HACKING WITH KALI LINUX

THE COMPLETE GUIDE TO KALI LINUX AND THE ART OF EXPLOITATION, BASIC SECURITY, WIRELESS NETWORK SECURITY, ETHICAL HACKING AND PENETRATION TESTING FOR BEGINNERS

JOHN MEDICINE

Hacking with Kali Linux:

The Complete Guide to Kali Linux and the Art of Exploitation, Basic Security, Wireless Network Security, Ethical Hacking and Penetration Testing for Beginners

JOHN MEDICINE

Download the Audio Book Version of This Book for FREE

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

Audible Trial Benefits

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

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

Click the links below to get started!

For Audible US

For Audible UK

For Audible FR
For Audible DE

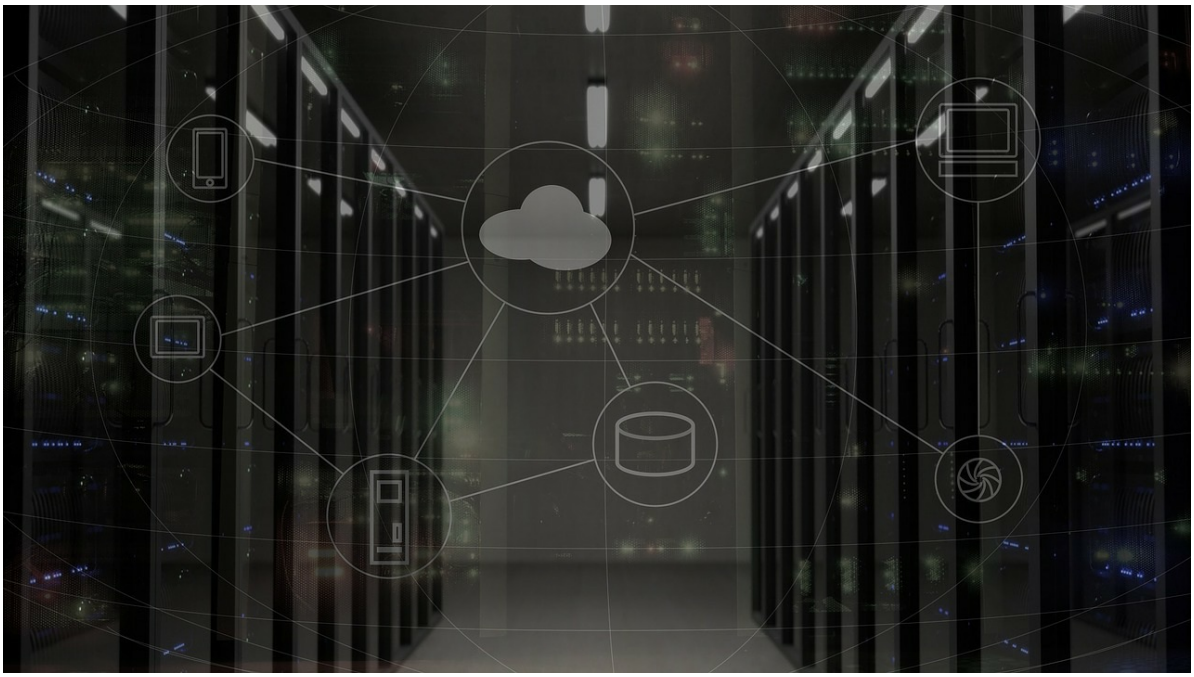
Table of Contents

Introduction

I would like to congratulate your first for downloading your eBook copy of the *Hacking with Kali Linux*. I am delighted to see that you have all shown interest to take a deeper glance into the very usefulness of Kali Linux along with its modern day effectiveness. Kali Linux can be regarded as a boon for all those who are into computing and networking.
Kali Linux functions as a security auditing software which also helps in hacking and networking. It comes with several useful tools which are intended for various security and information related tasks like security research, reverse engineering, penetration testing along with computer forensics. All the services provided are certified and comes along with deep controls that can provide you with the ultimate power for broader accreditations.

Kali Linux is a part of the Linux distribution. It helps in all possible fields of cybersecurity. It is a great tool for the companies for understanding their vulnerabilities. It is built upon open-source, which means it is absolutely free and is 100% legal to be used in a wider range of the enterprise scenarios.

There are various other eBooks available in the market on Kali Linux. Thank you for choosing this eBook. Every effort has been made for making this book as much interesting as possible. Enjoy!



Chapter 1: Analyzing and Managing Networks

Innovations in the digital world have reached unpredictable levels of productivity along with efficiency which is also easily available to all the organizations and businesses. With the rise of new capabilities in the world of technology, have also come brand new challenges. The prime challenge is vulnerability of the organizational networks to cyber threats. A simple failure in the system or IT breach can easily devastate a whole organization or business within seconds. It is directed to specially those organizations that lack a proactive system to deal with the various potential threats and problems.

For effectively resolving all the performances of IT and its relevant issues, you just need to have a detailed understanding of the existing network of IT infrastructure of your organization. With no detailed idea, you will not be able to tackle the potential threats and issues of your IT network. For this, you need to analyze your infrastructure first for gaining proper idea about its working and functionality.

Most of the IT administrators of today just ask their staffs to opt for the powerful automated technology for network assessment. It is more or less

like a temptation of the new technological innovations. Most of the people are of the notion that the available tools for network analysis are very effective, useful and instructive as well. However, if you really want to analyze your network in the proper way, opting for the automated tools might not be the right option.

Overlooking the sirens

The recent temptation of deploying and relying on the tools of automated analysis and monitoring might seem like the siren calls to Ulysses for the network administrators. However, the automated system of network analyzing and monitoring might be a little dangerous for your business. In case you hand over the complete monitoring of your system to the automated tools and rely heavily on them, you might turn out to be a prey to the syndrome called out of mind and sight with the attacks on your network going unobserved. The skills of analysis of the IT might also turn out to be eroded with time as the staffs are directed for other tasks, turning them away from the task of analysis. The network users within an organization might introduce various applications which are of unauthorized nature. Such applications might also disrupt the overall applications of your business and it is of utter importance to remove such items. That is why monitoring of your network needs to be done without the use of any kind of automated tools.

Most of the ultra-modern network and security products in the market have their source of origin within the application’s command line and in the scripts. The IT administrators, in turn, have developed several tools for monitoring, analyzing, collecting and responding to the various security-related issues. The variants of such automated applications are easily available as freeware, open-source or shareware software. However, in spite of such automated tools, it is always better to prepare a customized toolkit for the purpose of analyzing and monitoring.

Assessments and the various methods

You, as the owner of a business or organization, can ask your staffs to

perform certain measures for the ultimate monitoring of your network.

- **Verifying the forwarding configuration policy of firewall:** You can use traffic-generating tools like ping for verifying that the rules of firewall blocks or allows the traffic between the trusted or shared networks and external networks. It needs to function according to the policy of security which you want to enforce in the network.
- **Verifying the configuration policy of egress traffic:** For this, you need to place a testing system just outside your network firewall. On the system of testing which has been placed outside the firewall, try to run applications like Port Listener. You need to use port scanner like nmap and then try to connect to the system of testing at each and every port of listening that you have configured. It needs to be done for confirming that the firewall is allowing access to all those services that you generally want to make accessible to the web and restricts all those services that all the users tried to connect with your trusted networks. The restricted services will only be allowed depending on the AUP or Acceptable User Policy.
- **Find out who is trying to probe into your networks and also from where:** Open up the log of your firewall. Select the source of traffic that is attempting or trying to probe into your network. Use a program of route analysis such as tracert or traceroute for properly identifying the forwarded attack traffic path along with the IP addresses on that path, the service providers which are along the same path and the network from which the traffic of attack has originated. You can use several other utilities like whois, dig and nslookup for performing lookups of reverse DNS along with the whois queries. In the real situations, your website is generally the target of DDOS or distributed denial of service attack.
- **Try to take stock of the network:** An analysis program along with LAN traffic capture program like Ethereal helps in providing the most important information about the networks. By simply observing the application types which are in use, you can

very easily identify the hosts which are providing the various unauthorized services. You can even determine if your employees within the organization are adhering to AUPs, whether any other harmful code and rootkits are trying to establish any type of back connections to the computer of the attacker and if your network is hosting any kind of spam bot.

Strategy for improvisation of the assessment skills

You can nurture the various skills of assessment with your staffs with the help of several exercises. You can start by introducing to your staffs the various techniques of information-gathering which are used by the attackers. Ask your staffs to perform scans of ping and then port the ping scans with the use of nmap. As they advance, introduce other complex techniques like service fingerprinting. Let them assess whether the present measures of security are enough or not.

Chapter 2: Hacking Process

Kali Linux is well known for the purpose of hacking networks. The term “hacking” is not always negative and might also a lot in certain serious events. By having a clear idea about the process of hacking which is carried on every day by the hackers, you can easily track the process and make yourself aware of such events. It can also help you to stay protected when you have a clear understanding of the whole process of hacking.

In general, when a hacker tries to hack the server of a company or organization and gain overall access to all confidential data, it is performed in 5 definite steps. Let’s have a look at them:

- **Reconnaissance:** This is the first step in the process of hacking. In this phase, the hacker tries all possible means for collecting information about his target. The means might include identification of target, finding the range of the target IP address,

DNS records, network and many others. In short, the hacker collects all the contacts of a server or website. The hacker can do this by using various search engines such as maltego, research about the target, for example, a website or by using other tools like HTTPTrack for downloading an entire website for the purpose of later enumeration. By doing all these, a hacker can easily determine the names of the staffs, their designated positions in the organization and their email addresses as well.

- **Scanning:** After the hacker is done with collecting relevant information about the target, he starts with scanning. In this phase, the hackers use various tools such as port scanner, dialers, sweepers, vulnerability scanners and network mappers for scanning the server or website data. In this step, the hackers seek for the information which can probably help them in executing an attack like the user accounts, IP addresses and the names of computers. After the hackers are done with collection of basic information, they move to the next step and start to test the target network for any other attack avenues. The hacker chooses to use various methods for helping them in mapping the network like Kali Linux. The hackers look out for automated system of email or simply based on the gathered information, they try to email the company staffs about various queries, for example, mailing an HR with a detailed enquiry about job vacancy.
- **Gaining of access:** Gaining access is the most important phase when it comes to the process of hacking. In this step, the hacker tries to design the target network blueprint with relevant information which is collected during the first and second phase. After the hackers are done with enumerating and then scanning, they might decide to gain access to the network based on the information.

Suppose, the hacker decides to use Phishing Attack. The hacker might try to play safe and so might use a very simple phishing attack for gaining access. The hacker might decide to penetrate from the department of IT. The hacker might find out that some recent hiring

has been done and they are not to speed the procedures. The hacker sends a phishing email using the actual email address of the CTO by using a specialized program and will send it out to all the techs. The email will have a phishing website that will gather the login ids and passwords. The hacker might use a number of choices such as website mail, phone app or something else for sending an email to the user and asking them to login into a brand-new portal of Google by using their relevant credentials. When the hackers use this process, they already have a special program running which is known as the Social Engineering Toolkit and uses it for sending an email along with the server address directly to the users by masking the same with tinyurl or bitly.

They can also use some other options such as by creating reverse TCP/IP shell in PDF file with the use of Metasploit. They might also use buffer overflows based on stack or hijacking of session for gaining access to the server.

- **Maintaining server access:** Once a hacker gains access to a server, they try to keep the access safe for exploitation and attacks in the future. As a hacker owns an overall system, they can easily use it as their base for launching several other additional attacks. When a hacker gains access and owns the system, such system is known as zombie system. As the hacker gathers multiple email accounts, he can now start to test all the accounts right on the domain. At this point, a hacker tries to create a new account as an administrator and tries to blend in the system. As a precautionary measure, the hacker starts to search and identify all those accounts which have not been used for a very long time. The hacker changes the passwords of such accounts and then elevates all the privileges to the administrator just like a secondary account for maintaining safe access to the target network. The hacker might also start sending out emails to all the other users with a type of exploited file like a PDF with reverse shell for extending their overall access. The hackers wait for any kind of detection in the system and when they get sure that there no one has detected any kind of disturbance in the system, the hacker starts to make copies of all the user data such

as emails, contacts, messages, files and many other for later usage.

- **Track clearance:** Just before the attacks, the hackers try to plan out their whole track of identity so that no one can trace them. They start by changing the MAC address of the attacking machine and run the same through a VPN for covering up their identity.

Once the hackers are done with their job, they start clearing their tracks. This whole step includes clearing of the sent mails, temp files, server logs and many others. He will also lookout for any kinds of alert message by the provider of email that might alarm the organization about any kind of unauthorized logins in the system.

Chapter 3: BASH and Python Scripting for Hackers

BASH Scripting

Any reputed or self-respecting hacker will be able to script. With the introduction of Windows PowerShell, the administrators of Windows are required to script for performing the automated tasks and also for being more efficient.

The hackers might often need to automate the overall usage of various commands and sometimes from various tools. For becoming an elite hacker, you are not only required to grab some scripting skills but you also need the ability for scripting in some of the most widely used languages of scripting like BASH and Python. Let’s have a look at the basics of BASH scripting.

Shell types

The interface between the OS and the user is called shell. Shell enables us to run various programs, commands, manipulate files and many other functions. When it comes to Linux, there are various types of shells. Some of them are Z shell, Kom shell, Bourne again shell or BASH and C shell. BASH shell is the one which is available on all the distributions of UNIX and Linux. So, it is being used exclusively for the purpose of hacking.

Basics of BASH

For creating script of a shell, you need to start with any kind of text editor. You have the freedom of using any kind of text editor available in Linux such as vim, vi, gedit, emacs, kate and many others.

For the first scripting, you can start with a very simple script that will return one message on the screen which says “Hi, null byte”. You need to start by entering #! Which is also known as the shebang. This will tell the OS that anything that follows shebang, will act as the interpreter that you will be using for your script. You need to use the BASH shell interpreter right after shebang by entering the command, /bin/bash right after shebang. So, in this case, it will be like #!/bin/bash. Next, all you need to do is to just enter “echo” which will indicate the system for echoing back to the screen whatever you enter with it. So, you need to enter echo “Hi, null byte!”

Setting the permissions for execution

After you have created a new file, it might not be executable, not even by the owner. When you create a file, you can see the designated permission right beside it, like rw-r- - r- -. This means that the file owner only has the permission to write and read with no permission to execute or x. You can modify the permission of execution with the help of the command chmod.

Running the script

For running the script, you need to type ./Hinullbyte. The command ./ right before the script indicates the system that you want the system to execute the

script right in the present directory.

Use of variables

In case you want to create a more progressive script, all you need to do is to just use some variables. Variables are nothing but area for storage where you can easily hold up something in the memory. When it comes to “something”, it can either be strings, letters or numbers.

Python Scripting

Python comes with some very important features that might turn out to be very useful when it comes to hacking. It comes with various libraries which are pre-built in nature that also provides the hackers with some great functionality. It can be easily said that scripting the languages is much easier in Python when compared to other languages of scripting such as BASH.

Adding the modules of Python

The standard library of Python along with the modules provide the hackers with a wide range of capacity that also includes exception handling, file handling, built-in data types, internet data handling, numeric and math modules, cryptographic services along with interaction with the IPs. Despite all the available pre-existing modules and standard libraries, you might also need some third-party modules in addition to the existing ones. All the third-party modules which are available for scripting in Python are comprehensive in nature and that is the prime reason why a majority of the hackers try to opt for Python when it comes to scripting.

Formatting

Formatting is a very important feature when it comes to scripting in Python. The interpreter in Python uses the style of formatting for determining how the codes are being grouped altogether. The formatting particulars are of less importance than being logical. So, in case you are working with a group of code that you are going to start with indentation which is double in nature, you need to be persistent with double indentation for scripting in Python for

recognizing that the codes exist together. This case of formatting is completely different in the other languages of programming where the requirement of formatting is optional.

Running files on Python

The process of running the files in Python is somewhat similar like BASH. You need to start with #! Followed by /usr/bin/python. This will indicate the system that you want to use the interpreter of Python. Following this, you can enter your required command just like BASH. For running the script, you are required to change the permission first by using the chmod command.

Comments on Python

Python comes with the capability of easily adding comments just like the other languages of scripting. Comments are nothing but simple sentences, words and paragraphs that helps in explaining what a particular code is supposed to perform. Though it is not necessary to use comments but it can help you when you open a file after many years and cannot understand the functions of the codes. The interpreter cannot see the comments.

Variables

Variables are capable of storing data in a location of memory. The Python variables are capable of storing various types of values like real numbers, integers, lists, dictionaries, Booleans and floating numbers. The variable types in Python are treated like class.

Functions

Python comes with a wide array of functions which are built-in. The users can import them and then use the same immediately. Some of the functions are:

- exit(): exits from program
- int(): will return the portion of integer in the argument

Chapter 4: Installation of Hacker ’ s OS Kali Linux

If you are pursuing your career in cybersecurity, it is very important to have an operating system which is security-focused. With a suitable OS, you can easily perform several tedious along with time-consuming tasks in no time at all. There are various OS based on Linux today but Kali Linux is regarded as the best and the most famous of all. It is being widely used for the purpose of penetration testing, assessment of network security along with ethical hacking.

Kali Linux in detail

Kali Linux is the leading distribution of Linux which is being widely used for ethical hacking, network assessment and penetration testing. Kali Linux comes with various built-in command line tools for hacking which is also geared for several tasks of information security.

Why use Kali Linux?

Kali Linux is the most preferable Linux distribution for the following logics:

- It comes with approx 600 tools for penetration testing.
- Kali Linux comes with multilingual support.
- This OS is completely customizable. In case you are not satisfied with the current features and settings, you can customize it according to your need.
- It supports various wireless devices.
- It is developed in an environment which is highly secure.
- It comes with custom kernel which is patched for the injections.
- It is absolutely free and functions as a software which is open source in nature.

If you want to use Kali Linux for ethical hacking and cybersecurity, you need to learn how to install the OS first. Let's have a look at steps for installing Kali Linux.

How can you install the OS Kali Linux?

The installation of Kali Linux is a very simple process. You will also get various options for installation. The most preferable options for installation are:

- Installing Kali Linux via hard disk
- Installing Kali Linux by creating a USB drive which is bootable in nature
- By using software virtualization like VirtualBox or VMware
- Dual system of booting Kali Linux with the OS

Installing Kali Linux with the help of virtualization software like VMware is the most preferable option for installation.

Requirements for installation of the OS

You need to fulfill the following requirements for installing the OS.

- Free space of minimum 20 GB in the hard disk of your machine
- USB/ DVD drive support
- A minimum of 4 GB RAM capacity while using VirtualBox or VMware

Getting started with the process of installation

- **Start by installing VMware**

For the purpose of running Kali Linux in your machine, you need some kind of virtualization software at the first place. Install VMware and then launch the application.

- **Downloading the OS Kali Linux and checking for integrity of image**

For download the OS, you can directly visit the official website of Kali Linux and select the version that you need. On the page of download, you will come across various hexadecimal style numbers. Those numbers are for security tasks and you are required to check the image integrity right before downloading the OS.

- **Launching an advanced virtual machine**

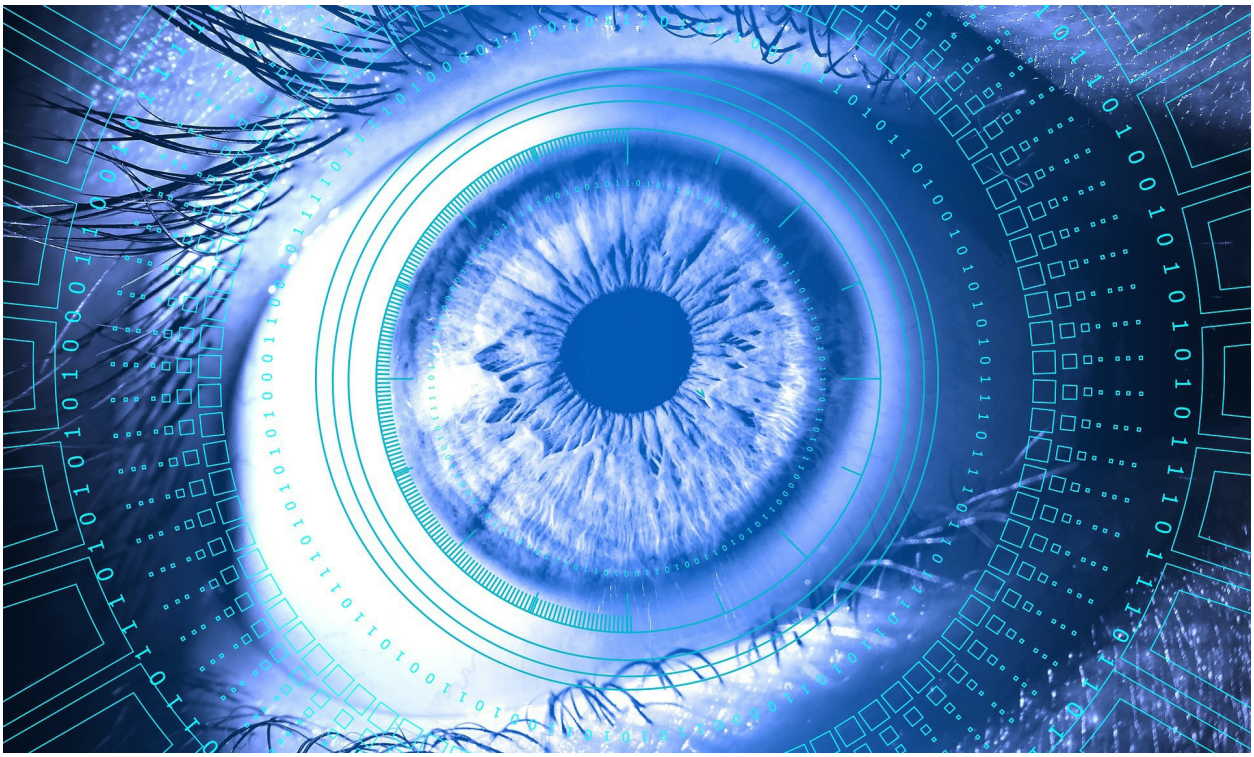
On the homepage of VMware workstation, select the option of create new virtual machine. After that choose the iso file of Kali Linux OS and then configure all the required details of virtual machine. You can start with the virtual machine by choosing Kali Linux VM and then selecting the green button which indicates Power On. After you have completed all the steps, the machine will start.

Procedure of installation

- Once the machine powers up, you need to select the preferable mode of installation right in GRUB menu. Choose graphical installation and then select continue.
- The next few screens will be asking you for selecting the locale information like your preferable language, location of origin and also layout for the keyboard.
- Once you are done with all the additional local information, the installer will be automatically installing various additional components. It will then configure the settings related to your network. The installer will immediately prompt for your hostname along with the domain for completing the process of installation. You need to provide all the appropriate and required information and then continue with the process.
- Now you are required to set up a password for the Kali Linux machine. You need to remember this password as long as you are going to use the machine.
- After you have set your password for the Kali Linux machine, the OS installer will prompt for setting up the time zone. It will then pause for partitioning of disk. The installer of OS will provide you with four different disk partition choices. The easiest option out of all is the Guided-Use Entire Disk option. If you are an experienced user, you can opt for the manual disk partitioning for having granular options of configuration.
- You need to select the disk partitioning and then click on continue.
- Make sure that you confirm all the changes that you have made on the host machine to the disk. In case you continue with the process, it will be erasing all the data on the disk.
- Once you have confirmed the changes in the partition, the OS installer will start the process of file installation. The system will be installing the files automatically. The whole process might take up some time.

- After completion of file installation, the system will be asking you for setting up the network mirror for obtaining future updates. Make sure that you select this function is you are going to use Kali Linux in the future.
- The installer will be configuring the package manager for all the related files.
- Then you will be asked for installing boot loader of GRUB. Click on yes and select the device for writing up the required information of boot loader directly to the hard disk which is necessary for booting Kali Linux.
- Select continue for finishing the process of installation.
- After this the installer will be installing some files in the final stage.

After this, you can use Kali Linux for all your requirements.



Chapter 5: Insights on Kali Linux Concepts

Linux has been well-known as one of the most powerful operating systems in the world of cybersecurity and coding. Among its various components, Kali Linux is one of the distributions which can be treated like a boon for the ethical hackers and the IT people. However, everything comes with a number of problems. In this world of today, people have excessive trust in Kali Linux capabilities by default only. As the end result, most of the users are not paying attention to the various manual aspects of the Linux security. It is true that with Linux, you can automate many of your tasks. However, it also requires some manual touch for keeping everything with the pace. This fact even becomes more evident when it comes to the concept of security.

You are required to be more attentive

Though an operating system might automate all your tasks, it is your task to be anxious always. You are required to keep a close eye on the settings of our application and various other details. When you have a well-configured system of Kali Linux, it might turn out to be the most difficult thing to crack.

However, most of the users of Kali Linux do not have profound knowledge about what is required for keeping their whole systems locked up. In case you start using a brand-new application, try to pay very close attention to the details of its configuration. Running the application with the same example settings and then using it is not the ideal option. It is not at all recommended. Some of the developers in the past also put decoy settings in the applications for making sure that the applications are prevented from running. This was a great way for ensuring that all the users have checked out the file of configuration of the application.

Handling all the permissions in the right way

When it comes to permissions, it forms an essential part of Linux. It is very important for a user to clearly understand how each and every permission function along with the implications of the various components of the OS. In case you are shifting from Windows to Linux, the generalized concept might be a bit different and awkward for you. The general rule of Kali Linux is that you are not supposed to use root for your daily work. This might sound like a bit of a surprise for all the Windows users in which the operating system handles the various permissions which are critical in nature in a different way. It is surely an inconvenient function where you are required to type a password each and every time when you want the machine to execute a function. However, it is practical as well as it will surely help in preventing some serious security problem of your machine in the future.

Kali Linux does have viruses

Linux comes with a widespread reputation of being virus-free. It is really a surprising thing for all the newcomers. However, in actual, the picture is completely different. Linux is less popular as an operating system as compared to Windows or Mac. So, it is not much targeted by the hackers and so the development of viruses for Linux is not much. But, Kali Linux malwares do exist. The malwares of Linux are even more destructive than the counterparts of Windows. This might turn out to be more dangerous for all those Kali Linux users who avoid to pay attention to the application permissions and various other core concepts of Linux security.

The security tools are available

When you start using Kali Linux, you will find out that the security tools that you used earlier are not available for Linux. This is a very common scenario for most of the antivirus solutions. The developers of antivirus cannot maintain completely two different versions for the same application along with two different underlying systems. There are various exceptions, however with them as well, you will find out various applications that will work differently for Linux. While using Kali Linux, you can enjoy an easier access to a large variety of security tools for general purpose. Kali Linux is such a distribution of Linux that comes with security as the main goal. You can also control your connection of VPN in a streamlined way with Kali Linux. Kali Linux comes with various built-in tools for working with networks which are complex in nature.

Being open source is not secure always

Kali Linux is an open source software which has made this OS the most favorite for all the ethical hackers and IT personnel. Many people think being open source is the ultimate key for being more secure. The same goes with Kali Linux. However, in reality, it is not like that. You might think that being an open source software which is exposed in front of the entire world, any kind of issue will be taken care of immediately. That’s absolutely not the case. There have been various recorded cases of security breaking and backdoors in the system of Kali Linux. In many of the cases, the security holes were put there in the system purposely. So, it can be concluded that being open source is not the ultimate sign of security. Having a closed system and reviewing the same by experts in case of any issue has its own benefits. You should never underestimate the tools of security in Windows just because of its nature being close-source.

Kali Linux is indeed a fantastic operating system for all the ethical hackers and for those practicing penetration testing. Kali Linux is obviously secured than the other distributions. However, its full effectiveness can only be pictured after computing it for a long term. Without proper insights into the application settings and its permissions, you might expose the entire system to some serious risks of security without you even realizing the same. Starting off as a beginner and having a Kali Linux distribution which has

been configured poorly might turn out to be a disaster as a whole. So, make sure to check each setting and if you want, you can customize them according to your need.

Chapter 6: C.I.A. and Its Relation with Cybersecurity

The C.I.A., also known as the Central Intelligence Agency is an intelligence service related to foreign affairs which belongs to the U.S. federal government. It is responsible with various tasks related to data gathering, analyzing and processing. C.I.A. is responsible for the national security and thus functions for protection of the same. It is well-known for gathering of information from all over the world with the use of HUMINT or human intelligence. C.I.A. is one of the most important members of the U.S. IC or United States Intelligence Community and it reports to the National Intelligence Director.

Unlike the FBI or Federal Bureau of Investigation, which is related to the domestic service of security, C.I.A. comes with no forms of function related to law enforcement and is targeted for gathering of overseas intelligence. C.I.A. functions as the central authorizing unit of the HUMINT.

Functions of C.I.A.

The primary function of C.I.A. is collection and gathering of data for the purpose of national security. According to the basic principles of C.I.A., it has five basic functions:

- Counterterrorism as the main priority
- Nonproliferation of weapons regarding mass destruction
- Informing the state about various important events overseas
- Counterintelligence
- Cybersecurity and intelligence

Chapter 7: Cybersecurity

With the advancement in the world of technology, the task of information gathering and dissemination of the same has turned out to be a very easy job. With high power machines and operating systems like Linux, the task of securing the same has been made much easier. However, with the picture of growth of any sector, comes along various threats and disadvantages. In the growing world of IT today, the security and attacks are increasing its power day by day and that too at a massive rate of progress. That is why, having a very powerful background in the concept of core security is of utter importance. When you start running a business or organization without proper knowledge about cybersecurity it might result in exposing various essential and confidential details of your work or even about individuals.

Cybersecurity in details

Cybersecurity is nothing but protection of your networks, systems and

various programs from the attacks digitally. The cyber attacks are generally targeted at changing, accessing and destroying of very sensitive data, money extortion from the users and also interruption in the processing of businesses. Cybersecurity is also known as electronic information or information technology security. Now, you might be thinking that what is cyber attack then? It is a deliberate and malicious form of attempt by a hacker in general or also maybe by an organization for the purpose of breaching organizational data.

The term cybersecurity in various contexts

The term cybersecurity can be applied in various contexts, starting from mobile computing to businesses. It can also be divided into some common categories as well.

- **Network security:** It is the term used for practicing cybersecurity for securing the network of a computer from the attackers, whether from malware which is opportunistic or targeted hackers.
- **Application security:** It is focused on keeping your devices and software free from the various forms of threats. Any form of compromised application can easily give access to all those data which it is meant to protect.
- **Information security:** This helps in protecting the privacy along with the integrity of your data, which are both in transit as well as in storage.
- **Disaster recovery:** This term defines how an organization is supposed to respond to any kind of cybersecurity incident or any other type of event that might lead to loss of data or operations. The policies of disaster recovery dictate the way in which an organization restores all its information regarding operations right in the same capacity of operation as it used to function before the event.
- **Operational security:** It includes all those processes along with the decisions required for protecting along with handling of all

your data assets. The user permissions along with the access policies of a network, the procedure of data storage and where it is stored all come under the umbrella of operational security.

- **Education of end-user:** This addresses one of the most uncertain factors that come with cybersecurity which is people. Any person can unknowingly introduce a malicious virus within a system which is super secure by not being able to follow the required measures of security practice. Teaching all the users of a system to remove all types of suspicious attachments that come with emails, not plugging any kind of unidentified hard drive or USB drive along with various other lessons is important for the organizational security.

Why is cybersecurity so important?

The world of today is dependent on technology more than it was any before. That is why there has been a noticeable surge in the creation of digital data. Today, most of the business organizations along with the government bodies stores up maximum of their confidential and important data on the computer machines. For the purpose of transmitting those across various sections of an organization or between various departments of government, they use network. The devices along with their base systems are accessible very easily when exploited from outside source. This, in turn, undermines the overall health along with the objectives of the organizations.

Breaching of data can result in a devastating condition for an organization, especially at a time when all the organizations use networks for data transmission that includes government, corporate, medical, financial and military organizations. It might turn out to be a threat for national security as well when confidential data is leaked from the government networks. A large portion of such data might turn out to be ultra-sensitive in nature, whether the data is financial data, intellectual data, information of individuals or any other form of data. Cybersecurity helps in describing the form of discipline which is required for the protection of data and data systems which are being used for processing and storing of data.

Data breach can also have a huge impact on the corporate revenues just

because of not following the regulations of data protection properly. According to some recent studies, a data breach on an average can cost an organization about $3.8 million. As the volume along with the sophistication of cyber attacks are developing day by day, the organizations and those bodies which are entitled with the task of information safeguarding in relation to national health, security and financial records, are required to take necessary steps for protecting all forms of personnel as well as business data. According to a recent survey in the year 2016, it has been cautioned that the acts of digital spying and cyber attacks are the most dangerous threat to the security of a nation, much more even than terrorism. So, the organizations are required to implement and adopt strong approaches towards cybersecurity.

Various types of threats related to cybersecurity

- **Ransomware:** It is a kind of dangerous malicious software which has been designed for the purpose of money extortion by blocking away file access or networking system until and unless the amount of ransom is paid. However, there have been various cases where the access to the files or the systems was still blocked after payment of the ransom.
- **Malware:** Malware is nothing but malicious software. It includes various types of software such as ransomware, spyware, worms and viruses as well. The functioning of malware is very simple so that the user cannot even detect any kind of breaching in the network. It is done by taking advantage of the vulnerability of a network when any user clicks on any dangerous email attachment or link that readily installs the risky software in the system. Once the malware has been installed in the system, it can do anything it wants such as:

    1. Blocking of access to the network key components
    2. Installation of other harmful software
    3. Obtains information from the storage drive without even letting the user know
    4. Disrupt various components of a system and then leave the

system fatal.

- **Phishing:** It is the practice of cyber attack where fraudulent communication is sent and appears as a genuine form of communication from any kind of reputable source. It is most commonly done via email. The primary goal of this type of attack is to steal confidential personal data such as credit card details, information regarding login and many more. This form of cyber threat is increasing day by day.
- **MitM:** It is also known as man in the middle attack or eavesdropping attack. It takes place when the attackers place themselves in between a two-party communication. Once the attackers are successful in interrupting the traffic, they can easily filter out and steal relevant data. There are two very common points of entry for the MitM attackers:

  1. By accessing through public Wi-Fi which is not secure at all, the attackers can easily place themselves in between the device of a user and the network. The user, without even knowing, passes all the relevant information via the attacker to the network which results in data breaching.
  2. When a malware has breached the device of a user, the attacker can install any form of software for processing out all the information of the victim user.

- **Social engineering:** This is a tactic which is used by the attackers for tricking the user into exposing various forms of sensitive and personal information. The attackers can easily engulf over any form of monetary form of payment or even gain all-over access to the confidential data. It is generally done by combining with any other form of cyber attack such as malware.
- **DoS attack:** DoS or denial of service, floods up the servers, systems or networks with huge amount of traffic for exhausting up the bandwidth along with the resources. In return, the system of the network becomes unable to carry out the legitimate requests. The attackers can even use up several devices for

launching this type of attacks which are known as DDoS attacks.

- **SQL injection:** Also known as Structured Query Language injection, it occurs when the attackers insert various harmful and malicious form of codes into the server that functions with SQL. This, in turn, forces the victim server to reveal out all forms of confidential information. Attackers can perform SQL injection by simply inserting malicious codes into any form of search box.
- **Zero-day exploit:** This attack hits only after the announcement of vulnerability of a network. It is generally done right before a solution or patch is being implemented. The attackers try to attack the vulnerability of the network during this time frame. The detection of this type of attack requires immediate attention.

Challenges regarding cybersecurity

For an all-round system of cybersecurity, a company or organization is required to coordinate all its available efforts within the overall system of business operation. The hardest form of challenge that comes in cybersecurity is the everyday growing structure of the risks in security within itself. In the past years, the government bodies along with the business organizations used to focus only on their very own resources of cybersecurity for the sole purpose of security of their perimeter for protecting only those components of their system which are crucial in nature. They used to defend only against the known threats. But, in today's world of cybersecurity, this form of approach is not at all sufficient. This is mainly because of the fact that the threats have evolved in size and are advancing day by day. The threats of today are on the verge of changing themselves much before the organizations can learn to cope up with the older versions of the threats. This, in turn, results in the promotion of the advisory organizations for more adaptive along with proactive form of approach towards cybersecurity. The NIST or National Institute of Standards and Technology also issued various guidelines in the framework of assessment of risk that strongly recommends a steep shift in the way of regular monitoring along with on-time assessments, which will be focusing on an approach which will be focused on data for security directly in opposite to the traditional model which was based on perimeter.

Management of cybersecurity

According to NCSA or National Cybersecurity Alliance, the organizations are required to be completely ready for responding to the incidents of cyber attacks. It is necessary for restoring the normal mode of business operations and also for ensuring that the assets of the organization along with its reputation are not in stake or danger. The guidelines primarily focus on three different areas: identification of the most important data that needs ultimate protection, identification of the added risks in relevance to the information and planning out the possible loss or damage that the organization might face if the information gets exposed or is breached. The assessment regarding cyber risk also requires all the types of regulations that might impact the procedure of data collection, storing of data and securing the same, like HIPAA, FISMA, SOX, PCI-DSS and many others.

With thorough assessment of cyber risk, you need to develop and also implement the plans for mitigating all types of risk related to cyber attack, protection of the prized possession of the company as outlined in the assessment and also detecting and responding to the security breaching incidents. This whole plan of managing your cybersecurity needs to encompass both technology and the processes which are required for building up a program of cybersecurity which is also mature in nature. The cybersecurity programs are required to cope up with and handle the sophisticated style of attacks which are carried out by the attackers. Organizations can combine a sound system of cybersecurity along with a powerful base of security employee in order to come up with the best security defense in opposite to the network attackers who are trying to access the confidential data of the organization.

Cybersecurity and the C.I.A. triad

When it comes to security models for cybersecurity, the C.I.A. triad is regarded as the most valid model of security. The security model includes three different main principles which are confidentiality, integrity along with availability. These three key principles are required for ensuring any type of system related to security. The principles which are included within the C.I.A. triad are regarded as the heart or prime component of data or information security. This model is applicable for all forms of security analysis.

Confidentiality

Confidentiality is nothing but privacy, only with very little difference in between the two. Confidentiality makes sure that no individual can view or access the resources which are super sensitive in nature without any form of proper authorization. In simple words, only the person who has been authorized as a user is permitted for the access or to view the related information in the network. The prime motive of the principle of confidentiality is to main all the secrets of an organization as secrets only. This principle is directed to the safeguarding of all forms of sensitive details from going exposed or breached due to the interference of unwanted individuals or groups. So, the principle of confidentiality is related to the all-round protection of organizational details which is accessible and visible to only those people who have been given the required access privileges. Financial transactions, plans related to business and medical details are some of the examples of the details that need to be kept confidential for the protection of information.

How can confidentiality be maintained properly?

The maintenance of confidentiality along with ensuring the same is of utter importance for protection of data that comes with the risk of being leaked to the third parties and that might lead to potential loss or damage. The most common ways of maintaining confidentiality are:

- **Steganography:** It is the technique which is used for hiding away any piece of secret and important information in the form of a simple image or text.
- **Cryptography:** This technique comes with the process of code generation, which in turn allows both the parties within a communication to communicate with each other by authenticating their identity with the help of secretive keys.
- **Access control:** This is the most widely used form of maintaining confidentiality. It takes into account proper mechanism of access control for preventing any form of unauthenticated along with unauthorized access of information

or data.

Integrity

Integrity is nothing but the assurance of completeness, trustworthiness along with accuracy of all kinds of sensitive data and information. It makes sure that no person can alter the existing information in the overall lifecycle of the data. It involves dissemination of protective steps for preventing all types of unauthenticated data alteration which is in transit. When the organizations fail to ensure integrity of information, they open up the doors to huge number of malware since it will be the prime target of all the attackers. There are various factors that ultimately compromise the overall functioning of integrity such as malicious users, computer virus, software errors and failure of hardware. With a rapid growth in the rate of corruption and sabotaging of data integrity, the integrity of data is turning out to be a huge concern for all the organizations and there is has been a huge search for the ways in order to avoid the attacks.

How can integrity be ensured?

There are three primary ways in which the organizations ensure integrity of their data. They are:

- **Hashing:** It comes with data integrity by simply combining the function of hash along with a secret key which is shared.
- **Validation of input:** It makes sure of data integrity by validating or also restricting those values which are entered by the users.
- **Digital signature:** It comes with a unique technique of mathematics that ensures there is no type of alteration or modification in the sent message.

Availability

A very common picture in most of the organizations today is that they find out that their main resources are not at all responding or is not available for the clients. The websites of the organizations are also getting slower or are not reachable as well. But, how are the organizations supposed to react to this serious issue? That is where the ultimate assurance of 100% availability of service comes in the picture.

When a situation arises when one particular system is not functioning properly and the data of that site is available very easily and is not at all secure as well, it affects a lot to the availability of information with the security of the site being affected as well. So, the enforcement of the application being available or the users using the available resources as required within a controlled environment is of utter importance. Another factor that affects the availability of resources is time. This is mainly because, when a system is not capable of delivering the services or the required details within time, the availability of the resources is also compromised a lot. So, it is required to provide the information to the authorized user within a definite period of time.

The services and products are generally described in accordance with the availability of data which in turn guarantees the availability of data for the user within a specific performance range in any kind of situation. DoS or Denial of Service attack always targets the availability of the systems simply by flooding the server with huge amount of traffic. This attack single-handedly can force a system to shutdown.

Authorization, Authentication and Accountability

Also, known as A.A.A, it is a term which is used for controlling the overall access to the resources of the system, enforcing policies, auditing usage and offering the need for details for taking charge of the services.

Authorization

It ensures that the users include all the privilege or permission which is required for performing a specific type of action. For instance, when a user is playing the role of network access, it should only have the rights of accessing with the actions of the network and nothing more than that. The user who has the access to the network only, is not allowed with any other access permission such as storage or any other type of network component. The actions of authorization and authentication are interrelated to each other. Also, it is to be noted that the process of valid authorization starts only after a successful process of authentication.

Authentication

It generally deals with all forms of personal identification. It comprises of the mechanism required for the process of validation of the incoming requests in against to some identifying credentials. The verification of identity is done in three ways:

- **Knowledge:** It is based on something the user knows or based on the knowledge of the user
- **Characteristics:** It is based on the characteristics of the user
- **Ownership:** It is based on something you are having or based on the ownership of the user

Accountability

This is the third pillar of the framework of A.A.A. This pillar of A.A.A offers the administrators with the power to easily track down the activities of a user based on a specific situation. It is the primary procedure for viewing the utilized services and also the quantity of the resources which has been used up by the users. In general, the enforcement of accountability is done by performing the audits too as establishing the systems for making and keeping the trails of audit. This form of management of logs can be very effective in respect to the accountability of IT and security of data. It administers that the actions can be determined easily and can also be traced back.

Access control

This is an aspect of the entire security of a network that manages how the users as well as the systems communicate with each other and also use up the resources. For enforcing ultimate security of the system, it is very essential to control all the resources along with every system access along with ensuring that only the authorized personnel are allowed the access. This feature is very useful for protecting the unauthorized destruction, modification, disclosure along with corruption of the system resources. It functions as the first defense line for avoiding unauthorized entry along with access. It comes with a variety of controls that prohibits the access to all the resources of the system completely based on the group identity, membership, logical & physical

location along with clearance. The access can take the form of permission for entering, consuming, restricting, controlling and protecting the system resources for guaranteeing the A.A.A framework in the system.

Non-repudiation

This deals with making of the evidences for proving various actions. This feature is all about justifying that an action or an event has happened that is not possible for repudiating at a later time. This can be achieved easily by using:

- **Timestamps:** It comes with the date and time when the composition of the document was done for generating evidences that the composed document was there at a certain time.
- **Digital signature:** Adding up to the integrity of data, the digital signatures make sure of the identity of the sender. It generally enforces the identity that cannot be denied by the sender later.

Non-repudiation levels

For experiencing complete non-repudiation communication level, it is important for ensuring the same at three different levels:

- **Of origin:** This can be very easily ensured by sending the data with certificates and digital signatures.
- **At delivery:** This can be ensured with the acknowledgement of the recipient.
- **For submission:** This can be ensured simply by sending the delivery recipient directly to the sender.

Evolution of cybersecurity

The traditional form of cybersecurity is constricted only around the usage of defensive measures within a specific boundary. Several initiatives of enablement just like BYOD or bring your own device and remote workers policy have helped in completely dissolving the boundary and have also expanded the surface of attack. Today, the incidents of data breaching are developing rapidly despite of the huge amounts of spending on security. Most

of the global organizations are turning towards a new kind of approach towards cybersecurity which is completely human-centric. This new approach focuses on the rapid changes in the behavior of the users in place of just tracking the growing number of threats. This form of cybersecurity helps in providing deep insights into the interaction of end-user with the data and also extends the controls of security of all systems.

Chapter 8: The Threat of Malware and Cyber Attacks

Malware

Every year, there are various campaigns launched by the medical communities for protecting everyone from flu by giving them flu shots. The outbreaks of flu have a particular season, a fixed time when it starts to spread and infects people. When it comes to the world of technology, they are also infected by flu. However, there is no predictable season for the infections of smartphones, PCs, tablets, organizational networks, servers etc. It is always a season of flu for the world of technology. But, the flu of the technology world is completely different from that of the human world. It is known as malware.

Malware, also known as malicious software is the term which is used for describing any type of malicious or harmful code or program which is

dangerous for the health of a system or network. The malware is intrusive in nature, invades the systems and damages the system of computer, network and even mobile devices. Some malware is so dangerous in nature that they can even take over the functioning of a system. Malware cannot damage the hardware of the systems; however, it can steal, delete or encrypt confidential data without the permission of the user.

Most common ways of getting malware in the system

When it comes to malware, it can enter the system via various pathways. However, two of the most common pathways via which malware access the systems are email and internet. So, it can be said that malware can enter a system whenever the user is connected to the internet if proper methods are not adhered for the security of the system. Malware can get into computer systems when anyone surfs through websites which have been hacked, click on demos of games, install malicious toolbars in the browser, open a dicey form of mail attachment and many more. In short, any sort of item which is browsed online that lacks in proper security measures can allow malware in the systems. Malware attacks can never function without the most important component which is the user. It depends on the user what they browse and they need to take care that the items or websites they are using on the internet are actually safe and authenticated.

A user can make gateway for malware when they install a software from a credible source as well if proper attention is not paid to the request of permission at the time of installing.

Common types of Malware

When it comes to malware and to its types, the list is huge. Here are the most common types of malware:

- **Adware:** This is a form of unwanted software which has been designed for throwing up unwanted advertisements on the screen of the user and is most commonly found while using a web browser. Generally, this type of malware hides itself as being legit and tricks the users in installing the same on their PC or mobile device. Such malware might turn out to be really

dangerous and the most common form of target of this malware is credit card and bank details.

- **Spyware:** This malware can easily be understood by its name “spy”ware. Just like a spy, such software observes the activities of the users in a secret way and then reports the recorded activities to the author of the software. Such malware function in a secretive way without even letting the user to know that his actions are being watched.
- **Virus:** This is a form of malware that attaches itself with some other program. When such infected programs are executed, generally without any attention of the user, the malware replicates by the process of modification of other programs and infects the other related programs with its infected series of codes.
- **Worms:** Worms are similar to viruses only and are also of self-replicating nature. It generally spreads via the computer networks and causes harm to the same network by destroying the important files and data.
- **Trojan:** Also known as Trojan horse, it is regarded as the deadliest type of malware. Such malware tricks its existence as being very useful for the system. When the Trojan gets into the system, the attackers behind the malware gains overall unauthorized access to the target system. Trojans are used for stealing confidential data such as financial information, business plans and personnel data or even installs other ransomware.
- **Ransomware:** It is a form of malware that locks out the users from the systems or encrypts essential data. The attackers of such malware force the victims to pay out a ransom amount for getting the access of their systems back. The existence of such malware is increasing day by day and has been the most threatening form of malware.
- **Rootkit:** This form of malware provides the attackers with all forms of administrative privileges on an infected system. It has been designed for staying hidden from other forms of software

on the system, from the users and from the operating system of the infected system as well.

- **Keylogger:** This malware is regarded as the trickiest of all. It records the keystrokes of the user which he makes right on the keyboard. This malware stores all the gathered data and then sends it directly to the attacker who is looking out for details of credit cards, usernames, passwords and various other sensitive forms of data.
- **Cryptomining:** Also known as cryptojacking, it is a form of prevalent malware which is being installed by Trojan. It allows someone else to operate the system of an organization for mining out cryptocurrency such as Monero or Bitcoin.
- **Exploits:** It is a type of malware that takes full advantage of the bugs along with the prevalent vulnerabilities within a system for allowing the attackers to take overall control. Among all the other form of threats, exploits can be linked with malvertising that is well known for attacking via a legit website that pulls harmful content from any bad site unknowingly. The harmful content tries to get installed in the system and take over it completely.

Who are the prime targets of malware?

To be very honest, anyone might turn out to be the target of malware. There are huge numbers of consumers who use various types of devices every day. The devices are connected to various accounts in retail stores, banks and other types of data. In short, most of the devices of today have something that is worth stealing. Spyware and ransomware are the most widely found forms of malware in the devices of today. The victims fall in the trap without their own concise. Whenever the attackers find out any form of vulnerability in the devices, they try to attack it and steal information from it. One can easily find out millions of bank fraud cases every day where the details about one’s credit card or bank account get exposed to the attackers. All of this has been possible only due to one reason, malware. So, it can be said that anyone around you or even you might turn out to be their next target.

Moving away from the personal device threats, the big organizations are being threatened every day. The malware just gets within their information boundary and mines out all the information required by the attacker. It might also happen that any competing organization might also try to get into the data bank of some other rival company. So, it is best to always take care of the security of data bank as malware attacks cannot be traced at all.

How to protect the devices and networks from malware?

In order to protect the devices along with the organizational networks from malware, the prime thing that can be done is to update the security of the systems. It might not be possible to that extent when it comes to personal devices but it is possible in case of organizational database and networks. That is where cybersecurity comes into play. It helps in protecting all forms of sensitive data from external attacks by updating the systems from time to time according to the evolution of the attacks. It is true that malware attacks are not going to stop that easily, but it is the duty of the organizations to take care of their system with proper cybersecurity in place.

When it comes to personal devices like PCs and mobile devices, it is best not to open any kind of suspicious attachment in emails or suspicious advertisements on the websites. Stay vigilant always and this way you can easily prevent any form of malware attack.

Cyber Attacks

With the advancement in technology, the attacks of third parties on organizational networks and servers are increasing day by day. Gone are those days when people used to store all their confidential data and information in files as physical items in the lockers. With new technological innovations, this storage of data has been shifted to online networks and servers. The online storage of data on clouds and servers allows the users to store as much data as they want and also access the same whenever they are in need of them. But, every form of advancement comes with certain side effects that adversely affect the whole functioning of a system. The same

goes in the case of organizational and personal data stored in online servers and networks. The attackers are always ready to find a victim and steal everything that they get.

Cyber attack is nothing but stealing of information which launched from one or various computer systems against another system or network. Cyber attacks can be easily broken down into two significant parts: attacks where the main motive is to disable the functioning of the victim system and the attacks where the main goal is accessing the confidential data of the victim system and gaining administrator privileges.

Examples of cyber attacks

The news of cyber attacks can be heard every day, some make it to the headlines where some does not. Whatever maybe the intensity of the attack, the motive is the same in most of the cases. Here are some of the greatest cyber attacks in the recent years:

- **WannaCry:** This was a ransomware attack that broke in the year 2017. Like every other ransomware, it also took over the systems of computers and encrypted all the information on the storage. In turn, the attackers demanded for Bitcoin for decrypting those data. The game of malware is nothing new but WannaCry left its mark as it oppressed the susceptibility in Windows by the use of a code that was developed by the US National Security Agency.
- **GitHub:** GitHub is famous for the service attack with about 1.30 TB per second of traffic that hit many popular sites.

Types of cyber attack

Phishing

Phishing is a very common form of cyber attack. The attackers use this technique for fooling the victims. The attackers craft emails in such a way that the victims assume the emails to be legit and fall prey to the harmful actions. The victim might get fooled in downloading dangerous malware that

might be disguised in the form of any important document or any website link. It is most commonly done using website links where the victim is asked to enter their bank or credit card details and passwords. Such websites are generally fake and are made for such purpose only. Most of the emails of phishing are coarse in nature and are sent to thousands of victims at a time. But, there are also specific phishing emails that are sent only to a particular target to get the information that the attacker wants. Phishing can be done via email, website, advertisements and even game demos that can be found online.

SQL injection

It is means used by the attackers for exploiting susceptibility in order to take complete control over the database of the victim. There are many databases which have been designed for obeying all the commands which are written in SQL or Structured Query Language. There are also various websites that take up information from the users and then sends the gathered data to the databases of SQL. In the case of SQL injection, the attackers try to write some commands of SQL in the web form that will ask for address along with information of name. In case the website along with the database is not properly programmed, the attackers will gain control over the database with the database trying to execute all the commands of the attackers.

MITM

MITM, also known as man in the middle is another method of cyber attack which is used by the attackers. In this method, the attackers impose themselves in a secretive way between the pathway of the user and any type of web service that the user is trying to or wants to access. This is mainly done across free Wi-Fi networks where there is no form of security. The attacker can easily hack such networks and wait for the user to establish a connection with any web service. Once the user sends in important information to the web service via the attacker being in the middle, the attacker gains access to all that information that he needs, without even the user knowing anything about it. The user unknowingly sends in all the information like bank or credit card details. The attacker can easily harvest any form of data that he wants including the passwords of bank accounts.

DoS & DDoS

DoS or denial of service is a form of cyber attack which is used by the attackers for stopping some online services to function in the proper way. The most common way in which it is done is by sending a huge amount of traffic at a time to a website or a huge number of requests at a time to the database that the database loses its ability to handle so much traffic at a time and thus stops functioning. DDoS or distributed denial of service is another form of cyber attack that uses number of computers that comes with malware under the guidance of the cyber criminals and sends up all the traffic towards a particular target.

Maps of cyber attack

Cyber attack map is nothing but a source that easily shows what kind of attacks are emerging up from which countries. It also provides information about the main targets of the cyber attacks along with providing a bird's eye view of the present threat of internet landscape. It is really useful for the big organizations but it comes with one drawback. It shows up everything in absolute details but the data that it presents is not live. It is not that much comprehensive as well. However, they can be used for beginning any kind of conversation regarding security, cyber attacks and the security tools that can be adopted by a company.

MAC Spoofing

Every device that people use comes with a NIC or network interface controller. NIC is the thing which is responsible for allowing the users to directly to a network such as the internet. Every device that has the capability of connecting to a network like laptops, PCs, router, smartphones etc. comes with NIC. Each of the NIC comes along with a special MAC address which is hard-coded and it cannot be changed as well. However, in spite of the fact that MAC addresses cannot be changed, some of the major operating systems such as Windows or Linux, allows the users to change the MAC addresses without any kind of hardship.

According to the tech world, as the users cannot change the MAC addresses which are built in the NIC it does not mean at all that the users cannot make the other devices to think that their MAC addresses are completely different. Each and every data that will be leaving your device will be in your control.

The data packet headers come with the device address, IP address along with the MAC address. So, it is possible to instruct the NIC to completely discard the MAC address that is built-in and instead of that use something which is customized by the user. It can be anything, in the way the user wants. This changing of MAC address is known as MAC spoofing.

What are the various ways in which hackers use MAC spoofing?

MAC spoofing opens up a wide range of options for all the hackers as they can easily hide behind their customized MAC address, without the risk of getting caught or traced. MAC spoofing provides a variety of variety of vectors for the hackers such as:

- It makes it easier for the attackers for MITM or man in the middle attacks.
- The attackers can easily hack any Wi-Fi network by spoofing their MAC address.
- The attackers can directly target those devices which are connected to the LAN.
- In case an attacker has been banned on a particular Wi-Fi network, they can easily gain access to that network by tricking the network to think that they are someone else.

Other uses of MAC spoofing

Anonymization

There are various users who prefer to hide their identity and of their device right behind a customized MAC address which is not theirs. Such people are not hackers but are those who handles large amount of confidential data every day over the internet. This is done for protecting the privacy of the users. The main reason behind this is because the MAC addresses which are sent over any LAN or WLAN network which is public in nature are actually unencrypted. So, any user on the same network can track the devices which are registered within that network. People on that network can also access the data of the other systems and can also use the same for illegal activities. That is why masking the MAC address of those devices that functions over public

LAN networks is a great option for protecting privacy and preventing data loss.

Theft of identity

For the protection of the IT systems from all kinds of external as well as internal dangers, the administrators many times implement various security measures for restricting the access of the authorized devices to the LAN. In such cases, linking elements like Ethernet switch helps in separating the bigger networks into various small segments. Once a connection has been linked from one segment to the other, Ethernet switch checks sender device's MAC address and then matches it with the administrator record. In case the address does not match, the connection is blocked. However, the users of Windows and Linux OS can easily establish connection with the LAN without the use of MAC address.

ARP Spoofing

ARP spoofing is another type of cyber attack in which the attacker sends false Address Resolution Protocol or ARP messages over LAN. As a result, the MAC address of the attacker gets linked with the IP address of the target system or server. Once a connection has been established between the MAC address of the attacker and the IP address of the target system, the attacker will be receiving all those data which is being sent to the targeted IP address. ARP spoofing leads to interception of malicious attackers which can even result in modification or stopping of data transfer. ARP spoofing can only be done on LAN networks that work with ARP.

Attacks of ARP spoofing

Like other cyber attacks, ARP spoofing is a very serious one. It can have serious effects on the functioning of big enterprises. ARP spoofing is mainly used for stealing all forms of confidential and sensitive data from the target system. Not only that, but ARP spoofing attack also helps in several other types of attacks such as DoS attacks, MITM attacks and hijacking of session as well.

Detection and protection from ARP spoofing

There are various ways in which you can detect ARP spoofing and protect your system from the same.

- **Packet filtering:** The packet filters help in inspecting the data packets as they are transferred across any network. Packet filters can help in preventing ARP spoofing as it is capable of easily filtering and blocking those packets which comes with any form of suspicious information of source address.
- **Using ARP spoofing detecting software:** Most of the organizations today are using detection software for ARP spoofing. Such software functions by properly inspecting and then certifying the data before the transmission takes place. It also helps in blocking those data that seems like being spoofed.
- **Using protocols for cryptographic network:** SSH or secure shell, TLS or transport layer security and HTTPS or HTTP secure are some of the protocols that can help in preventing the attacks of ARP spoofing by encrypting all the data just before the process of transmission and then also authenticates the data when received.

Rogue DHCP Server

DHCP is the main reason behind the assigning of logical addresses of the systems which is the IP address. In case of a DHCP attack, the attacker sends out huge number of requests of DHCP packets along with MAC address which is spoofed in nature which is generally done by the use of tools like DHCP Rogue Server. When a lot of requests are sent, the server of DHCP starts responding to all the requests, allowing the attacker to consume all those IP addresses which are available to the server for some time. This is a form of DHCP DoS attack. In such attacks, the available pool of IP addresses is consumed by the hacker and blocks out any other new request.

More about DHCP and DHCP server

DHCP also known as Dynamic Host Configuration Protocol is the protocol which is responsible for the management of DHCP server which assigns the available IP addresses to all the hosts which are alive along with other information of configuration like default gateway and subnet mask. DHCP is

responsible for IP address assigning for each and every network.

How does DHCP work?

A DHCP server serves the function of issuing IP addresses to the systems and also configures all other information of a network. In small networks and in homes, DHCP is available within the router and for large organizations, it is available in individual PCs as well. DHCP server shares this overall information to the DHCP client with the help of exchange of a message series which is also known as DHCP transaction.

DHCP attack

DHCP attack or DHCP starvation attack is a form of attack vector in which the attacker sends out large amount of requests for DHCP data packets along with spoofed addresses of MAC. DHCP attack is known as attack on a network of computers in which all the available IP addresses which have been awarded by DHCP to one single client can be registered. This can also be compared to DoS attack in which the attacker floods the database of a system with so many requests that blocks away the acceptance of any new request.

Details about Rogue DHCP server

The Rogue DHCP server is a form of DHCP server which is situated on a network and is unauthorized and not permissible by the administrator of the network. This form of DHCP servers is created by the cyber attackers in which all the IP addresses which are available are starved, forcing the victim network to connect to the malicious server of DHCP of the attacker in the similar network.

DHCPig

It is a tool of networking which is used for the initiation of an advanced form of DHCP starvation attack in which all the available IP addresses on the LAN will be consumed. As a result, it will block the new users from getting the IP addresses, block any form of IP address which is in use and then sends ARP for knocking all the host windows offline. This feature of DHCP server attack comes built-in with Kali Linux. It requires no form of configuration. The

attacker only needs to pass on the interface as the parameter of the network.