Take note that while this is the reason for network services being deactivated by default, if something happens, "not knowing what I did" is not a valid excuse, and an inexperienced user may just find themselves landing in hot water.

However, for professional penetration testers or "white hats", or even for those who are still studying or practicing with the aim of becoming a

professional, Kali Linux has one of the best and most expansive toolkits available, especially at its price point – free.

Chapter 4. Bash and python scripting

So why do we even use Python for collaborative processing? Even though GIL does not allow CPython programs with multiple threads to get all the advantages of multiprocessor systems in certain situations, most of the operations with blocking or long-term execution, such as input / output, image processing, as well as grinding numbers in NumPy, occur outside the existing one. Gil Thus, the GIL itself becomes a potential bottleneck only for programs with many threads that spend significant time inside the GIL. As you will see in subsequent chapters, multithreading is just some kind of co-processing programming, and although the GIL does make certain calls for multithreading CPython programs that allow more than one thread to access shared resources, other forms of parallel programming do not have this problem. For example, applications with many processes that do not share any common resources between processes, such as input / output, image processing, or grinding NumPy numbers, can work seamlessly with GIL.

In addition, Python has gained increasing popularity in the programming community. Thanks to user-friendly syntax and general readability, more and more people believe that it is relatively easy to use Python in their development, whether it’s a beginner learning a new programming language, users with an average level of training in searching for available modern Python functionality, or experienced Programmers using Python to solve complex problems. There are estimates that Python code development can be up to 10 times faster than C / C ++ coding.

A large number of developers using Python have come about as a result of a powerful, still growing community. Every day, Python libraries and packages are developed and released, supplying various tasks and

technologies. Currently, Python supports an incredibly wide range of programming - namely, software development, GUI workstations, video game design, web and Internet development, as well as scientific and numerical calculations. In recent years, Python has also grown as one of the top tools in data science, Big Data, and machine learning, competing with a long-term player in the field, R.

Running Python Scripts

To excel in Python programming, it is essential for you to have an in-depth knowledge of how to run scripts and code in Python. It is imperative because scripts and codes are the only way with which you can check the functionality of your codes. So, the key to functional codes lies in being able to run scripts and codes. In this section, the focus is going to be on all the process you can use to run python scripts regardless of the operating system platform, requirements, and skill set you have obtained as a programmer.

To begin, let's consider the concepts of scripts and modules first.

- **Scripts and Modules:**

In computer programming, a script can be defined as a file which contains a logical sequence of orders. It can also be seen as a batch processing file. It is typically stored in a plain text file as a simple program. To process a script, an interpreter is needed. The interpreter has to run each command sequentially. Thus, any plain text file which contains python codes is known as a script, a term used informally to refer to a top-level program file. However, not all plain text files containing codes in Python are scripts. A module is a plain text file composed of python codes which are designed for importation to another python file from which it is used.

Bringing both terms into comparison; a module is distinguishable from a script because while the former is crafted to be imported, the latter are meant to be run directly. Whatever the case may be, the critical thing is to learn how to run the codes you write in Python into your scripts and modules.

- **Interpreter:**

To better understand the concept of scripts and modules, let's delve into the concept of the interpreter. Python can be an interpreter language. An interpreter is a vital program necessary to run python scripts and codes. In technical terms, an interpreter is a form of software which runs the code by working between the hardware of your computer and the program. There are different interpreters spanning across the different types of platforms. Thus, your interpreter can be any of the following depending on the python implementation you use:

1. A program coded in C such as CPython — the core implementation of the programming language.
2. **A program coded in Java. For example, Jython.**
3. A program coded using python, such as PyPy.
4. **A program implemented in .NET. For example, IronPython.**

Any code you write would be executed by the interpreter regardless of the form it takes. As such, the primary condition for being able to execute python scripts is to have an interpreter correctly installed in your PC. An interpreter is capable of executing python codes in the following ways;

- As a block of code entered an interactive session; or
- As a module or script.

- **How python codes are run an interactive session:**

Running python codes via the interactive session is one of the popular ways of executing scripts and modules. To begin the python interactive session, the terminal or command-line is opened. Next, depending on the version of python in use, input the word "python" or "python 3" in and click to enter. The default prompt in the interactive mode is the sign (>>>). So, whenever you see these characters, keep in mind that you have entered the interactive interface. Here, you can attempt to write and run your python codes. However, as simple as this method seems, it has one major downside: your code lasts as long as the session. Once you terminate your session, your codes are gone. The upside to this method is that any statement and expression you input is immediately evaluated and executed. That it allows you to test each line of code written makes a great tool for development, and a fine platform to practice coding python easily and quickly. To leave the interactive mode, you could use any other following methods:

- You can use built-in functions such as exit() or quit().
- You can also use a combination of keys. For systems with Unix-styled platforms, you can use Ctrl and D. In Windows, on the other hand, you can use the keys, Ctrl + Z and click to enter.
- Take note that the primary general guideline to keep in mind when coding with python is to use the interactive session when in doubt of the function(s) of any code.

If you have no experience using the terminal or command-line, below are some steps you can use:

1. When using Windows, locate the command-line otherwise known as the MS-DOS console or command prompt. The command-line is a program known as cmd.exe. However,

the path to this program can change with the version of your system.

2. **To gain quick access to it, you can use the codes Win + R key to get to the Run dialogue. Once the interface opens, input cmd in and click to enter.**
3. On platforms that run on GNU or Linux as well as other versions of Unixes, there are numerous applications which provide access to the system command-line. Some of them include Konsole, xterm, Terminal, and Gnome. The tools run terminals or shells such as csh, ksh, Bash, among others. In this scenario, the path to each application is more diverse and is dependent on the way it is distributed, as well as the environment of the PC you use. Hence, it is essential for you to take note of the documentation regarding your system.
4. **On systems running on Mac OS X platform, the system terminal is accessible through the following processes;**
5. Go to Applications, enter Utilities and click on Terminal.

- **How the interpreter runs python scripts:**

The process of running python scripts is riddled with multiple steps undergone by the interpreter. In doing this, the interpreter does the following:

I. Processing the statements of your script in a manner of sequence.

II. Compiling the source code into bytecode — an intermediate format:

The bytecode represents the conversion of the code into a lower-level language which is independent of the platform. The purpose of the bytecode

is to optimize the execution of the codes. As such, in running your code, the interpreter boycotts the compilation process. Take note that only modules undergo code mobilization because they are imported, executable scripts don't.

II. Send off the code to be executed:

Here, the PVM (Python Virtual Machine) which is the runtime engine of python is used. The PVM works as a cycle which iterates over the instructions contained in your bytecode, running them one after the other. However, do not consider the Python Virtual Machine to be an isolated part of python. No. It is merely a part of the python system which is installed in your machine. In the Python interpreter, the PVM is the final step.

The entirety of the processes required to execute python scripts is referred to as the Python Execution Model.

- **How Python Scripts Can be Executed Using the Command-Line:**

The interactive session in Python would allow you to write many different lines of code, but the minute you close the window, everything you have written would be lost. This explains why python programs should be written using plain text files. Conventionally, files created this way would be attached with a .py extension which could also be .pyw on Windows operating systems. Any plain text editor can be used in the creation of python codes. To make this section more practical oriented, you would have to create a sample test script to explain how to run a python script.

To begin, open a text editor and enter the following lines of code.

```
1 #/usr/bin/env python3
2
```

3 print("Hello World!")

Proceed to save the file to your directory under the file name, hello.py. This marks the completion of writing your test script.

- **How to use the python command:**

To run your sample python script or any other python script, you would have to use python command. Begin by opening a command-line and entering in the word python 3 or just python depending on your installed version. Next, attach a path to your script in the following fashion;

$ python 3 hello.py

Hello World!

Click enter to run the script. If your coding is error-free, the execution should work out well, and the words "Hello World!" would be displayed on the screen. So that is how you run a python script. If the script is unable to run, chances are you have made a mistake in your coding or in adding the path, or there might be problems with your installed version of python. Cross-check your text file to ensure it is error-free. If it is, check your path; the way and place the file is saved. If that is also all right, check your python installation. Basically, it is the simplest and most practical way to execute a python script.

- **How to redirect output:**

It is sometimes helpful to save the output of a python script for analysis at a later date. To do that, enter the following line of code:

$ python3 hello.py > output.txt

In doing this, you would redirect the output of the python script to a file named output.txt instead of to stdout — the default system output file. If

before now output.txt file doesn't already exist on your system, the procedure would automatically create it. However, if it already exists, the new output would be used to replace the contents in it. Thus, your line of code should be as such:

$ python3 hello.py >> output.txt

Now, instead of being replaced, the output script would be attached to the end of output.txt.

- **How to run modules with the -m option:**

In Python, some command-line options are made available to meet the many different needs of users. For instance, if you want to execute a module in Python, you can run it under the command python -m <module-name>. The function of the -m option is to search the sys.path for a module name whose content runs as __main__. Take the instance below:

$ python3 -m hello

Hello World!

Take note that the module-name has to be named after a module object rather than a string.

Chapter 5. Ethical Hacking

Ethical hackers, or “white hats” as the cyber – community identifies them, are technically hackers, in that their job is to find vulnerabilities and other exploitable weaknesses in various computer networks and systems. These “white hats” are called such because white is associated with good, and as such, they are working for the good of the network, by trying to find out its weaknesses in order to be able to fix them.

Ethical hackers are employed by companies in order to better improve their security systems, as network security is paramount for any company or business to ensure that they are not cheated, stolen from, or otherwise compromised, as a network open to hacking would allow malicious attackers or hackers to steal data, cause financial loss, or cause other kinds of damages.

Note that in terms of operations and tools used, ethical hackers often actually operate similarly to hackers. After all, hackers go in with the intent of finding vulnerabilities, and a lot of the best tools of the job are also available to those who have less noble intentions. In addition, ethical hackers or “white hats” often also intentionally use the same software and tools as freelance hackers or malicious hackers, i.e “black hats”, as their job is to find the same vulnerabilities before the “black hats” do, or failing that, find ways to patch and fix these network vulnerabilities and weaknesses. In order to do this, it would only be logical to approach the problem in a similar manner as “black hats” do, allowing them to “put the hat on” of their counterparts in order to think like they do.

Note that the mere employment of a hacker by a legitimately registered entity such as a business or corporation does not mean that they are automatically “white hats”. Some businesses employ “black hats” in order

to steal corporate data or other sensitive information from their rivals. The characteristic of a “white hat” is that they only look for vulnerabilities in their own employer’s network security, and they are given the express authorization to do so, and they have the duty and obligation to report any and all vulnerabilities found to their employer as soon as possible.

There is also another type of hacker, often called the “grey hats”, which straddle a middle ground between “black hats” and “white hats”. These “grey hats” function similarly to “white hats” in that they look for vulnerabilities in order to report them, allowing the owner of the network to fix these vulnerabilities, but these “grey hats” do not work with the express authority of the network owner, meaning that while they may have good intentions, what they are doing is still most likely violating the cyber – crime laws of the country that they are in.

Step by step process of ethical hacking

What happens when your internet connection gets hacked? Your connection not only slows down, but your identity and location also gets used for any illegal activity that a criminal hacker may do using your network. At the same time, it also becomes very possible for a criminal hacker to get deeper access in your personal computer, thanks to discovered vulnerable ports and shared network devices such as printers. If your mobile phone is also synced to your computer, there is a risk that a criminal hacker would also get access to that device.

For this reason, it is very important to know how your internet connection can be hacked. In this chapter, you will learn how most criminal hackers opt to crack your Internet connection through the most popular hack tools.

Method 1: Check for Unchanged Router Passwords

This is probably the easiest way to hack Internet connection. All you need to do is to see all the available networks that you can connect to. To do that, switch on your computer's WiFi and look at the list of available networks in your vicinity.

Now, you would see that there are common router names in the list of available networks, such as Linksys. There is a big chance that the default password for these routers are unchanged, so all you need to do is to log in the manufacturer's given password. How do you do that? You just need to go to the manufacturer's website and look up for the router's manual.

If you are able to go into the target network using the default password, pull up a fresh browser and log in into the GUI of the target router. If your target is a Linksys router, the IP address to show its GUI is 192.168.1.1. Once you are prompted for log in credentials, leave the username blank, and type in "admin" for password. (Note: Some routers have different default log in credentials depending on the model. You can check for these on the manufacturer's website.)

Once you are in the GUI, you can change the SSID, the router password, and the security protocol of your target router. This way, you would be able to take full control of the router and prevent the network owner from connecting to his own ISP!

This method assumes that there are just too many Internet users that are not too careful when it comes to securing their Internet connection before putting it to use. You would be surprised that there are people who do not even bother changing the SSID of their Wi-Fi, which is almost a giveaway that it is not secured by a password other than what the manufacturer uses.

Method 2: Hack Internet Password

What would hackers do when the Wi-Fi that they are trying to hack is secured? The next thing that they would do is to check how possible it is to guess what the password of their targeted network is. At this point, you would need to learn a few key terms when it comes to identifying and assigning security to Wi-Fi connections:

1. WEP – means Wired Equivalent Privacy. This is the most basic form of Internet encryption, thus an unsafe option for most Internet users when it comes to assigning security to their wireless connection. This type of encryption can be cracked with ease using the most basic hacking tools. Older models of Wi-Fi still use this type of encryption.
2. WPA – means Wi-Fi Protected Access. This is a more secure option for newer computer and router models, which can only be efficiently cracked through the old-fashioned trial-and-error method of guessing potential letter or word combinations (also known as dictionary attacks). If a strong password combination is used, a WPA connection may almost be impossible to crack. Another variation of this security protocol is the WPA-2, which is tougher to penetrate.

At this point, you have the idea that most hackers would opt to hack available networks that are protected through WEP protocol, since it is faster and much easier to crack. Here is a list of tools that a hacker needs in order to crack a WEP-protected Internet connection:

1. A wireless adapter – you would need to have a wireless adapter that is compatible with a software called CommView. This software allows your wireless card to enter monitor mode. To see if your wireless card is compatible with CommView,

you can head over at tamos.com and see if your adapter is on the list.

2. CommView – CommView for Wifi is a software that is used to capture packets from your target network. All you need to do is install this software and then follow the installation guide to install its drivers for your wireless card.
3. Aircrack-ng GUI – this software enables you to crack the password of your target network after you are done capturing packets.

Follow the steps below to start cracking a WEP-encrypted network:

1. Run CommView for Wifi to start scanning for wireless networks according to channel. Leave it running for a few minutes. You would then see a long list of networks that your wireless adapter can reach.
2. Choose a WEP network (you would see this right next to the name of networks on the list.) Select a network that has the lowest decibel (dB) rating and has the highest signal.
3. Once you have chosen your target, right-click it to open a context menu. Click on Copy MAC Address.
4. Head over to the Rules tab on the menu bar and select MAC Addresses. Tick on the MAC Address rules.
5. For the Action option, choose CAPTURE. Afterwards, head over to the Add Record option and choose BOTH.
6. Once you are done formatting the rules, paste the mac addresses that you copied on your clipboard to the box that you

would find below it.

7. When capturing packets, remember that you would only need to capture the ones that you would be using for cracking. To make sure that you only capture the packets that you need, select option D (which you would find on the bar right above the window) and deselect Management Packets and Control Packets.
8. Make sure that you save the packets that you have captured so that you can crack them for later. Go to the Logging tab on the menu bar and enable Auto Saving. Afterwards, set the Average Log File Size to 20 and the Maximum Directory Size to 2000.
9. Now, wait until you capture enough data packets. Make sure that you wait until you have at least 100,000 data packets so you can get a decent signal for cracking.
10. After collecting enough data packets, head over to the Log tab and select all the logs that have been saved during capture. Head over to the folder where your saved logs are stored. Click on File, and then Export, and select Wireshark tcpdump format to save it as a .cap file. Choose any destination that you would easily access later on. Do not close CommView.
11. Now, you are ready to crack. Run the Aircrack-ng GUI and choose the WEP option. You would be prompted to open the .cap file that you have exported a while ago. Once you retrieve that file, select Launch.

12. Once your Aircrack-ng GUI is running and decrypting the data packets that you had on your log, open the command prompt. Type in the index number of the network that you have selected a while ago.

13. Wait until the wireless key appears.

If everything goes well, you would easily get the wireless key of your targeted network. If you missed some packets, you would be prompted by Aircrack-ng that you need to capture more of them. If that happens, you just need to wait for CommView to get the additional packets that you need.

Can Tougher Security Measures be Breached?

At this point, you would realize that it is fairly easy for most hackers to gain access to the type of Internet security that you are using. At the same time, you should also have the idea that once criminal hackers know what type of encryption you are using, the easier it is for them to identify the tools that they should use for hacking your network.

Is it possible for hackers to breach more advanced protocols such as WPA and WPA2? Yes, they could accomplish such a feat, but it would take them more time – making the process inefficient, especially given that their goal for hacking network connections is to enjoy better bandwidth and have immediate internet access, or even to mask their location. For this reason, it would be best to enable WPA (or other better encryption options) should your devices allow it.

Now that you have a general idea on how hackers can steal your Wi-Fi, it is time to take some preventive measures. The next chapter will tell you more about that.

Chapter 6. Cybersecurity essentials

Cyberterrorism can be conducted in order to reach some kind of personal objective through the use of computer networks and the internet with some experienced cyberterrorists being able to cause mass damage towards government systems, hospital records as well as national military and security programs that leave a country in a state of turmoil, terrified of further attacks. The objective for many cyberterrorists is often related to political or ideological agendas.

Cyberterrorism can be challenging to prevent or protect systems from as it can be largely anonymous with unknown motivations and uncertainty over whether there could be repeated attacks again in the future. There is some argument over the exact definitions of cyber terrorism or whether it should be referred to as terrorism at all since the actions are not closely linked with conventional methods of terrorism and instead are towards information warfare, however since many of the motives are political in nature and targeted towards the disruption of infrastructure, the term loosely fits into the category of terrorism.

Cyberterrorism can be committed by individuals, groups and organizations and in some cases by nation states attacking rival governments. Cyberterrorism is currently a major concern for both government and media sources due to the potential damages with government agencies such as the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency establish targeted strike forces to reduce the damage caused by cyber terrorism.

Cyberterrorism can be accomplished through a variety of techniques such as a network penetration and viruses that are created in order to disrupt and immobilize the system. Cyberterrorism is more dangerous than simple

cybercrime for personal gain. Cyberterrorism can have serious consequences on the country and institutions that are attacked, placing lives at risk. As our technology improves, there are a number of ways to combat cyberterrorism by first anticipating and preparing for attacks and to implement a plan for prevention, following this we prepare for incident management to mitigate an attack limit the damage caused in the case that an attack has reached the target. Once an attack has occurred, the next stage of defence is to implement consequence management which is assessing the damage and taking note of how we are able to improve defences in the future, starting the process over once again.

Traits of Cyber Terrorism

After understanding the definition of cyber terrorism, many cyber terrorists have found to have very similar traits in common which can place them in the category of cyber terrorists. One such trait is that the victims of cyber terrorist attacks are specifically targeted rather than random in the case of hackers without clear objectives other than financial gain or entertainment. While there can be randomised cases of hackers releasing viruses or worms into the general public, there are often clear objectives for doing so with the victims being a specific group or nation that has been targeted for predetermined reasons by the hacker. Other objectives involve attacking an organization, industry, sector or economy for the purpose of inflicting damage or destroying their target.

Finally, another common trait within cyber terrorism is to further the terrorist group's own goals which could be financial, political, religious or ideological. These terrorists seek to achieve this goal by inflicting heavy damages on their target and make their own objectives obvious by publicising them.

Types of Cyber Terrorism Attack

Cyberterrorism has been placed within three main categories by the Centre for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate school in Monterey, California. These categories are simple-unstructured, advanced-structured and complex-coordinated.

Simple-Unstructured - These are small-scale attacks and are generally performed by inexperienced hackers using widely available tools created by other people. The hackers behind these kinds of attacks generally lack command and control skills as well as possessing a limited learning capability.

Advanced-Structured - These types of attacks are more sophisticated and can target multiple systems or networks and the hackers responsible possess the capability to modify or even create basic hacking tools. While the hackers possess limited command and control skills, they have an increase learning capability and present a significant risk depending on the organization they are targeting.

Complex-Coordinated - At the higher end of the scale, coordinated and complex attacks can have a devastating effect on the system under attack with mass disruptions against integrated and heterogeneous defences. These types of hackers have the ability to create sophisticated hacking tools and have a strong command and control as well as an advanced capacity for further learning and skill development.

Understanding each type of attack allows organizations to develop the proper counter measures to combat and prevent an attack as well as implement damage control in the wake of an attack.

Incursion - The objective of an incursion attack is to gain access or penetrate the networks and systems which contain valuable information for the attacks. This is one of the more common attacks and has a much greater success rates for the terrorists. Due to the high number of loopholes available to hackers, terrorists are able to take advantage of weak security and vulnerabilities to obtain or even modify secure information which can then be recycled for further attacks against the organization or for the personal gain of the attackers.

Destruction - This is a far more severe attack with the objective to infiltrate a computer system and inflict damage and ultimately destroy the network. For the organizations who are victim to these types of attacks, there can be incredible costs involved both in terms of repair and loss of revenue. An attacker intent on destruction can render an organization inoperable with their entire system thrown into disarray, impacting them financially and in some cases destroying their reputation as clients fear the security of their information following a serious attack. In terms of governments, a destruction attack can plunge the systems into chaos. It can take some amount of time for an organization to recover fully from the most severe destruction attack, as is the objective for the hacker.

Disinformation - Equally devastating can be that of disinformation. This involved spreading credibility destroying rumours and information, having a severe impact on the target. The rumours that are launched may or may not be true however they can be equally devastating and can still have long term effects on the organization or nation involved. Once these attacks are carried out, damage control can be quite challenging as information can spread regardless of whether the infiltration is contained. Information can relate to certain scandals and claims of corruption which can tarnish the

reputation of individuals within the organization or the organization itself, leading to disruption of the order that has held the organization together.

Denial of Service - We have mentioned denial of service earlier in this book as it one of the most common and widely known forms of attack. In terms of cyberterrorism, DoS attacks occur with businesses and entities that have an online presence with the attack rendering the website or service useless at the time of the attack. These types of attacks can therefore cause immense issues in both the social and economic function of the business, causing organizations to suffer massive losses.

Defacement of Web Sites - While not as severe or damage, the defacement of a website can still have immense consequences for a business. Defacement of websites can involve websites to be changed completely, including a message from cyber terrorists for either propaganda or publicity purposes for them to achieve some type of cause. In other cases, hackers may cause the website to redirect to one in which they have established earlier which could also contain a message that they have devised to gain publicity and awareness of their propaganda or cause. These types of attacks have decreased in recent years as security measures have been heightened and hackers have a lower probability of access to web pages long enough to implement the changes and most major organizations effectively putting a stop to it.

Intro to VPN's

It is possible to hack a computer or a system using its IP address. The steps are given below.

1. Obtain the IP address of the target system. E.g: 101.23.53.73.

2. Download the advanced port scanner and install it.

3. Open the install the software and enter the IP address of the target in the right column. After entering the IP address, click on scan.

4. Now, it will scan and will provide you with the list of all open ports on the target system or target router. E.g: Port 96.

5. How the application will ask you to enter the login information, type the username and password and press enter. In case if there is no password, just give the username.

With this, you will be able to access the documents and files on the target's system. You can use command prompt for copying, creating or deleting files.

Hiding

Nowadays, most of the users have Wi-Fi Routers. All of the devices like mobile phones, laptops, tablets, televisions, etc, connect to the Wi-Fi router. The Internet service provider will provide the router with a public IP address. Any device connected to the router will be given a private IP address. If you connect to the Internet from your device, your router will

look like your computer. In some cases, the users only use one device and they won't need a router. Then, the computable directly connect to the Internet and the public IP address will be given to that single system. The host from the other end can track your Internet activities, as your assigned IP address is public.

Conceal your IP address with a Virtual Private Network

If you want to hide your IP addresses, you can use the service of a VPN.VPN stands for Virtual Private Network. It is a private network that allows the users to connect to the internet or another network without revealing the actual IP address of the user’s system. The VPN assigns its own IP address to the user’s computer. The IP address assigned by the Internet Service provider will not be provided and remains hidden.

The following are some popular Virtual Private Network providers

- Hide My Ass
- Pure VPN
- Vypr VPN (Free Trial)
- ZenMate VPN
- Express VPN

Protect your identity

If you are using your own IP address for surfing on the Internet, there are chances for the attacker to monitor your sensitive information. There can be a breach in your privacy, security and location if the attackers get hold of your IP address. You can solve this problem by using the IP address of other users. This way, you can protect your identity and yourself from attackers. There are several tools available which will help you to mask your IP address. These masking tools use the IP address is from public companies, which are third-party IP addresses.

Mask your IP address with Proxies

There are many proxy servers on the Internet and you can make use of them to surf anonymously. If you use a proxy server to visit a website, your original IP address will be hidden and a new IP address will be given to you. However, the IP address given to you will be a temporary one. In other words, using a proxy browser lets you access websites indirectly.

Use someone else's network

Instead of using your own Internet, you can actually use free Wi-Fi as an alternative. There are many hotels and coffee shops that provide their customers with free Wi-Fi. If at all you connect to the Internet from a different location, the IP address with which you are connecting will also change. This is because different locations have different IP addresses.

Chapter 7. Introducing Malware and cyber attacks

Malware (malicious software) software or hardware tools that the Hackers use for penetrating of exploiting into the computer or network of others with the motto of retrieving personal or sensitive information from individuals are from an organization. Malware can also be used for disrupting or crippling the operation of a computer or network, given the attacker a chance to retrieve information by accessing it. These are specifically designed with the intention of causing harm to the entities they infect. Malwares usually we have against the requirements of user. Malicious software is of two types, the ones that cause unintentional harm and the ones that are specifically designed for causing harm. We use the term badware for defining them.

Malware are designed to gather information, in stealth. They gather information without the consent or permission of the user and they are designed to work for extended periods of time. Without the proper tools, it is extremely hard to find them. They make themselves with system files. Some of their functionalities include causing harm, information retrieval, sabotaging the system and payment extortion. The inclusion software and hostile software both come under malware. They include software programs like viruses, Trojan horses, spyware, adware and other malicious software. Malware usually disguise themselves as non-malicious programs so that they can continue working in stealth. Basing on the recent studies, viruses and Trojans horses are the most widely used malware. Viruses are now being replaced with worms and of their numbers are declining recently.

Types of Malware

Adware : Adwares to be the most lucrative and least harmful of the lot. They're designed with the sole purpose of displaying advertisements on your computer.

Spyware : Spywares are designed to keep an eye on the user and to constantly spy on their activities. At all times, they keep track on the user activities. Basing on the user's Internet activities, they display advertising accordingly. After gathering the required information, they team up with Adwares and what when the user goes online.

Virus : A virus, in computer science, can be defined as a contagious program or code. They select software and attached to them. This way, they can multiply by reproducing themselves. It is hard to detect a virus unless you have the proper tools. They can easily spread from programs, folders and files that are infected, using a network or through direct file sharing. For instance, if you plug-in an USB device to the infected computer, the virus will attach itself to the file transferred to the USB device and infects it. Any device connected to that USB will get infected. Viruses can also attach themselves to email attachments like text files, music files or videos. Once the second party downloads them, they will start infecting them too.

Worm : Worms are small and simple programs specifically designed for sabotaging the system files of an operating system, thus crippling the overall functionality of the system. They are similar to viruses in a lot of ways and they can also replicate themselves. They disguise as system files and hide in folders. They use up the system resources like hard disk space and processor, affecting the performance of the system by slowing down the processes and emptying the hard disk space.

Trojan : The main motive behind designing Trojan horses is to steal sensitive user information, including personal and financial information. Trojan horses, out of all malicious software, are considered to cause the most harm. They're the most dangerous of the lot. Trojan horses are used as the major tool by attackers for performing denial of service attacks. They constantly track the user activities in the background and notifies the person who placed it, by creating and maintaining a complete log of user activities. Trojan horses can be hard to detect and they can stay hidden for very long periods of time. Some types of Trojan horses claim to delete viruses from the user's computer, but in reality, they will be adding viruses of their own. The name Trojan horses came from the Greek mythology, where the Greeks used a wooden horse for deceiving the Trojans. They made a wooden horse and hid inside it. They left the wooden horse on the shores of Troy, as a sacrifice to the gods. The Trojans took the horse inside their tall walls, and it is when the Greeks attacked the city of Troy from within. If you think of it, did the Trojan horse is a good fit.

Rootkit : We know that every system has a firewall protecting it, which blocks most of the malicious software. Attackers designed the rootkit for compromising the firewall protection of a system. Rootkits do not directly infect the system, but they work as backdoors that allow other malicious software into the system. They hide themselves from the user and in the background they open gateways, so that other malware can enter. From the user's point of view, it would seem like nothing is wrong.

Keyloggers : Keyloggers are designed with a specific purpose of recording the keystrokes of user. Whether online or offline, they continue to record and store the user inputs from the keyboard and when the user goes online, they will send it to the person who placed them. The initial versions of keyloggers could only store the keystrokes given from keyboard. The latest

versions can even take the keystrokes from virtual keyboards. The Hackers use the information sent by keyloggers for retrieving user information like credit card details, email ids and passwords. Keyloggers cannot differentiate passwords from regular text and for this reason; they store everything and sends it to the hacker. The hacker will then try to retrieve password is from the obtained information.

Ransomware : Ransomware can be considered as infections present inside a system. They lock the computer from within, often displaying messages like “you have been locked from your system; follow the instructions given to unlock it”. Those instructions usually demand money from the victim. The attacker will only unlock the computer of the victim after getting the money. In most of the cases, the computer will be rendered useless if left locked.

We will discuss about the above malware briefly in our next chapters.

Vulnerability to malware

Whenever we use the term system, it implies that it can be anything from a single application, single computer, a large group of computers connected over a network, an operating system or the network itself. So when we say that the system is attacked, it means that any of the above mentioned entities are attacked. Malware take advantage of these vulnerabilities for making their way into a system. Some of those vulnerabilities are mentioned below:

Security issues in software: The security defect in software is a major vulnerability that the malware take advantage of. Both big and small software are included in this and this means all software, right from simple programs to complex operating systems are in it. Software distributing

companies constantly update their software after fixing the security vulnerabilities found. They do this by releasing patches.

Some of the commonly found software vulnerabilities are present in the browser plug-ins. Using outdated plug-ins is not advised. You cannot say that your software is saying just by updating it, even after updating it might still have a few security vulnerabilities. Keeping the older versions of plug-ins even after updating with newer versions is not safe.

User error or insecure design : Another method that is commonly used for spreading malware is by taking the users to install download an infected file. Such attempts May include hardware like flash drives or USB devices, infected with malware. When this hardware is attached to the computer, the infected files automatically execute themselves, infecting the system of the user. If this infected system is on a network of systems, the malware might possibly spread across the network and infect other systems connected to it. This is very effective for spreading malwares.

Outdated Antivirus : Outdated or free antiviruses cannot provide the same level of security that the purchased versions provide. An updated antivirus will have the list of all the latest viruses in its database. The older version of antivirus may protect you too an extent but not completely. If your computer encounters a latest virus, it might view that virus as non-malicious software.

Over Privileged code and over privileged users : In the area of computer science, religion can be defined as the access given for modifying the system. Privileges are given to users and programs. Some programs and users are given more privilege than the privileges they should have. This happens with poorly designed software. This is the vulnerability and a

malware can take advantage of it. There are two types of problems possible by giving more privileges. They are:

Over Privileged users : Some systems provide their users with what privileges than they should be having. These users can modify or change the code of a program. Such users are called over privileged users.

Over Privileged code : Some systems provide more privilege to be called executed by the user. Search code is called over privileged code and they have permissions to access the system resources. There are a few operating systems and scripting languages giving more than required privileges to the code, making it vulnerability. When this kind of code is executed, the system will give all the permissions to code, thinking that the user ran it.

Homogeneity

We can call a set of systems as homogeneous systems if they're running on the same OS and connected to the same network. When homogeneity is present, are given malware can spread itself easily to all the systems in that network. For instance, if there is a Trojan horse on a single system, it can easily spread itself across the network and infect other systems on that network. Homogeneity can be found on systems present in organizations like software organizations, schools and colleges. Most of the systems either run on the Windows operating system or the Mac operating system. By concentrating on any of these operating systems, a hacker can easily exploit the systems running on them. A solution for this is to use different operating systems on the computers. By doing this, a hacker will have a hard time spreading his malware. Following this has its own disadvantages. In the initial stages, maintenance and training expenses are included in the disadvantages.

Cover your tracks

If you plan on becoming a good ethical hacker, you should not leave the traces of intrusion behind. By leaving evidence, you're only risking your chances of getting caught. You can actually use malware for clearing your records of intrusion. Event logs can be cleared in using malware, providing a clean exit. There are many different types of malware available, using which you can hide your network traffic and clean the directories.

Proxy Server : Taking the help of a proxy server when tunneling through a network’s sensitive areas is a really good idea. Intrusion detection software cannot detect your presence if you are using a proxy server. This is because proxy servers leave no trace behind.

For most of the cases, Trojans are usually the best and the reason for this is their ability to monitor in stealth for extended periods of time.

Crimeware

Crimeware can be defined as the software or hardware tools that hackers use for hacking. Crimeware can be defined as something that is:

- Not enabling the crime involuntarily.
- Mostly used for online criminal activities.
- Not a desirable software or hardware, in general.

Out of all the Crimeware, bots are the most widely used ones. Bots are described below in brief.

Bots

What exactly is a Bot?

The term ‘bot’ is the short form for the word robot. These robots are different from the ones shown in movies. They aren't the robots that companies manufacture from production line. Bots are most sophisticated of the Crimeware that people are facing today. They are similar to worms and Trojan horses in many ways. Bots are unique when compared to other malicious software and their uniqueness is because of the wide range of automated tasks that they are capable of performing. They perform these automated tasks on the half of the attacker. Attackers place bots from someplace safe on the Internet. Bots are capable of performing the denial of service attack by sending spam messages. When the computer is infected by a bot, it completely falls under the control of the person who placed the bot. These infected machines are called zombies.

Bots can infect a computer in many ways. On the Internet, they usually search for unprotected computers for attacking. After finding a computer with vulnerability, they quickly sneak into it and reports back to the person who placed it. They usually stay hidden, doing nothing, until they are commanded to do something by their master. Just like Trojan horses, these work in stealth. Most of the people do not realize that they have fallen victims to bots until they get notified by their service provider about the spam messages from their computers to other users. They sometimes even clean the whole computer on which they are staying, for making sure that they don't get replaced by other bots and get bumped off the computer. They work along with Trojan horses, which help them to spread to other computers on the Internet. Trojan horses spread them by sending emails from the infected system.

Bots are always designed to work together with other zombie machines, and they can't work alone. Then designed to work in groups and this group are called botnets. By using any of the mentioned techniques, attackers create botnets. They do it by repeatedly infecting computers with bots. This will start a chain reaction where the bots from infected computers continue to other computers with vulnerabilities. The attacker will control the zombie machines from the command and control center, which is nothing but his master computer. They use the command and control center for instructing other zombie machines with instructions to perform the tasks on their behalf. In general, a botnet usually comprises of many infected machines. All these zombie machines will be connected through the Internet and they spread across the globe. Even in the smallest botnets, there will be a hundred to a few thousand bots, while the larger botnets have more than 100,000 zombie computers. All of the zombie computers will be under the command of the attacker.

Chapter 8. Quickly scanning the servers and the network

Hacking tools are software programs that are designed with one specific purpose, to allow hackers to gain unauthorized admission to a network or system. There are many hacking software packages that you can make use of to make the job simpler and then move on to tougher techniques. But if you are really desperate and wish to crack a password, it is best that you consider using hacking software.

The different types of hacking tools are as follows:

- Vulnerability scanners
- Port scanners
- Web application scanners
- Password cracking tools
- Packet sniffers

Vulnerability Scanner

Vulnerability is defined as an unintended software flaw that can be used as an opening by hackers to send in malicious software like Trojan horses, viruses, worms, etc.

A vulnerability scanner is a very efficient tool used for checking weak spots in a network or a computer system. It is basically a computer program. The sole purpose of the scanner is to access networks, applications, and computer systems for weaknesses. Both black hat hackers use this and computer security managers, who are usually white hat hackers or blue hat hackers, use this. The black hat hackers use it to find weaknesses and gain

unauthorized access from those points. White hat hackers also check for weaknesses, but they do it to protect the computer systems rather than to gain entry.

The data is transmitted through ports. The vulnerability scanner is used to check the ports that are open or have available access to a computer system. This is used for quickly checking the network for computers with known weaknesses. By limiting the ports, the firewall defends the computer, although it is still vulnerable.

Benefits of Vulnerability Scanners

- Early detection of problems
- Security vulnerabilities can be identified easily
- As it shows the vulnerabilities, they can be handled

Types of Vulnerability Scanners

Port Scanner

A port scanner is a computer application that is designed solely for searching open ports on a host or a server. The person who intends to use this should have basic knowledge of TCP/IP. The attackers use it to identify services running on a server or a host with the intention of compromising it. The administrators, on the other hand, use it to verify their network's security policies. A port scan is a process that sends requests to a selected range of ports with the goal of finding an active port. This can only find vulnerability and cannot be used for attacking or protecting. Most of the uses of this scan are to probe rather than attack. One can use the port scanner to scan multiple hosts in order to find a specific listening port. This process is called port sweep. These are particularly used for a specific type of service. One of them is a computer worm, which is SQL based. It may be used to port sweep ports that are listening on TCP.

Types of port scanning:

TCP scanning

These simple port scanners use the operating systems' network functions when a SYN scan is not possible. This is called for when we scan by the Nmap (discussed in later chapters). The computer's operating system will complete a three-way TCP handshake and then the connection will be closed immediately to avoid a DoS attack. An error code will be returned otherwise. The advantage of this mode of scanning is that the user doesn't need any special privileges. However, this type of scanning is not very common, as the network function of an operating system prevents low-level

control. In addition, this kind of scanning is considered to be 'noisy' when using port scans. Therefore, this type of scan is not the preferred method, as the intrusion detection systems can log the IP address of the sender.

SYN scanning

This is also a type of TCP scan. Here, the port scanner will generate raw IP packets by itself and will monitor for responses instead of using the network functions of the operating system. SYN scanning is also called "half-open scanning." This is so called because a complete TCP connection will never be opened. The SYN packets will be generated by the port scanner. The scanner will send a SYN-ACK packet when an open port is found. The host will close the connection before completing the handshake by responding with an RST packet.

There are several advantages when we use raw networking. They are

1. **The scanner gets complete control of the packets sent.**
2. The connection will not be received by the individual services.
3. Scanner gets complete control of the response time. This type of scanning is recommended over TCP scanning.

UDP scanning

UDP scanning is a connectionless protocol. Though this type of scanning is possible, there are technical challenges. A UDP back up will be sent to the closed port and the post will respond with an ICMP response saying that the port is unreachable. The scanner looks for the ICMP responses. If there is no response from the host, the port is open. However, if the host is protected by a firewall, the scanner will receive a response saying that there is an open port, which is false. The ICMP rate limiting will also affect this method. All the ports appear to be open if the message is blocked. For this we can send some application-specific UDP packets as an alternative and hope that the application layer response is generated.

Window scanning

This method is outdated and is rarely used. But window scanning is fairly trustworthy and can determine if a port is closed or open, filtered or unfiltered. This method can be used if there is a firewall on the host's system.

Network vulnerability scanner

This type of scanner identifies the vulnerabilities in the security of a computer system that is connected to a network in order to tell if that particular system can be exploited or threatened. It is software that has a database of known flaws. It'll scan the computer system for these known

flaws by testing the system in order to make these flaws occur. Then it will generate a report of all these findings on that individual computer system, or a given enterprise.

Web application scanner

There are many ways in which architectural flaws and safety fallbacks can be checked. One such method is a web application security scanner, which acts as a communicator between the user and the application and identifies these issues. There are many tests that a scanner can perform to find these vulnerabilities in web applications.

The most frequently used test is the black box test. This means that the user will have no idea what the logic behind the result is but will have clear-cut information about results that will give the complete information required. Mostly these scanners analyze by throwing random test cases that might occur in real-life scenarios and give results. These web applications are mostly entertained by users because they act as an easy platform to communicate with the system and therefore the user interface of these web applications play a major role in the success of an application.

There are multiple actions the user can perform using these applications; among them are creating an account, querying the database by giving search criteria, adding a lot of required content, and also making different types of transactions. When there is a lot of information being stored, the

user tends to store some of their personal information in these applications as well.

It seems like an easy, convenient option but the fact that the security of the data is being compromised is one that most users tend to miss. And this is the very fact that the insider leaks and hackers cash in on. So it is not just the convenience that the user has to see, but they also need to make sure they keep a check on the extent of information they are sharing on these web applications.

There are many various strengths of web application scanners; here are a few of them:

- They come in handy for last-minute hurried checks for flaws.
- They can check a lot of possible results that may be obtained when the same scenario is given different inputs and then they can recognize the anomalies.

The tools that are used for web application testing, such as scanners, are independent of the programming language used. So, irrespective of the language that the web application is coded in, the tool can work in its own way, dynamically changing the inputs for different languages. This gives the users complete freedom to test all their applications.

Where there are strengths, weaknesses exist too. Here are a few of the weaknesses:

- One of the major weaknesses of these tools is that the hackers use the same tools. So if the users are able to find flaws in the system, the hackers can find them easily, too. This poses a major threat to the community.

- Many updates are being made to the languages that are used in designing web applications and most of the users use tools that are available for free. These free tools are normally built to a basic level, so new modifications and updates will not be available. Therefore, the random inputs that are being thrown at the system to find the anomalies will not have the updated inputs. This means there are a lot of potential threats that can be caused because of these missing inputs.

- There is a high chance that the first few tools will have zero results; this causes high anxiety in the users, which will ultimately result in them using the new tools. This will cause the creation of new tools and the extinction of old tools.

- The excessive use of the tools can also be a problem, as it will help the attackers to check their test cases theoretically. It makes it easy for them to send botnets.

These cause spam in the web applications that might lead to information leakage.

- The malware used by the attackers can be updated using these botnets. This type of updated malware can be very difficult to remove.

- As already mentioned, the software that is being used in web application designs is constantly being updated and the tools that are being used are dynamically programmed depending on the language that is being used by the web application. No one can give a 100% guarantee that the results obtained belong to the whole source code. To get the complete coverage of the web application there are testers, called penetration testers, who carefully and closely analyze the results to verify that the entire source code of the web application has been covered.

- The users must be aware that these tools will not be able to detect logical flaws in the source code, such as leakage of information and low level of encryption of the data.

- These tools also have a difficult time detecting any technical flaws. It doesn't mean that they are incapable of doing so, but the web application has to provide the right clues to enable these tools to identify the technical flaws.

Chapter 9. Web security

As more devices that use web applications are released onto the market, such as mobile phones, tablets, and computers, hacking web applications has become more prevalent as there are more and more web applications available, each with its own bugs, exploits, and vulnerabilities. Hacking web applications becomes easier every day as hackers discover new exploits in web applications. Below are some forms of web application attacks.

Fundamentals of Web security

Session Hijacking is a type of cyber attack where the attacker exploits a web server's session tokens. The hacker does this by exploiting a control mechanism, which controls the session tokens.

Web servers must communicate with several different TCP connections. The server needs to keep track of the connections, so it issues a session token after the computer or device is authenticated. This token can be used in cookies, the header of an http request, or in the body of the header requisition.

A session hijacking attacks the session token by predicting a token or by stealing one. Once the hacker compromises the session token it can exploit the following:

One kind of attack predicts the ID values and allows the hacker to get into a system without authentication.

A session sniffing attack happens when a user sends a request with a session ID to the web server, and the hacker intercepts the session ID and

uses it to create their own requests on the web server, effectively hiding the attacker as a user.

A client-side attack is a type of attack that exploits the vulnerabilities in software clients such as web browsers, pdf reader/writers, instant messengers, and other software with vulnerabilities. IBM's Knowledge Center (***www.ibm.com/support/knowledgecenter/en***) lists two types of client-side attacks. They are content spoofing and Cross-site scripting (XSS). Content spoofing is when a user thinks that the content on the site is valid and legitimate and not originating from external sources. XXS is when an attacker executes scripts in a browser.

A Man-in-the-middle attack (MITM) occurs when a hacker intercepts an http transaction. The attacker takes the TCP connection and splits it in two, allowing the attacker to read, function as a proxy, or modify the data in the message. A popular tool for MITM attacks is Ettercap.

- Man-in-the-browser attacks are similar to MITM attacks, except they use a trojan horse to attack banking information like transactions and balances.

SQL Injection

SQL injection is when an attacker adds SQL queries into an input form on an application. The SQL statements are executed and allow the attacker to read sensitive data from a database, have admin access allowing it to shut down, modify the database, recover content in a file in the database, and issue commands to the OS. SQL injection is often used on financial data such as changing balances or voiding transactions. It also allows the attacker to spoof identity, disclose all of the data in the database, destroy data, or gain administer privileges of the database.

Cross-Site Scripting (XXS)

There are three types of XXS attacks: Stored or non-persistent XXS, Reflected or persistent XXS; and DOM-based XXS.

- Stored XXS attacks happen when a user's input is saved on a web server. This attack often occurs in a database, on forums, or in comments sections of a website.
- Reflected XXS occurs when a message is returned from the web server with an error message or a search result that is sent to the client.
- DOM-based XXS occurs when the data is in DOM, and the data does not leave the browser. DOM stands for Document Object Model and is an HTML and XML interface for documents.

Wireless Networking

Wireless networks are a set of multiple devices that communicate over radio waves within a certain range. Wireless networks let multiple devices connect to the internet via a modem and a wireless router. The router controls the settings of the wireless network including IP addresses, MAC addresses, the wireless network's authentication, and other settings. Wireless routers use IEEE 802.11, which is a set of MAC addresses and physical layer settings. Attacks on wireless networks are generally sniffing attacks that attempt to obtain the SSID and gain access to the wireless network.

Wireless DoS attacks

Wireless networks are susceptible to two types of attacks. The first is physical attacks, and it occurs when there is radio interference from cordless phones. The second type of attack is a network DoS attack. A network DoS attack is easy to accomplish. Like other DoS attacks, it operates by sending multiple requests, in this instance to an Access Point. Because the requests are taking up resources and clogging the queue, legitimate devices cannot connect to the network with their requests.

Mobile Platforms

The majority of attacks on mobile platforms come in the form of malware for the different mobile platforms. The major mobile platforms are Android and iOS. Android is a mobile platform, and since Android devices have a large market share, there is a large number of devices to attack. Not all malware is installed via an app store, however, some malware attacks via a QR (Quick Response) code. Hacking mobile devices provide a wealth of information about the user. Hackers can access contacts, GPS data, the microphone, the camera, emails, MMS messages, and SMS messages.

Android

Android was developed by Google and is available as an open-source mobile platform. The majority of the malware written for mobile devices is for Android because it there are more avenues to attack it. The Android OS allows users to add software from third-party application stores as well as the official Google Play store. Malicious apps can come from either source, as Google does not put their apps through as strict a vetting process. The software on Android phones is susceptible to reverse-engineering, which increases the danger inherent in the platform. Also, a large number of

Android phones do not come encrypted, making malware attacks easier to perform. Adware is popular malware for Android devices.

AndroidVulnerabilities.org lists several exploits that fall into the categories of kernel, network, signature, and system vulnerabilities.

Apple

Apple developed three mobile platforms iOS, tvOS, and watchOS. They are operating systems for iPhones, iPads, Apple TVs, and Apple Watches. There are fewer malware attacks on the Apple products due to the higher level of security and because the App Store is monitored heavily and it is hard to get malicious apps onto the App Store for any length of time. The Apple Mobile OSs does not allow for silent SMS which makes it is more difficult to spread malicious software.

Web Servers

A web server is the computer, hardware, and software that stores information on a web service, and makes that information available either over LAN or the internet. Web servers hold large amounts of sensitive data such as social security numbers, credit card numbers, email addresses, and passwords. An example of a famous attack on a web server is the Equifax hack in 2017. The hack exposed the personal data of millions of people including information about the victims' credit. Hacking a web server is a complex attack.

Web servers have several vulnerabilities. These vulnerabilities include using default settings, the web server is misconfigured, exploiting bugs, or there is simply a lack of security. The types of web servers are:

- Apache: Apache web servers are the most commonly used. Apache typically is run on Linux.
- Internet Information Services (IIS): IIS is a web server for Windows. It is the second most used, after Apache.
- Other: There are other web servers on the market including Novell's web server and Mac OS X server.

Types of Attacks

There are several types of attacks a hacker can use to crack a web server. These types of attacks include directory traversable attacks, DoS and DDoS attacks, domain name system hacking, sniffing, phishing, pharming, and defacement. Domain name system hacking is when an attacker changes the Domain Name System (DNS) settings so that the internet traffic for the web server is instead sent to the hacker's web server. A pharming attack is when the attacker changes the DNS settings on the user's computer. There are defacement attacks, which is when the attacker replaces a website's webpage with another one that including the hacker's name and whatever media the hacker chooses to post. Defacement is often done to build a hacker's reputation.

Tools to keep your system secure

When you are just beginning, it is much easier if you have some help and these are some of the best software and hardware elements you can use to get started on your journey:

Metasploit

This is more of a hacking infrastructure that a complete set of exploit tools. With Metasploit, you can build your own hacking tools, suited to your purpose. It’s free to use and is, without a doubt, the most popular of all the cybersecurity tools that let you find vulnerabilities on different platforms. Metasploit has the backing of over 200,000 contributors and users to help you find all the weaknesses your system could have.

Metasploit allows you to simulate a real-world attack on your own system and then tells you where your weak points are. It is a great tool for penetration testing, pinpointing the vulnerabilities using Nexpose closed-loop integration, providing Top Remediation reports for you.

Supported Platforms:

Metasploit works on all the major platforms, including Mac OS X, Windows, and Linux

Acunetix WVS

Acunetix is a WVS tool or a Web Vulnerability Scanner. It is used to scan a website and find any potentially fatal flaws. It is a multi-threaded tool that crawls websites looking for SQL injection, Cross-site scripting, and many other vulnerabilities. It is a fast tool, easy to use and can easily be used to find more than 1200 different vulnerabilities on WordPress sites.

Acunetix comes complete with a Login Sequence Recorder that lets you access areas of websites that are protected by passwords. The tool has AcuSensor technology that helps to cut down on false positives, making Acunetix one of the best tools of its type.

Acunetix only works on Windows XP or above, no other platform

Nmap

Nmap is short for Network Mapper and it is a port scanner. It is free and it is open source and is one of the most popular of all port scanning tools. Nmap allows for highly efficient security auditing and network discovery. It is used for many different services and uses raw IP packets to find out what hosts are on a network, what services they offer, the details of those services, the operating systems used by the hosts and what firewall they use, amongst other things.

Supported platforms include all the major ones such as Mac OS X, Linux, and Windows

Wireshark

Wireshark is one of the best-known packet crafting tools of all time and is used for finding vulnerabilities in networks and probing the rule-sets of firewalls. It is used by many thousands of professionals in the security world for analyzing networks, capturing deep pockets and carrying out deep scans on many protocols. Wireshark lets you read live data from the following protocols:

- 802.11
- ATM
- Bluetooth
- Ethernet
- FDDI
- Frame Relay
- IEEE
- PPP/HDLC

- Token Ring
- USB
- And many others

Originally known as Ethereal, Wireshark is open source and free to use.

Supported platforms include Linux, Mac OS X, and Windows

oclHashcat

If you are interested in password cracking then Hashcat is the free tool you need. It is CPU-based and oclHashcat is a more advanced version of the tool that makes use of your GPU power. It is known as one of the fastest password cracking tools in the world and is the first tool in the world to have the GPGPU-based engine.

One other major feature of oclHashcat is the fact that it is open source and under an MIT license; this means that integrating or packaging it is easy with the most common of the Linux distributions.

Supported platforms include all different versions of Windows, Mac OS X, and Windows

Nessus Vulnerability Scanner

Nessus is one of the best free vulnerability scanners and it works with a client-server framework. It was developed by Tenable Network Security and is the most popular tool of its kind. Nessus works differently for different users, including tools called Nessus Professional, Nessus Cloud, Nessus Manager and Nessus Home.

Nessus can be used to scan several types of vulnerabilities, including misconfiguration alerts, remote access flaw detection, preparing for PCI DSS audits, detecting malware, Denial of Service attacks against TCP/IP Stack, searching for sensitive data and many others. Nessus is also able to externally call on Hydra, another highly popular tool.

Apart from all this, Nessus can also be used for scanning multiple hybrid, IPv4, and IPv6 networks. Scheduled scans can be set to run when you want them and you can use a feature called Selective Host Re-Scanning to rescan all or some of the hosts previously scanned. The most popular Linux distributions, such as Kali, Ubuntu, Debian, etc., Windows and Mac OS X

Maltego

Maltego is another free and open source platform that allows for deep mining and gathering of information, providing a picture of the threats on your system. Maltego is one of the best tools for showing how severe and complex the failure points are in your system and in the environment around you. It is used for analyzing real world links between companies, people, domains, websites, DNS names, documents, IP addresses and much more. Maltego is based on Java and has a user-friendly GUI with loads of options for customization.

Supported platforms include Linux, Mac OS X, and Windows

Social-Engineer Toolkit

If you’ve watched Mr. Robot, you will recognize this tool, developed by TrustedSec. It is a highly advanced tool for the simulation of several social-engineering attack types, such as phishing attacks, credential harvesting and much more. The tool will automate each attack and generates malicious

websites, spoof emails, and other things. It is based on Python and is the industry standard tool or penetration testing for social engineering attacks.

Netsparker

Netsparker is one of the most popular scanners for web applications, looking for flaws such as local file induction, and SQL injection. It will come up with remedial actions that you can take in a safe and read-only manner. You will not need to verify the vulnerability yourself because Netsparker will provide you with the proof of the exploitation. If it is unable to automatically verify a flaw, you will get an alert message.

Netsparker is very easy to use; all you do is input the URL of the web application you want scanning and it will get on with it for you. Netsparker has support for AJAX and Java-based applications so there is no need for any complex configurations for scanning. You can get a free demo version of pay for the full package.

Netsparker is only supported on Windows systems

w3af .

w3af is open source and free and is another scanner for web applications. It is used by penetration testers and hackers and the name stands for Web Application Attack and Audit Framework. W3af allows you to get information on security vulnerabilities that may be used in penetration testing. It claims to be able to identify in excess of 200 different vulnerabilities, including SQL injection, cross-site scripting, PH misconfigurations, unhandled app errors and easy-to-guess credentials. It also claims that it can make any web application more secure. W3af is

available in GUI and command-line interfaces and is user-friendly. W3af comes in GUI and command line interfaces and is very user-friendly.

Supported platforms include Mac OS X, BSD, Linux and older versions of the tool are supported on Windows.

Other Top Hacking and Security Tools

Web Vulnerability Scanners

- AppScan
- Burp Suite
- Firebug
- Grendel-Scan
- Nikto
- OWASP Zed
- Paros Proxy

Vulnerability Exploitation Tools

- BeEF
- Core Impact
- Netsparker
- Sqlmap
- WebGoat

Forensic Tools

- Autopsy
- EnCase
- Helix3 Pro

Port Scanners

- Angry IP Scanner
- NetScanTools
- Unicornscan

Traffic Monitoring Tools

- Argus
- Nagios
- Ngrep
- NtopSplunk

Debuggers

- GDB
- IDA Pro
- Immunity Debugger
- WinDbg

Rootkit Detectors

- DumpSec
- HijackThis
- Tripwire

Encryption Tools

- KeePass
- OpenSSH/PuTTY/SSH
- OpenSSL
- Tor

Password Crackers

- Aircrack
- Hydra
- John the Ripper

Best practices to prevent yourself from getting hacked

Hackers are not the nicest of people, at least some of them aren't. It doesn't matter whether they work alone, as part of some shady syndicate or for someone with a political agenda, they have the power and the knowledge to gain access to your system and your information. A hacker could easily find tons of information on the internet about that company and they would then

use what information they learned to find the weaknesses and exploit them. This puts any data that you have entrusted to that company in very real danger.

Think of the computer system and internet network you use at home as a company. Is it protected? What can you do to make sure hackers can’t get into it? Instead of just sitting there and waiting for an attack to happen before you take any action, do it now; fight back against the hacker!

Here are 10 ways that you can protect your system against a hacker:

Update, Update, Update

Keep your operating system and all your applications and software updated as often as possible. Every time an update is released, apply it. This stops hackers from being able to get into your computer through holes and weaknesses in programs that haven't been updated. If you use Microsoft Windows, ensure that automatic updating is turned on or, at the very least, set to inform you when the latest updates are available. Make sure those updates are applied immediately they become available. That way, every Microsoft application you use will be updated as well, including Office. If you use software like Flash or Java, find safe alternatives because these are incredibly susceptible to attack.

Use Up to Date Security Programs

I’m talking about things like antivirus software, anti-malware tools, anti-spyware tools and, of course, your firewall if you use one other than what was provided by your operating system. If you wanted to trick even the very worst of hackers, invest in anti-exploit technology, like Malwarebytes Anti-Exploit – this will stop any attack before it can happen

Destroy Personal Information

This is more so if you are selling or throwing away your computer or hardware device. Make sure your hard drive is completely erased because, if a person is looking to find information on an old device, this will make it so much harder to do. If your information is very critical and you are discarding the device, consider using a chainsaw to destroy the hard drive. It might seem drastic but that is the best way to stop your information from being found.

Never Use Open Wi-Fi

Using open Wi-Fi makes it easier for hackers to steal your network connection and download data from your computer. Use an encrypted password to protect your Wi-Fi connection and think about buying a new router every couple of years. Some routers do develop vulnerabilities that may never be patched up and newer ones provide the ability for you to give guest users segregated access, without having to hand over your password. Also, change your password on a frequent basis.

Password Protect All Your Devices

This includes your desktop computer, laptop, smartphone, tablet, smartwatch, everything that can take a password. Because mobile devices are so highly used these days, they are more vulnerable than ever before. Make sure your phone is locked and the screen timeout is as short as possible. If available on your device, use fingerprint locking or any other form of biometric security that may be available. Don’t forget; for many people, a phone or a tablet is a tiny computer that contains an awful lot of data, a real haul of personal information for any hacker and, should anyone be able to access it, it can use you a lot of heartaches. The same goes for your laptop or desktop; never leave it open and unattended. If you have to leave it, make sure it is, at least, locked and on the password screen.

Make Sure Your Passwords are Difficult to Guess

All of your passwords should be difficult ones to crack and should be changed regularly. If you really do find it hard to remember so many passwords, consider using a password manager – that way you only have to remember the one password. If available, apply two-step verification where possible. Most devices, applications and other software provide this option now. For those who don't know what it is, it is an extra layer of protection that makes accessing data more difficult.

Make Your Security Question Answers Creative

Most people choose their Mother's maiden name or the name of a pet for their security questions but these are so easy to guess these days and, in many cases, the answers can be found using a simple search on Google. Consider answering a question in a daft way. For example, if one of your security questions is, "What color was your first car?" Answer it with something totally unrelated, like "lasagna." You get the picture. Just don't forget what your answer was if you ever need to supply it!

Be Smart When Emailing and Surfing

Phishing is still a big thing but they are much cleverer now than they used to be. When you get an email, hover your mouse over any links – this will show you the email address the email was sent from. If you aren't sure about an email, look hard at how the sentences have been constructed and formatted. If something still seems off, search on the internet for the subject line of the email. If it is a known scam, there will very likely be plenty of information about it.

Never Link Account

If you are on a website that requires you to join before you can do anything, never take the option of signing up using your social networking account. Many websites give you the option of signing in using Facebook, Google+ or Twitter but this is a dangerous path to tread. It may seem convenient but it opens up a whole heap of personal information and you can’t always be sure you are using a genuine site to log into in the first place.

Don’t Save Sensitive Data to Your Cloud Account

It really doesn’t matter how you look at it; any data that is stored in the cloud doesn’t belong to the person who stored it there and many cloud storage solutions offer encryption for stored “at rest” data, only for data in transit. Only use the cloud for things that aren’t too important.

Important Note

No doubt you have received at least one popup message telling you that your computer is insecure and has lots of critical errors on it; hopefully, you haven't clicked on any of these. No operating system worth its salt will ever do this to let you know about errors. These are from scammers and clicking on them opens your computer up to attack

Chapter 10. Basics of Firewall

Today, a network design is incomplete without firewalls. This is a networking device that can either be a software- or hardware-based. A firewall can control access to a network. The objective of the controlled access is to ensure resource and data protection from external intruders. To control the access, firewalls will be installed at the exit/entry points of a network. For instance, a firewall may be placed between the Internet and an internal network. When put in place, it can control the flow of traffic to the network at the point.

Although they are used for protecting internal networks from public ones, they can also control access between segments within a specific network. For instance, a firewall may be placed between the Sales Department and Accounts Department. As I mentioned earlier, firewalls can come as a software or a hardware device. Some organizations implement this device through their network's operating systems such as Windows servers, Linux/Unix, and Mac OS servers.

In this case, the firewall will be configured on the network's server in order to grant permission to some network traffic types. When used at home or in small offices, it can be installed on the home or office's local system where it will be configured for controlling traffic. You can also find some third-party firewalls. Today, you can find hardware firewalls deployed in different networks. These firewalls are usually dedicated network devices and needs only little configuration for implementation. All the systems behind the firewall will be automatically protected from outside sources.

You can get these firewalls whenever you need them because they are readily available and can be combined with some other devices. For instance, many wireless access points and broadband routers have built-in

firewall functionality. In such situation, the WAP or router may have some ports where systems can be plugged into.

CSUs/DSUs

Known as Channel Service Unit/Data Service Unit, this device plays the role of a translator between the WAN data format and the LAN data format. The translation is absolutely necessary because WAN and LAN use different technologies.
Some people are of the opinion that a CSU/DSU is a digital modem. However, unlike a modem that can easily change its signal from digital to analog, this device changes signal from a digital format to another digital format.

A CSU/DSU is designed with a physical connection that can be used for LAN equipment. This can be via a different connection for a WAN or a serial interface. The CSU/DSU is not the regular networking equipment because it is always kept separate from others. However, as more WAN links are used, router manufacturers have seen the need to include the CSU/DSU functionality in their routers. When they are not included, the manufacturers give the WAN expansion capability to accommodate the CSU/DSU.

If you are a computer specialist working in an organization, you might come across cases in which more than one computer system’s OS is under one network. In situations like these, you must install software that provides a security firewall. The Windows operating system has an inbuilt firewall that you can activate and use directly. This firewall feature comes in different versions of Windows, including Windows XP, Windows Professional, Windows 10 and the other versions.

Installing a firewall or creating a strong set of passwords and having detailed access control settings is not enough to stay protected. In addition to all of the standards and vulnerabilities mentioned above, you must understand that the largest and most tedious obstacles to securing your wireless network are the complexities found within the network. However, no wireless network can be completely secured. There are some things that are not complex but may still be considered an obstacle. For instance, a plain old AP and a wireless NIC (interface card) might not actually be complex, although you can deduce that a lot more is going on at the backend.

The 802.11 protocols aren't developed to be perfect because they have big issues. These protocols don't simply help you send and receive information with optimal management overhead, like the old Ethernet. Rather, the 802.11 protocols are deeply complex. Most of the wireless networks simply transmit and receive RF (radio frequency) signals which carry a packet of network data. The 802.11 network will actually perform more complex functions, such as:

· Encrypting data to improve data privacy.

· Authenticating clients to be sure only authorized personnel have access to their network.

· Setting timing message packets to be certain about client synchronization and to help avoid data-transmission conflicts.

· Checking the data integrity to make sure that all information remains uncontaminated.

As complex as the 802.11 protocols are, their network design is associated with more complexities such as:

· Staying updated with your wireless devices, which may include laptops, APs and PDAs (Personal Digital Assistants).

· The kind of antennae to implement and where to locate them.

· Knowing the exact type of devices that are allowed on your network and also those that are not.

· Adjusting signal-power settings which will prevent your radio frequency signal from leaking outside your residence.

All of these wireless network complexities add up to a multitude of security weaknesses that are not available in the old traditional wired networks.

Chapter 11. Cryptography for beginners

Currently, cryptosystems are divided into two kinds: (1) Symmetric Key Encryption and (2) Asymmetric Key Encryption. This way of classifying cryptosystems is based on the method of encryption/decryption used for the entire system.

The major difference between the symmetric and asymmetric encryptions is the connection between the encryption and decryption keys. Generally speaking, all cryptosystems involve keys that are closely related. It is impossible to create a decryption key that is totally unrelated to the code's encryption key. Let's discuss each kind of cryptosystems in more detail:

Symmetric Key Encryption

Cryptosystems that belong to this kind have a single key. This key is used to encrypt and decrypt the information being sent. The study of symmetric encryption and systems is known as "symmetric cryptography." Some people refer to symmetric cryptosystems as "secret key" systems. The most popular methods of symmetric key encryption are: IDEA, BLOWFISH, DES (Digital Encryption Standard), and 3DES (Triple-DES).

During the 1960s, 100% of the cryptosystems utilized symmetric encryption. This method of encrypting and decrypting information is so reliable and efficient that it is still being used even today. Businesses that specialize on Communications and Information Technology consider symmetric encryption as the best option available. Since this kind of encryption has distinct advantages over the asymmetric one, it will still be used in the future.

Here are the main characteristics of symmetrically encrypted cryptosystems:

- Before transmitting the message, the sender and the receiver must determine the key that will be used.
- The key must be changed regularly to avoid any intrusion into the cryptosystem.
- A stable form of data transmission must be established to facilitate easy sharing of the key between the involved parties. Since the keys must be changed on a regular basis, this mechanism may prove to be expensive and complicated.
- In an organization composed of “x” individuals, to facilitate two-way communication between any two members, the required number of keys for the entire system is derived using the formula: “x * (x-1)/2.”
- The keys used are often small (i.e. measured through the number of bits involved), so the encryption and decryption processes are faster and simpler compared to those used for asymmetric systems.
- These cryptosystems do not require high processing capabilities from computer systems. Since the keys used are small and simple, ordinary computers can be used to establish and manage the cryptosystem.

Here are the two problems usually encountered when using this kind of cryptosystem:

- Key Determination – Before any message can be transmitted, the sender and the receiver must determine a specific symmetric key. That means a secure and consistent way of creating keys must be established.

- Trust Issues – Because all the people involved use the same key, symmetric key cryptography requires the sender to trust the receiver, and vice versa. For instance, if one of them shares the key with an unauthorized party, the security of the entire cryptosystem will be ruined.

Modern day communicators say that these two concerns are extremely challenging. Nowadays, people are required to exchange valuable data with non-trusted and non-familiar parties (e.g. seller and buyer relationships). Because of these problems, cryptographers had to develop a new encryption scheme: the asymmetric key encryption.

Types of Symmetric Encryption Algorithms

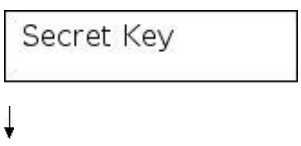
There are many types of symmetric encryption algorithms, including:

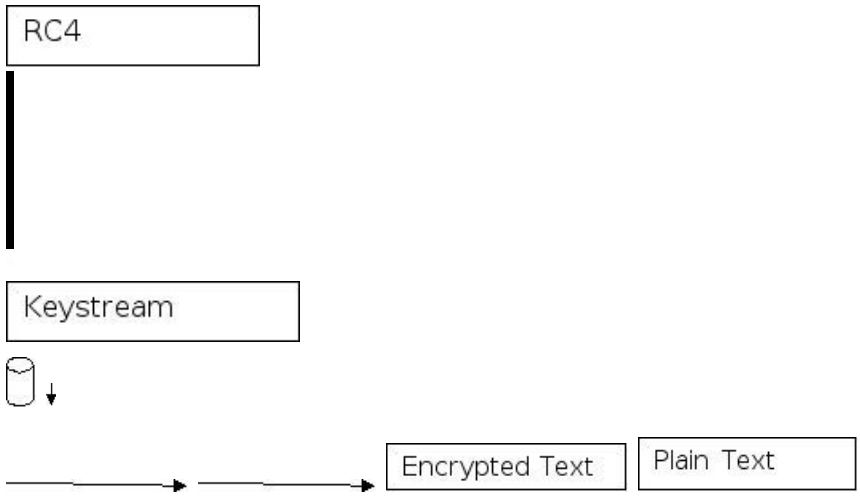
1. Rivest Cipher or RC4

This encryption algorithm was designed by Ron Rivest in 1987. It is a type of stream cipher. It is known for its simplicity and speed. But, experts discovered later one that RC4 has multiple vulnerabilities and it is insecure to some extent.

RC4 normally uses 64 bit and 128 bit key sizes. This algorithm is strong cryptographically and relatively easy to implement. The RC4 or Rivest Cipher has two parts – Pseudo-Random Generation Algorithm and Key Scheduling Algorithm or KSA. The most popular implementation of this algorithm is in SSL and in WEP for 802.11 wireless networks.

Here’s a diagram of how RC4 works:





The secret key is the password that's used to encrypt and decrypt the message. The RC4 block in the diagram is nothing but the encryption engine. So what happens is that the user inputs a plain text file with the secret key. Then, the encryption engine generates a key stream and converts the plain text bit by bit into an encrypted text.

RC4 initiates an array of 256 bytes and runs the KSA or key scheduling algorithm on them. The output of the KSA is then plugged into the Pseudo-Random Generation Algorithm which will generate the keystream. Then, the keystream will perform the XOR operation on the data and turn it into encrypted text.

2. RC2

RC2 is also known as ARC2. This was also designed by Ron Rivest. RC stands for Rivest Cipher. The development of this algorithm was supported by Lotus. It is a 64 bit block cipher that has a variable size key. It uses 18 rounds. The 18 rounds are performed using this interleaved sequence:

- Five mixing rounds
- One mashing round

- Six mixing rounds
- One mashing round
- Five mixing rounds

RC2 uses the key expansion algorithm.

3. RC6

RC6 was also designed by Ron Rivest. The algorithm is patented by RSA Security. It has a block size of 128 bits and it supports key sizes 192, 128, and 256 bits. Leaked reports show that the NSA systems that are used to intercept internet communications produce RC6 UDP or User Diagram Protocol traffic.

4. Serpent

Serpent is a symmetric key algorithm that was designed Lars Knusen, Eli Biham, and Ross Anderson. It has a block size of 128 bits and supports a key size 256, 192, and 128. Serpent has a conservative approach to security as it has a large security margin.

The Serpent cipher is not patented and it is in a public domain. Anyone is free to incorporate this algorithm in their hardware or software implementation.

A number of studies show that the XSL attack can weaken Serpent.

5. Twofish

Twofish is a symmetric block cipher published in 1998 by Counterplane Labs. It has a 128-bit block size. The key size ranges from 128 to 256 bits. It is also optimized for 32-bit CPUs. Two-fish is license-free and unpatented so anyone can use it. Twofish was designed to meet the design criteria of NIST (National Institute of Standards and Technology). It has no weak

keys. It is also efficient both on the Intel Pentium and other hardware and software platform. It has a flexible design so it accepts additional key lengths. The design of this algorithm is simple and easy to implement.

6. DES

DES stands for Data Encryption Standard. This was once the most commonly used symmetric-key algorithm for encrypting electronic data. This was developed at IBM in the 1970s. This was used by the NSA in the 70s so many suspected that there is a backdoor to this cipher. Before the rounds, the block is classified into two 32-bit halves. The halves are processed alternately. This process is known as the Feistel scheme.

DES is now considered as unsecured primarily because of its 56-bit key size which is too small.

Asymmetric Key Encryption

These cryptosystems use different keys for encrypting and decrypting the message. Although the keys involved are dissimilar, they still have a logical and/or mathematical relationship. It is impossible to extract the message using a decryption key that is totally unrelated to the encryption key.

According to cryptographers, this mode of encryption was developed during the 20th century. It was developed in order to overcome the challenges related to symmetric key cryptosystems. The main characteristics of this encryption scheme are:

- Each member of the cryptosystem should have two different keys – a public key and a private key. When one of these keys is used for encryption, the other one must be used for decryption.

- The private key is considered as confidential information. Each member must protect the private key at all times. The public key, on the other hand, can be shared with anyone. Thus, public keys can be placed in a public repository. As such, some people refer to this scheme as “public key encryption.”
- Although the private and public keys are mathematically related, it is practically impossible to determine a key using its “partner.”
- When Member1 wants to send information to Member2, he needs to do three things:
    - Obtain Member2’s public key from the public repository.
    - **Encrypt the message.**
    - **Transmit the message to Member2. Member2 will acquire the original message using his private key.**
- This mode of encryption involves larger and longer keys. That means its encryption and decryption processes are slower compared to those of symmetric encryption.
- The asymmetric key encryption requires high processing power from the computers used in the cryptosystem.

Symmetric key encryption is easy to comprehend. The asymmetric one, however, is quite difficult to understand.

You may be wondering as to how the encryption and decryption keys become related and yet prevent intruders from acquiring a key using its

“partner.” The answer to this question lies in mathematical principles. Today, cryptographers can create encryption keys based on these principles. Actually, the concept of asymmetric key cryptography is new: system intruders are not yet familiar with how this encryption works.

Here is the main problem associated with asymmetric key cryptosystems:

- Each member needs to trust the cryptosystem. He/she has to believe that the public key used for the transmission is the correct one. That person must convince himself that the keys in the public repository are safe from system intruders.

To secure the cryptosystem, companies often use a PKI (Public Key Infrastructure) that involves a reputable third party organization. This “outside organization” manages and proves the authenticity of the keys used in the system. The third party company has to protect the public keys and provide the correct ones to authorized cryptosystem members.

Because of the pros and cons of both encryption methods, business organizations combine them to create safer and practical security systems. Most of these businesses are in the communications and information technology industries.

Chapter 12. Using VPN

Most users nowadays have routers, which connect the devices like mobiles, tablets and computers to the Internet. The router will be given a public IP address by your Internet service provider and each of the devices that connect to the Internet will be given a private IP address. The router gives the private IP address. Whenever you connect your computer to the Internet, it will look like your computer is your router. In cases where the users have only a single computer, they can connect it directly to the Internet and their ISP will give a public IP address to it. Since the assigned IP address is public, a host from the other end can track your Internet activities.

Conceal Your IP Address with a Virtual Private Network

VPN (virtual private network) allows the users to connect to another network. The VPN will provide your computer with its own IP address. VPN can be used for hiding your original IP address and your IP address provided by your ISP will be hidden. VPNs are not just used for hiding IP addresses. You can access any network from your organization, which may be blocked from certain networks. There are many commercial and free VPN and proxy services available on the Internet. Using these you can connect to the Internet with a new IP address and your original IP address will be hidden.

Here are some of the virtual private network providers.

- Hide My Ass
- ZenMate VPN
- Express VPN

- Pure VPN
- Vypr VPN (Free Trial)

Why Would You Hide Your IP address?

There are many reasons for hiding an IP address. Here are some of these reasons why people wish to hide their IP addresses:

Hide your identity from your competitors - Commenting on your competitors' products on forums will reveal your identity. In such cases, you can hide your identity by hiding your original IP address.

Hide your geographical location - Not all the content the Internet is available to all. Some websites prevent users from some countries from visiting their websites. Using a proxy server in such cases will solve the problem and you can access those sites.

Prevent website tracking - Every web page or website that you visit will track your data. The web server saves all this data. You can keep the Web servers from tracking you by using a proxy server to hide your IP address.

Protect your identity - People can monitor your sensitive and private information if you use your own IP address for navigating the Internet. Your location, your security, your privacy can be breached if the attackers know your IP address. You can use someone else's IP address instead of your own to protect yourself and your identity from others. There are several tools that can mask your IP address. They use the third-party IP addresses provided by public companies.

Mask Your IP Address with a Proxy

You can surf the web anonymously using the proxy servers available on the Internet. There are a few thousand of these proxy servers that will hide your

IP address. When you are browsing using a proxy server, it means that you are accessing a website indirectly.

Use Someone Else's Network

You can make use of the free Wi-Fi services as an alternative. Free Wi-Fi can be found in public locations like coffee shops and hotels. The IP address will change with the location and you cannot have the same IP address when you connect to the Internet from a different place.

Alternatively, you may use free Wi-Fi services offered by a coffee shop, hotel, or any public location.

When you look at an IP address, do you ever stop and wonder where it is located, in the physical sense? You might be wondering if that proxy server you have been using is inside or outside of your local jurisdiction; or perhaps you have been exchanging email correspondence with someone and want to make sure that they are where they claim to be. On the other hand, you could just be an investigator who is trying to track a suspect who hacked into a system or sent threatening emails.

It is easy to find out the physical location of an IP address, without having to resort to getting a search warrant.

There is a company by the name of MaxMind. They are responsible for maintaining a complete database of every single IP address in existence, no matter where it is in the world, together with the GPS co-ordinates of the location, the area code, the zip or postal code and the country. This is not your usual relational database, mind you; it is actually a flat file. To update the database, MaxMind requests a site license fee of $370 and then $90 per month or $1360 per year. Their software is built so that queries to the database are easy and can be made on either Mac or Windows systems.

MaxMind also allow people to sign up for a developer's version of the database, but do not give you the software or the tools needed to read it. As such, it is free but is not as accurate as the full-on commercial version. To find the location of any IP address using this free version, you need to have a tool or program that can read the data.

Two developers, T Williams and Jennifer Ennis, have come up with a Python script called "pygeoip." It has been released under a GPL license that lets you put an IP address in and returns the information on its physical location.

Chapter 13. Legal and ethical precautions to take care

Implement strategic plans to counter cyber terrorist efforts will ensure that your organization has the means to combat any threats it may face. There are a number of strategies which a business can employee or in order to stay ahead and heighten their security capabilities in the face of a threat. These are:

Prosecuting Perpetrators

Many attacks can behind the wall of anonymity with many smaller organizations failing to pursue and prosecute the hackers responsible. While this can be a costly activity, there are some advantages in identifying and taking the attackers to court. This can be a shock to the cyber terrorist community and set the standard for which other organizations should conduct themselves in the wake of an attack. If the case is particularly high profile, the organization can benefit from the hard-line response with the prosecuted hackers being an example to the rest of the criminal organizations that are determined to wreak havoc on your business. This example set can send waves throughout the rest of the community and can lead to improvements in the investigation and prosecution process of criminal cyber terrorists. Therefore, is always in the best interest of the parties that have been affected by an attack to seek justice.

Develop New Security Practices

As an organization faces an attack, they will follow through in revaluating their security and any potential loopholes that could be exploited. This involves further testing such as the pen-testing we explored earlier as a means of finding weaknesses and vulnerabilities and employing new

security means to combat these. These activities require cooperation and coordinated efforts amongst all departments within an organization to ensure maximum effectiveness. Corporations should review international standard guidelines for security information to detail the steps that should be taken in order to secure organizations in terms of information security. As organizations further develop their security capabilities, they are able to adapt and modify the standard guidelines to comply with their own operations and needs to achieve the best results.

Take a Proactive Approach

It is important for both corporations and the general public to take a proactive approach as the threat from cyber terrorism becomes more sophisticated and targeted. This involves keeping up to date with the latest information within the cyber security sphere such as threats, vulnerabilities and noteworthy incidents as they will allow security professionals to gain a deeper insight into how these components could affect their organizations. From there they are able to develop and implement stronger security measures thereby reducing the opportunities for hackers to exploit for cyber-attacks.

Organizations should constantly be on the forefront of cyber security having a multi-level security infrastructure in order to protect valuable data and user’s private information. All activities that are critical in nature should have security audits frequently to ensure all policies and procedures relating to security are adhered to. Security should be treated as an ongoing and continuous process rather than an aftermath of the consequences of an attack.

Deploy Vital Security Applications

There are many tools available for security professionals to protect their networks and they can provide a significant benefit to the job at hand. These applications involve firewalls, IDS, as well as anti-virus software that can ensure better protections against potential hackers. Using these security systems, security personnel are able to record, monitor and report any suspicious activities that can indicate the system is at risk. The applications are able to streamline the process, making the job far more efficient and effective. Utilizing these types of tools ensures that security personnel are assisted with the latest in prevention technology and have a greater probability of combating attackers.

Establish Business Disaster Recovery Plans

In the event that an attack does occur, all businesses should have a worst-case scenario contingency plan in place to ensure that processes and operations are brought back to normally as soon as possible. Without such plans, the consequences can be disastrous leading to a loss in revenue and reputation on behalf of the business. Once these plans have been devised, they should be rehearsed regularly in order to test their effectiveness and also provide staff with training in the event of an attack.

These plans should be comprised of two main components, these being, repair and restoration. From the perspective of repair, the attacking force should be neutralised as soon as possible with the objective to return operations to normalcy and have all functions up and running. The restoration element is geared towards having pre-specified arrangements with hardware, software as well as a network comprised of service vendors, emergency services and public utilities on hand to assist in the restoration process.

Cooperation with Other Firms

Your organization would not be alone in dealing with the aftermath of a cyber-attack. Many organizations exist in order to deal with cyber terrorism threats both public and private. These groups can go a long way in helping with issues relating to cyber terrorism such as improving the security within your organization, helping devise and implement disaster recovery plans and further discuss how you can deal with threats in the future and what this means for the wider community. Having this extended network available to you will enhance your efforts in resisting cyber-attacks as well as having a role in discussing other emerging threats and protecting organizations facing these same threats.

Increasing Security Awareness

Security threats are prevalent and this requires an increase in awareness with all issues relating to cyber security. Having your organization become an authority in raising awareness within the community will help educate other organizations in how they can defend themselves against attacks and strengthen their own security which in turn will damage the cyberterrorist community as they face a stronger resistance. You can also raise awareness within your own organization through security training programs which will help all employees equip themselves with the right skillset to combat threats that could arise through their own negligence and will also help them be more alert in times when threats could be present.

Conclusion

With this, we have now come to the end of this book. In the world of computer networking, security is given very high importance so as to protect data and safeguard the system from intruders. In spite of strict security guidelines and authentication schemes, hackers have managed to break into several systems skillfully, piquing the interest of common folk.

Some hackers were able to develop groundbreaking utilities and websites like Facebook and Netflix (the founders of these websites are self-proclaimed hackers), so it is not surprising to see so many young people wanting to learn hacking. Before venturing into the depths of hacking, one needs to have clear-cut ideas about the basics of hacking. That is exactly what this book is intended for.

I have explained all the concepts of hacking in a lucid and comprehensive manner; however, putting them all into practice may seem tough initially. But do not get discouraged. Hacking is all about practice, besides good problem solving skills. Make use of websites like “Hack this site,” which allow hackers to test their hacking skills legally. Also, do not think twice before seeking the help of a professional security specialist if you feel all of this is too technical for you.

And please note that the world of computers is always changing and advancing. The more advanced the system, the more you need to improve your knowledge.

It is also important to remember that misusing your hacking skills to perform illegal activities is punishable by law. Most countries have very strict laws against cybercrimes committed by black hat hackers. So, it is important to limit one's hacking skills to ethical hacking and use those skills

to test the security of one’s own devices, or to aid an organization in testing the robustness of its security system.