HACKING

— 2 BOOKS IN 1 —

Hacking with Kali Linux

Computer Networking for Beginners

Jason Callaway

HACKING

— 2 BOOKS IN 1 —

Hacking with Kali Linux
Computer Networking for Beginners

Jason Callaway

HACKING

2 Books in 1:
Hacking with Kali Linux & Computer Networking
for Beginners.

Practical Guide to Computer Network Hacking,
Encryption, Cybersecurity, and Penetration Testing

Table of Contents

BOOK 1:
HACKING WITH KALI LINUX

Practical Guide to Computer Network Hacking, Encryption, Cybersecurity & Penetration Testing for Beginners.
The Secrets of VPN Services, Firewalls and the Linux Command Line

Introduction

I am very much delighted to see that you all have shown so much interest in learning about the basics and usefulness of Kali Linux. Kali Linux is one of the most effective software of today. It can also be regarded as a boon for all computing and networking people.

Kali Linux does the job of a security auditing software and it also helps in various aspects of networking and hacking. Kali Linux comes along with various information and security-related tasks such as reverse engineering, penetration testing and security research. Computer forensics is also a part of Kali Linux. Each and every service which is provided by Kali Linux is certified and comes along with all-over control along with wider aspects of accreditations.

Kali Linux belongs to the family of Linux distribution. Cyber security is the prime concern of this Linux distribution. Many of the companies today take help of Kali Linux for checking and tracing out their vulnerabilities for ensuring 100% security of their infrastructure. It is an open-source program and is thus totally free. Not only that but it is completely legal and can be used for various scenarios in an enterprise or organization.

Chapter 1: Basics of hacking

Hacking is nothing but unauthorized intrusion within a network or computer which is executed by attackers known as hackers. The attackers try to attack those systems which are vulnerable to threats. They keep their prying eyes open all the time, searching around for vulnerabilities. They can act as an individual or even work in a group. Not only might that but the hackers also function as a part of an organization which works with the motive of disrupting the functionalities of other organizations. Most of the time they try to alter the system of an organization and target the security infrastructure for breaching of information and gaining access. However, hackers not only work as attackers but also use their skills for finding out the weak spots along with the various vulnerabilities within a system. This is also carried out for finding and mending the weaknesses for preventing all forms of malicious attacks from entering the system.

Different Types of Hackers

There are various types of hackers in the world of hacking which perform different types of functions. The types of hackers help in defining the relationship between the systems and hackers which are trying to attack. The most common types of hackers are:

- **Black Hat Hackers:** The term black hat had its origin from the old Western movies in which the villains used to wear black hats. The black hat hackers act as individuals who try to have unauthorized access into the system of an organization or network for the purpose of exploiting the security infrastructure for various malicious reasons. The hackers of this type do not come with any sort of authority or permission for compromising the targets. They attempt to do damage by compromising the infrastructure of the security systems, shutting down the systems or also by altering the primary functions of a website or network. The primary intention of the black hat hackers is to gain all-over access or steal the information regarding finances, access various passwords or gain insights into other forms of personal data.
- **White Hat Hackers:** The white hat hackers are the second type of hackers but they act as the good guys. The white hat hackers work with various organizations for the purpose of strengthening the security of any system. The white hat hackers come with all sorts of permissions for engaging the targets and also compromise the same within the provided boundary of rules. The white hat hackers are also known as ethical hackers. The ethical hackers specialize in this field with various forms of ethical tools and techniques meant for hacking. They use special methodologies for securing up the information system of an organization. Contrary to the black hat hackers, the ethical hackers exploit the security system of a network and then check out for the backdoors after being legally permitted to perform so. The ethical hackers always point out all forms of vulnerabilities that they dig out from the systems of the organizations to make sure that the gaps are mended for preventing exploitation by the malicious attackers.

- **Grey Hat Hackers:** The grey hat hackers gain access to the security systems of the organizations and networks in the same way just like black hat hackers do. But the grey hat hackers perform such actions without any form of malicious intent and disclose the vulnerabilities along with the loopholes to the agencies of law enforcement or various intelligence agencies. The grey hat hackers generally surf the internet and hack the computer systems for notifying the owners or the administrator of the network or system which contains various vulnerabilities which need to be mended immediately. The grey hat hackers might also extort the hacked systems by offering to inform about the defects for some fees too.

Common Tools of Hacking

For accomplishing the act of hacking, the hackers implement various types of techniques. Let's have a look at some of them.

- **Rootkits:** Rootkit acts like a program or a huge set of software which allows the attackers to gain complete access or control of a system or network which directly connects or interacts with the system of the internet. Rootkit was first introduced as a system of backdoor process for fixing various issues in regards to software. However, today this software is widely being used by the hackers for disrupting the functionality and control of a system from its actual owner or administrators. There are various ways in which rootkits can be installed in the system of the victim. The most common way of installing rootkit is by implementing phishing attacks along with social engineering. Once the rootkits have been installed in the system of the victim, the attacker gains access to the system secretly and controls the overall functioning with which they can easily steal confidential data and information and can also shut down a system completely.
- **Keyloggers:** This is a very special type of tool which has been designed for recording and logging each and every key pressed on the victim system. The keyloggers record the stroke of the

keys by staying attached to the Application Programming Interface or API. It tracks the key strokes when anything is being typed by using the keyboard in a system. The files which are recorded are then saved which contains various forms of information such as details regarding website visit, usernames, the record of opened applications, screenshots, bank details and many more. The keyloggers are also capable of capturing the personal messages, credit card details, passwords, mobile numbers and various other details which are generally typed in a system. The keyloggers generally arrive as a malware which allows the cybercriminals to breach all forms of sensitive data.

- **Vulnerability scanner:** A vulnerability scanner is used for the purpose of classifying and then detecting various forms of weaknesses in a system, network, communication system, computers etc. This is one of the most common forms of tool which is being used by the ethical hackers for finding out the potential vulnerabilities and loopholes and then fixes them up on urgent basis. However, a vulnerability scanner can also be used by the black hat hackers for checking the vulnerabilities and weak spots within a system and then finding out the proper tool for exploiting the same.

Techniques of Hacking

There are various techniques which are being used by the hackers for exploiting a system.

- **SQL Injection:** SQL or structured query language has been designed for the purpose of exploiting various forms of data in the database of the victim. This form of attack falls under the cyber attack which targets the databases via the statements of SQL for tricking the systems. This form of attack is generally carried out by the use of website interface which attempts in issuing the commands of SQL through a database for hacking the passwords, usernames and other related information related to the database. All those websites along with web applications which are coded poorly are very much prone to the SQL injection attacks. This is because the applications which are based on the web contains various user input fields like login pages, search pages, request forms related to support and products, comments section and many others which are very much susceptible to the attacks and can be very easily hacked by simple manipulation of the codes.

- **DDoS or Distributed Denial of Service:** It is a form of hacking attack in which the normal traffic of a server is distorted from entering the server and floods the traffic of the network. This ultimately results in denial of service as it serves just like a traffic jam which clogs the roads and also prevents the regular form of traffic from reaching the destination. All the devices of today such as IoT devices, computers, mobile phones etc. which connects with the network are very much prone to the attacks of DDoS.
- **MAC Spoofing:** Each and every form of device which are used by the people today come with network interface controller or NIC. It helps the users to connect with the network such as with the internet directly. The NIC of each device is accompanied with a MAC address which is assigned after various processes of hard coding. The MAC spoofing attack is a very deadly form of attack in which the hackers hide themselves and their system behind a customized and false MAC address. This reduces the risks on the part of the hackers from getting caught. So, you might give access to a new system thinking of it to be absolutely legitimate but it might happen that a hacker will hide himself behind a false MAC address which you cannot even realize.

By using this technique, the hackers can easily hack internet connection via Wi-Fi and can also gain access to all those devices which are connected to each other via LAN. The technique of MAC spoofing also leads to several forms of other serious crimes in which the hackers steal the identity of someone else and carries on with some serious form of data breaching in which someone will be held as guilty without even knowing about the actual hacker.

However, there are various OS in the market today such as MAC and Windows which can easily connect with the LAN without using the MAC address.

Chapter 2: What is Ethical Hacking?

Ethical hacking is also called as intrusion testing, penetration testing and also red teaming. In simple words, it is the controversial technique of finding out vulnerabilities and weaknesses in a system simply by imitating the actions and intent of the malicious hackers. An ethical hacker is a person or security professional who uses his skills for the purpose of various defensive measures on part of the administrators of an information system. An ethical hacker is also known as a white hat or white hat hacker. By conducting various tests, an ethical hacker tries to find out the answers to the following questions:

- What are the locations, systems or information can the attacker gain access?
- What will the attacker see before setting his target?
- What will the attacker do with the information which is available in the system?

- Is anyone able to notice the various attempts made by the attacker to gain access?

The ethical hacker who has been given the job of penetration testing operates on the permission along with the knowledge of that organization for which he has been assigned the job of defense. There are various cases in which an organization will not be informing the security information team about all the activities which is going to be carried out by the ethical hacker just for testing the effectiveness and concise of the security information team. This whole thing is also known as double blind environment. For the purpose of effective and legal operation, the organization needs to inform an ethical hacker about all those assets and information which are meant to be protected, the potential sources of threats and the limit to which the organization will be supporting the efforts of the ethical hacker.

Process of ethical hacking

All the ethical hackers follow a strict process in order to get the best usable and to the point legal results. Let’s have a look at the processes which are followed by the ethical hackers.

Planning

No matter what kind of project it is, for every successful project planning is of utmost importance. It provides the ethical hackers with the opportunity of thinking about what are the things that need to be done, set the goals which are to be reached and also for the assessments of risks for evaluating how to carry out a complete project. There are various factors which are considered by the ethical hackers before carrying out a project of ethical hacking. The list of factors includes culture, policies of security, laws, regulations, requirements of the industry and best practices. All of these factors play an important role in the process of decision making when it comes to the initiation of ethical hacking.

The phase of planning in ethical hacking will be having an overall influence on how the process of hacking is being performed, the information which is collected and shared and will also be directly influencing the integration and delivery of the results into the program of security. The planning phase is the very first step and will be describing most of the details about the controlled attack of hacking. It will also be answering all forms of questions regarding hacking such as how the process of ethical hacking is going to be controlled and supported, what are the basic actions which needs to be performed and for how long will the process go on.

Reconnaissance

It is the process of searching for all those information which are freely available for assisting in the process of attack. This whole process can be as easy and simple as just using a ping or browsing the various newsgroups which are available on the internet for searching that information which is leaked by the employees or as tough and messy as digging through a huge trash of letter or receipts. This process can also include several other processes such as phone tapping, social engineering, network tapping and also data theft. The process of information searching will be limited only to the extent to which the organization and the ethical hacker will want to go for the purpose of recovering all the required information which they are looking out for.

The phase of reconnaissance introduces the deep relationship in between the tasks which needs to be completed and all those methods which will be needed for protecting the information and assets of the organization.

Enumeration

It is also known as vulnerability or network discovery. Enumeration is the process of obtaining all those information which is available readily from the system of the target, networks and application which are used by the target. It is also to be noted that the phase of enumeration is the actual point where the thin line between malicious attacks and ethical hacking gets blurred very often as it is very easy and simple to go outside the dedicated boundaries which have been outlined in the original plan of attack. For the purpose of creating a clear picture of the environment of an organization, various techniques and tools are being used which are readily available. These available tools include NMap and port scanning. However, it is very easy to collect all the required information, it is very difficult to make sure of the value of information which is available in the hands of the hacker.

At the very first glance, the process of enumeration seems to be very simple in which data is collected then evaluated collectively for establishing a proper plan for more searching or building up a detailed matrix for the analysis or vulnerability phase. However, this phase is the actual phase in which the ability of ethical hacker in taking logical decisions plays a very important role.

Analysis of vulnerability

For the purpose of effectively analyzing all the data, an ethical hacker needs to employ a pragmatic approach which is logical in nature as well. In the phase of vulnerability analysis, all the information which has been collected is compared with all the known forms of vulnerabilities in the practical process. Any form of information is useful in the process, no matter from where it originates or what the source is. A small pinch of information can also help in finding out some new sort of vulnerability in the system and might also lead to several other discoveries of vulnerabilities which have not been found yet. The known form of vulnerabilities, service packs, incidents, updates along with various hacker tools helps in properly identifying the point of attack. The internet provides the ethical hackers with a huge amount of information which can be associated very easily with the system architecture along with weak and strong points in a system.

Exploitation

A considerable amount of time is spent for the purpose of evaluating and planning an ethical hack. It is very obvious that all of these planning will lead to some sort of attack. The level of exploitation of a system can be as simple as running a very small tool in the system or as tough as a collection of many complex steps which needs to be executed in a proper way for gaining access to the system. The process of exploitation can be broken into a collection of subtasks which can be either one single step or a collection of various steps. As each and every step is performed, a process of evaluation takes place which ensures that the outcome which has been expected is met. Any form of divergence from the plan of attack can be graded into two parts:

- **Expectation:** Are the expected results of exploitation met or the results are conflicting with the assumptions of the organization?

- **Technical:** Is the target system behaving in a manner which is not at all expected, which is actually having an impact on the system exploitation and the system engagement in total?

Final analysis

Although the phase of exploitation comes with a huge number of validations and checks for ensuring the success of the hack, one last final analysis is needed for categorizing the system vulnerabilities in accordance to the exposure level and also for assisting in the drawing up of a plan for mitigation. The phase of final analysis links up the exploitation phase and the deliverable creation. A comprehensive image of the complete attack is needed for the construction of a bigger size picture of the current posture of the security environment of an organization and also for expressing the vulnerabilities clearly.

Deliverables

Deliverable communicates with the test results in a variety of ways. Some of the deliverables are concise and short in nature which only provides the vulnerabilities list along with the ways in which it can be mended whereas, the other form of deliverables can be detailed and long which will provide a list of the probable vulnerabilities in a system which comes with the description regarding how the vulnerabilities were found, how they can be exploited, the results of having such vulnerabilities within the system and how to fix the situation. This phase is actually used by an ethical hacker in conveying his hack results to the organization. It can also be the case if the deliverables do not actually frighten the administrators, the test is considered as a fail.

Chapter 3: Cyber Security

In this world of today where technological innovations are taking place every day, the potential threats of cyber attacks are also increasing in equal pace. Cyber security plays a deep role in securing the information and data of the systems and networks in today's world of vulnerability. Cyber security is nothing but the employment of various tools and technologies for the purpose of securing the networks, programs, system data and network from the potential attacks, damages and various forms of unauthorized access. Cyber security is also known as security of information technology.

Cyber security and its importance

Most of the organizations and institutions such as military, government, medical along with financial bodies stores up an accountable amount of data on the systems of computers along with databases which can be found online. In most of the cases, the information which is being stored up in the servers and databases are highly sensitive in nature, leakage of which can result in serious troubles for the concerned organization. Unauthorized access to the systems of the organizations along with the database can lead to data breaching along with the exploitation of the security infrastructure of an organization.

The organizations which are targeted might lose up all forms of sensitive data along with complete loss of access to the systems. As the volume of cyber attacks is increasing day by day, the organizations especially those which are concerned with national health and security are required to take some serious steps for safeguarding all forms of sensitive data. Cyber security is the ultimate option which can help an organization in protecting all its data and servers.

Cyber Security & Encryption

Encryption is the process of encoding communication in such a way so that only the authorized parties can encode the message of communication. It is done by using SSL/TLS and PKI protocols. The very reason why is it important so much stems from the process in which the internet was built up by using the protocol of HTTP. Hypertext Transfer Protocol or HTTP is of the same age that of the internet. HTTP is the protocol of communication which allows the servers in the web and the web browsers for communicating and displaying the information in a proper intended way. When a user visits a website, it is not actually the way it looks in the browser. Websites are built up of a bunch of codes which are sent to the web browsers which are then visually arranged by the browser in the way the web designer intended to do.

The main problem of HTTP is that it is not at all secure. So, any person who knows the process can easily spy on the connections of HTTP on the internet. In simple words, a third party can easily read along with manipulate a communication over HTTP between the clients and the servers. Encryption is the technique that actually comes into play in taking care of the communication by serving the websites over the protocol of HTTPS. HTTPS is the secured version of HTTP. All the connections which are built over HTTPS are encrypted in nature. In simple terms, any form of communication over the protocol of HTTPS is highly secure. Encryption prevents spying on communication by the third parties. In case you are related with online business and you need to take the financial as well as personal details of the customers, make sure that your website is encrypted so that your customers are not at risk at the time of details exchange.

How does the process of encryption work?

The process of encryption begins when the web browser reaches one website which comes with an SSL certificate. The web server and the browser proceeds with what is known as SSL handshake. At the preliminary stages, the web browser verifies that the SSL certificate which is installed in the website is legitimate in nature and has been issued by a trustworthy authority of certification. After the web browser makes sure that the certificate is legitimate in nature, it starts to negotiate with the terms of the encrypted connection with the server.

When it comes to encryption, there are mainly two key pairs. The first is the asymmetric key pair which consists of the private and public keys. These keys have no function with the encryption bulk but they are used for authentication. When a web browser tests the authenticity of SSL certificate of a website, it makes sure that the certificate of SSL which is being questioned is actually the owner of the public form of key. It performs this by using up the public key for encrypting a small packet of data. If the web server is able to decrypt the data packet by using the respective private key and then send the packet back, it is proved that the server is the owner of the public key and everything is stated as verified. In case the web server fails to decrypt the data packet, the certificate of the server is taken as “not trusted”.

The other key pair is the session keys. This form of keys is generated after the authenticity of the SSL certificate has been verified and all the terms regarding encryption have also been negotiated. While a public key can be used only for encrypting and a private key for decrypting, the session keys can be used for both the functions of encryption and decryption. The session keys are smaller in size and also less secure in nature when compared with the asymmetric form of counterparts. However, the session keys are strong enough for performing both the functions. The server and the web browser use the session keys for the rest of the communication. After leaving the site, the session keys which are being used are discarded and brand-new session keys are generated for the new visit.

Common Types of Cyber Attacks

Cyber-attacks are increasing day by day with the innovations in the world of technology. There are various types of cyber-attacks that can be found today where some are used most commonly such as phishing, malware, XSS and many more. Let’s have a look at some of the most common types of cyber attacks.

Malware

Malware is a form of harmful software which is used for gaining access to the systems of the victims. The malware can also be called as viruses. Once a malware enters the victim system, it can lead to havoc starting from gaining overall control of the system to the monitoring of all sorts of actions, stealing sensitive data silently and also can lead to a complete shutdown of the system. The attackers use various ways for inserting malware in the target system. But there are also various cases in which the system users are being tricked into installing a malware in the system.

Phishing

Receiving emails with various unwanted links and attachments is a very common thing today. Such action of sending out harmful links and attachments via email is known as phishing. In phishing attacks, the attackers send out emails to the targets which seem like a trustable email. Most of the emails come with links and attachments which when clicked leads to the installation of malware in the system without even the user of the system knowing nothing. Some of the phishing links can also lead the users to a new website which might ask for confidential data such as bank and credit card details. Such websites are actually a trap which is used by the attackers for installing the malware in the target systems.

XSS

Cross-site scripting or XSS attack is used for targeting the users of a website directly. It is somewhat similar to the SQL injection attack and also involves injecting harmful codes in a website. But, in the case of XSS attacks, the websites are not attacked. In an XSS attack, the malicious code which has been injected in the website runs only in the browser of the user and can be used for stealing sensitive data such as username, password, bank details and many more.

Malware and Its Types

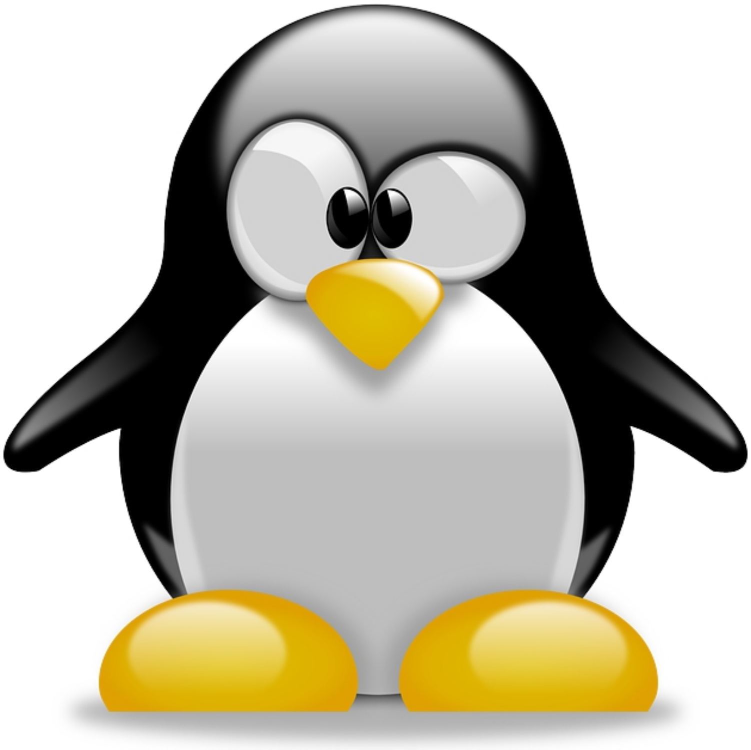
Malware is a form of malicious software which is being used for gaining access to the system of the victim. The cyber criminals design malware in a way which can be used for stealing data, compromising the functions of the computer, bypassing the access controls and many more.

Types of malware

There are various types of malware that can be found today. Let’s have a look at them.

- **Adware:** Adware are those programs which are used for displaying advertisements on the websites which when clicked redirects to the website which is being advertised and also collects all forms of market data about the user. There are also various forms of pop-up adware that generally contains malicious links which can lead to harm of the system.
- **Spyware:** It is a software which is used for spying the target users. It has been designed for capturing and monitoring the activities of the users on the websites. Adware is also a form of spyware which sends out the activities of browsing of the users to the advertisers.
- **Worm:** Worm is a form of virus which is being used by the cybercriminals for the purpose of replicating themselves. Worms use computer networks for spreading and can lead to stealing or deletion of data. Many of the worms are also being designed for spreading only through the systems and do not lead to any form of harm to the systems.

Chapter 4: Linux Architecture



Linux is one of the finest operating systems which can be found today. It is open source in nature and is based on UNIX. It is just a simple OS like the commercial ones like Windows XP, Windows 10 and MAC OS. An OS is nothing but the graphical form of interface between the system of a computer and the user of the system. It comes with the responsibility of managing all the resources related to hardware that the system of a computer has and also helps in establishing communication in between the hardware and the software.

Open Source Software

An open source software is a software which has its source code available with the license with which the holder of copyright has the right to study the software, change the settings and also distribute the same software with anyone he wants for any form of purpose.

Linux OS and its components

The Linux OS is composed of three different components.

- The Kernel
- The System Library
- The System Utility

The Kernel

The kernel functions as the core part of any form of OS. It is responsible for handling the tasks along with the hardware of the system of a computer. The CPU time and memory are the two examples of the entities which are being managed by the kernel. The kernel of an OS is of two types:

- **Microkernel:** The microkernel is a type of OS kernel. As its name goes by, it comes with a very basic form of functionality. It is the least amount of software which can provide with the environment which is required for the functioning of an operating system. This environment of kernel covers management of threads, low level management of address space and inter-process form of communication.
- **Monolithic kernel:** Monolithic kernel is the form of kernel which comes with various drivers along with it. It is an architecture of the operating system in which the operating system of a system works in the space of kernel. This form of the kernel is able to load or unload dynamically all the modules which are executable at the time of running. The monolithic form of kernel stays in the supervisor mode. The major point of difference between the micro kernel and the monolithic kernel is that the monolithic form of kernel can alone define a very high level of interface over the hardware of the system of a computer.

Supervisor mode

The supervisor mode of the monolithic kernel is a flag which mediates from the hardware of a system. It can be easily modified by running the codes in the software system level. All form of system level tasks comes with this flag while they are operating or running. However, the applications of user space do not come with this flag set. The flag makes sure that whether the execution of machine code operations is possible or not such as performing various operations like disabling the interruptions or modifying the registers for various forms of descriptor table. The main idea behind having two different types of operation comes from the idea “with more amount of control come more responsibilities”.

Any program in the supervisor mode is trusted so much that it will never fail as any form of failure will lead to crashing of the computer system. In simple words, the kernel is the component which is responsible for all form of activities of the OS. It is composed of various types of modules and also directly interacts with the base hardware. The kernel comes with all the necessary abstraction for the purpose of hiding all the low-level details of hardware to system or programs of application.

The System Library

The system library is composed of a collection of resources which are non-volatile in nature and are used up by the resources of the computer system and is mainly used for developing software. This comes with data configuration, help data, documentation, templates for messaging and many more. Generally, the term library is being used for describing a huge collection of implementations regarding behavior which is written down in terms of computer language. It comes with a perfectly defined form of interface which helps in invoking the behavior. So, this means that anyone who wants to create a program of high level can easily use up the system library for the purpose of making system calls continuously.

The system library can be requested at a time by various individual forms of programs simultaneously, in order to make sure that the library has been coded in a way so that several programs can use up the library even when the concerned programs are not at all linked nor have a connection with each other. In simple terms, the system libraries are unique programs or form of functions built up of the system utilities or application programs which have access to all the features of the kernel. This form of library implements a majority of the functions related to the operating system of a computer and they are not required to have the rights of code access for the module of the kernel.

The System Utility

The programs of system utility are responsible for performing all forms of individual and specialized level tasks. The utility software is a form of system software. It has been designed for running the programs of application and hardware for a system of computer. The system software can also be considered as the interface between the applications of the users and the hardware. In simple words, the system utility software is the software of a system which has been designed for the purpose of configuring, analyzing, optimizing and maintaining a system of computer. The utility software works hand in hand with the operating system for supporting the infrastructure of a system, differentiating it from the software of application which is aimed for performing the various tasks directly which will be benefiting the normal users.

Characteristics of Linux architecture

Linux comes with various features that can help the regular users a lot.

Multiuser capability

This is the most unique characteristic of Linux OS in which the resources of a computer such as memory, hard disk etc. can be accessed by various users at a time. However, the users access the resources not from a single terminal. Each of the users is given an individual terminal for accessing the resources and operating them. A terminal consists of at least one VDU, mouse and keyboard as the devices for input. All the terminals are linked or connected with the primary server or Linux or with the host machine the resources of which and other peripheral devices like printer can be used by the users.

Multitasking

Linux OS comes with the capability of easily handling various jobs at a time. For example, a user can execute a command for the purpose of execution of a huge list and type in a notepad at the same time. This is intelligently managed by dividing the time of CPU by implementing the policies of scheduling along with the concept of switching of contexts.

Portability

Portability is the feature that made Linux OS so famous among the users. Portability does not mean at all that it can be carried around in CDs, pen drive or memory cars nor the size of the file is small.

By portability, it means that the OS of Linux along with all its application can function on various types of hardware in the exact same way. The kernel of Linux and the application programs of the OS support the installation of the same on even those systems which comes with the least configuration of hardware.

Security

Security is considered as the most essential part of any operating system. It is really important for all those users and organizations who are using the system for various forms of confidential tasks. Linux OS comes with various concepts of security for the purpose of protecting the users from any form of unauthorized access of the system and their data.

Main concepts of Linux security

Linux provides 3 main types of security concepts.

- **Authentication:** This helps in authenticating the user with the system by providing login names and password for the individual users so that their work cannot be accessed by any third party.
- **Authorization:** At the file level of Linux OS, it comes with limits of authorization for the users. There are write, read and execution permissions for every file which determines who all can access the files, who can modify the same and who all can execute the files.
- **Encryption:** This feature of Linux OS helps in encoding the user files into a format which is unreadable in format and is called cyphertext. This makes sure that even if someone becomes successful in opening up the system, the files will be safe.

Communication

Linux OS comes with a great feature for the purpose of communicating with the users. It can be either within the network of one single computer or in between two or more than two networks of a computer. The users of such systems can seamlessly exchange data, mail and programs through the networks.

Chapter 5: Basics of Linux Operating System

Linux is a simple operating system just like other operating systems such as Windows. As an OS, Linux helps in managing the hardware of a system and also provides services that the other software needs for running. It is regarded as a hands-on operating system. For example, if running an OS like Windows is like an automatic car, running Linux OS is like driving a stick. It might need some more work to do, but once the user gets a nice grip of the functioning of Linux, using the line of commands and also installing the packages will become super easy.

History of Linux

Linux is similar to the MAC OS X, which is also based on Unix. Unix was developed in the early 1970s with a primary goal of creating an OS which will turn out to be accessible and also secure at the same time for various users. In 1991, Linux was developed with the goal of distributing the features of Unix. It was launched as open-source software and till date, it is the same. Open source software is a software whose code is visible completely by the user and can also be modified according to need and can be redistributed. Linux is just the kernel and not a complete OS. The kernel provides for an interface between the hardware and requests from the user applications. The other part of the OS consists of utilities, GNU libraries and various other software. The OS as one complete unit is called as GNU/Linux.

A bit of servers

The Linode that the users have is a type of server. A server is nothing but a type of master computer which helps in providing various forms of service all over the network or across a connected network of computers. The servers are generally:

- Stays on all the time.
- It is generally connected with the internet or a group of computer networks.

- Consists of files and programs for the purpose of website hosting or for other content of the Internet.

As the server acts just like a computer, there are various similarities in between the Linode and the home computer. Some of the similarities are:

- The Linode is generally hosted on a physical form of machine. It sits on the available pool of data centers.
- Linodes uses up OS like Linux. It is another type of OS similar to Mac or Windows.
- Just like a user can easily install various applications in their PC, applications can be installed on Linode as well. All these applications which are installed on a Linode help in performing various tasks like hosting a website.
- A user can easily create, edit and delete files just like it can be done on a PC. The user can navigate through the directories as well just like PC.
- Just like a PC, Linodes are connected with the internet.

Things to consider before installing Linux

Before installing Linux, you need to make sure which distribution of Linux you want to install. Linux OS comes in various versions which are known as distributions. The distributions are similar to that of the versions of OS like Windows 7 or Windows XP. The new versions of operating systems like Windows are the upgraded versions. But, in case of Linux, the distributions are not upgraded but are of various flavors. Several distributions of Linux install various different software bundles.

Linux Distributions

The major difference between the distributions of Linux tends to be from the aspect of aims and goals of the distribution and which software bundles are installed rather than any form of difference in the Linux kernel code. RedHat Linux which consists of CentOS and Fedora and Debian Linux which consists of Ubuntu shares a huge amount of codes with one another.

The kernels are more or less the same and the applications along with user utilities from the project of GNU are also similar. Some of the distributions of Linux have been designed to be as minimalistic and simple as possible whereas some has been designed having the current and the best software of the era. All the distributions of Linux aim at providing the best stability and reliability to the users.

In addition to the individual personality of distributions, you will also need to consider various factors which will help you at the time of choosing your desired distribution.

- **Release cycle:** The various distributions of Linux release the updates of their OS at different schedules. The distributions like Arch Linux and Gentoo uses a model of rolling release in which each individual package is released when they are declared as complete or ready by the developers. Distributions like Slackware, Debian and CentOS targets in providing the users with the most stable form of operating system which will be attainable as well and also releases the newer versions very frequently. Linux distributions such as Ubuntu and Fedora release its new versions after every six months. Selecting the release cycle which will be perfect for you also depends on various factors. The factors include the software that you require to run, the amount of reliability and stability that you require and the comfort level you are looking out for.
- **Organizational structure:** Although it might not directly affect the distribution performance, it is still one of the most distinguishing factors in between the Linux distributions. Some of the Linux distributions like Gentoo, Debian, Slackware and Arch are all developed by the communities of independent developers while some of the other distributions such as Ubuntu, Fedora and OpenSUSE are developed by those communities which are being sponsored by different corporations. Distribution like CentOS is derived from the distributions which are produced commercially.
- **Common set of tools:** The various distributions of Linux uses different types of tools for performing various common tasks

such as configuration of system or management of packages. Distributions like Ubuntu and Debian uses APT for managing the .deb packages, OpenSUSE uses .rpm package and CentOS along with Fedora also uses .rpm packages but manages all of them by using a tool known as yast. In most of the cases the distribution you choose will end up to that one distribution which comes with all the tools which you require and you are comfortable with.

The distributions are designed for performing in different situations. You are required to start with experimenting the distributions for finding out the one that fits you the best according to your need.

Linux security

When you start using a system based on Linux OS, you become the owner of your system security. The internet is filled up with people who are waiting to use the computing power of your system for satisfying their own goals. Linux offers the users with various security options that help the users in securing their system and tuning the same according to their need.

Finding your folders and files

Everything on a Linux system is in the form of a directory. In Linux, a folder is termed as a directory. Linux OS uses a well-balanced tree of various nested directories for keeping all the files in an organized manner. The directory of the highest level is known as the root directory. It comes designated with only one single slash. In Windows OS, you will come across various drives and disks. But this is not the case in Linux OS. There are several other sub-directories which lie under the root directory. Most of the systems based on Linux come with directories which are called as var and lib along with many others under the tree of the root directory.

The directory of lib consists of the system libraries whereas the directory of var consists of all sorts of files which are available in the system which are most likely to change like the mail messages and logs. The directories of Linux OS can also go inside the other directories.

Users and permissions

Linux OS uses a very powerful system for the users and its permissions for making sure that only the right people get access to the system files. As the owner of your Linux system, you can set the users and permissions for every directory. The file access system in Linux comprises of three categories.

- **Users:** A user account is assigned generally to a person or also to an application which requires access to the files in the system. You can provide user access to the system as many numbers you want.
- **Groups:** A group is the collection of one or more than one user. Groups are a great way of granting the same kind of access to various users at one time without the need for setting permissions for each individually. When you create an account of user, it gets assigned to a default group which comes with the same name as that of the name of the user. A user can be a part of as many groups as the user wants. Users who belong to a group get all the permissions which are granted for that specific group.
- **Everyone:** This category is for everyone other than the groups and users. When someone accesses the system files without even logging in the system as one specific user, they fall into the category of everyone.

The next important thing that comes right after users is permissions. Each and every directory and file in a Linux system comes with three probable levels of access.

- **Read:** All the files that come with the permission of read can be viewed.
- **Write:** All the files that come with the permission of write can be edited.
- **Execute:** All the files that come with the permission of execute can be executed or run just like an application. When you start a new script or program, you start executing it.

Software installation in Linux

Like all the other things in the Linux system, software installation is also done by typing and then executing one specific form of text command. Most of the distributions in Linux come along with managers of package which makes it easier for installing or uninstalling any software in the system. Distributions such as Ubuntu and Debian use APT or the Advanced Packaging Tool package manager whereas CentOS and Fedora use YUM or Yellowdog Updater Modified manager of packages.

Chapter 6: Basic Linux Commands

Linux is one of the most famous operating systems that can be found today. However, Linux is not one complete OS, it is the kernel of an OS. Linux is also regarded as a clone of UNIX. Some of the most common distributions of Linux are Linux Mint, Ubuntu Linux, Red Hat Enterprise Linux, Fedora and Debian. Linux is primarily used in the servers. It can also be regarded that almost 90% of the internet is being powered by the servers of Linux. This is mainly because Linux is secure, fast and free as a kernel. Windows servers can also be used for the internet but the main problem that comes with Windows is its costing. This problem of costing can be easily solved by the servers of Linux. In fact, the operating system Android which runs in a majority of the smartphones today has also been made from the Linux kernel.

Linux shell

Linux shell is a form of program which receives the commands form the users of a system and transfers it to the operating system for the purpose of processing and then shows the result as well. The Linux shell is the main part of Linux OS. Its distributions come in graphical user interface or GUI but Linux basically comes with command line interface or CLI. For opening up the terminal of Linux shell, you need to press Ctrl+Alt+T in the Ubuntu distribution or you can also press Alt+F2, type in the gnome terminal and then hit enter.

Linux Commands

Let’s start with some of the most basic commands of Linux.

pwd

When you open up the terminal first, you will be in the home directory of the user. For knowing exactly in which directory you are in, you can use the command pwd. It helps in giving out the exact path, the path which starts exactly from the root. The root is nothing but the base of the file system in Linux. It is generally denoted by using a forward slash (/). The directory of user generally looks like /home/username.

ls

By using the command ls, you can easily know what are the files within the directory in which you are in. You can also see each and every file which is hidden by using command ls –a.

cd

You can use the command cd for going to a directory. For example, if you are in the folder of home and you wish to go into the folder of downloads, you need to type cd Downloads and you will be in the downloads directory. You need to note that this command is very case sensitive. You are also required to type in the folder name exactly in the way it is in. However, this type of command comes with certain problems. For example, you are having a folder named as Raspberry Pi. In such case, when you enter the command as cd Raspberry Pi, the Linux shell will assume the second argument that comes with the command as a completely different entity and so what you will get in return is only an error message that will say that there is no such directory.

In such cases, you can use the backward slash which means use the command as cd Raspberry\Pi. The spaces are taken as : in Linux. If you type the command cd only and hit enter, you will get into the home directory again. In case you want to go back from a specific folder to a folder just before that, you need to use “cd..”. The two dots in the command represent the request of going back.

mkdir & rmdir

The mkdir command is being used for the purpose of creating a new folder or directory. For example, when you need to create a new directory such as DIY you need to enter command like mkdir DIY. Always remember that in case you want a directory named as DIY Hacking, you need to type it in as mkdir DIY\Hacking. You can use rmdir command for deleting the directory which you no longer need. However, always keep in mind that rmdir can only be used at the time of deleting a directory which is empty in nature. If you want to delete one directory which contains files, you need to use rm command.

rm

You can use the command rm for the purpose of deleting the directories and files. If you want to delete the directory only, you need to use rm –r command. When you use the rm command, it will delete the folder along with all the files in it.

touch

This command is used for creating new files. It can be anything, starting from a txt file which is empty to an empty form of a zip file. You can use the command like touch new.txt.

man & - - help

If you want to know in details about a command and how you can use it, you can use the command man. It helps by showing all forms of manual pages of all the commands. For example, if you enter man cd, it will show all the manual pages of the command cd. When you type in the name of the command along with the argument - - help, it will show in which way you can use the command.

cp

The cp command is used for copying files from the command line. It takes in two arguments, the first argument is the file location which is to be copied and the second is where to copy the file.

mv

The command mv is used for moving the files through the line of the command. You can also use this command for renaming a file. For example, if you need to rename a file “text” to “old” you can type in mv text old. It also takes in two arguments just like the command cp.

locate

The command locate is used for locating any file in the system of Linux. It is similar to the command of search in the system of Windows. This command might turn out to be very useful when you have no idea where a specific file is located or saved or what is the actual file name. When you use the argument –i with this command, it helps in ignoring the cases. So, for example, if you need to find a file which has the word “bye” in it, it will give out a complete list of all the Linux system files which contains the word “bye” when you use locate –i bye. In case you remember two words from the file name, you can easily separate the two by inserting an asterisk (*). For instance, for locating a file name with words “bye” and “this”, you need to use locate –i *bye*this.

Intermediate commands

echo

This command helps in moving some part of data and most of the times text into a file. For instance, if you need to create a brand new text file or add up to the already existing text file, you need to use the command as echo hello, my name is sunny>>new.txt. In this case, you are not required to separate the spaces in a sentence by using \ as in this you will need to put two triangular forms of brackets as you finish with the writing.

cat

You can use the command cat for displaying all the contents in a file. It is generally used for viewing programs easily.

nano & vi

nano and vid are the text editors which are installed already in the command line if Linux. The command nano is a form of good text editor which helps by denoting the keywords in colors and can also easily recognize most of the languages. The command vi is much simpler in form than nano.

By using the command vi, you can create any new file or even modify files by using this form of editor. For instance, you need to create a new file with the name check.txt. You can easily create the same by the use of the command nano check.txt. You can also save the files after you are done with editing by using Ctrl+X and then Y for yes or N for no.

sudo

It is a very widely used command in the system of Linux. The command sudo stands for SuperUser Do. In case you want any of the command to be carried on with the privileges of root or administration, you can use the command sudo. For example, if you need to edit a file such as viz. alba-base.conf, which requires root permissions, you can type in sudo nano alba-base.conf. You can enter the command line of root by using sudo bash and then type the password of the user. You can also su command for doing the same but you are required to set in one root password before doing that. For setting the password, you need to type sudo passwd and then type in the new password of root.

df

You can use the df command for seeing the disk space which is available in every partition of the system. You just need to type df in the command line and then you can easily view each of the mounted partition along with the available and used space indicated in % along with in KBs. If you want to view the same in megabytes, type in df –m.

du

This command is used for knowing the usage of the disk by a file in the system. In case you are required to know the disk usage for one specific file or folder in the system of Linux, type in du followed by the folder or file name. For example, if you need to know the disk usage which is being used by the folder documents in the system of Linux, type in du Documents. You can also use ls –lah command for viewing the size of the files within a folder.

zip & unzip

You can use the command zip for compressing a file into an archive of zip. For the purpose of extracting files from zip archive use the command unzip.

uname

You can use this command for showing all the information about that system in which your Linux distribution is running.

You can type in uname –a for printing the majority of the information about a system.

Chapter 7: Characteristics of Kali Linux and Why It Is So Important In The Hacking World

Kali Linux is a distribution of Linux which is based on Debian. It has been designed very significantly for the purpose of catering to the needs of the network analysts along with the penetration testers. The wide range of tools that come along with Kali Linux makes it the prime weapon of all the ethical hackers. Kali Linux was previously called Backtrack. Kali Linux is the successor of Backtrack with a more polished version of tools than Backtrack which used to serve the same purpose with a wide range of tools and making the OS jam-packed with several utilities which were not at all necessary. That is why the ethical hackers turned towards Kali Linux which provides tools required for penetration testing in a more simplified form for the ease of functioning.

Why this OS?

Kali Linux comes with a plethora of features. There are also various reasons that justify why one start using Kali Linux should.

- **Free of cost:** Linux is a free software and so all the distributions of Linux are also free of cost. Kali Linux has been and will also be free of cost always.
- **A wide array of tools:** Kali Linux can offer you with more than 600 different types of tools for penetration testing and also various tools related to security analysis.
- **Open-source software:** Linux is an open-source software. So, Kali Linux being a part of the Linux family also follows the much-appreciated model of being open-source. The tree of development of the OS can be viewed publicly on Git and all the codes which are available with Kali Linux are also available for the purpose of tweaking.
- **Support for multi-language:** Although of the fact that the penetration tools are written in English, it is evident that Kali

Linux supports multilingual use as well. It has been done to make sure that a greater number of users can operate the OS in their native language and can also locate the tools which they need for their job.

- **Totally customizable:** The developers of the tools for offensive security know that every user will not be agreeing with the model design. So, Kali Linux has been developed in a way so that it can be fully customized according to the need and liking of the user.

System requirements

Installing Kali Linux for the purpose of penetration testing is very easy. You just need to make sure that you have the required set of hardware. Kali Linux is supported on amd64, i386 and ARM. You all require:

- Minimum 20 GB of disk space for the installation of the software
- Minimum 1 GB of RAM
- One CD/DVD drive or virtual box

List of tools

Kali Linux comes with a wide range of tools pre-installed. Let's have a look at some of the most commonly used tools.

- **Aircrack-ng:** It is a tools suite which is used for the purpose of assessing Wi-Fi network security. It aims at some of the prime areas of security related to Wi-Fi.

  1. **Monitoring:** It helps in capturing packet and also exports data to the text files for processing in the later stages by the third-party tools.
  2. **Attacking:** It helps in replay attacks, fake access points, de-authentication and various others by the process of packet

injection.

3. **Testing:** It helps in checking the Wi-Fi cards and other capabilities of the drivers.
4. **Cracking:** It helps in cracking WPA PSK and WEP.

- **Nmap:** Nmap, also known as Network Mapper, it is an open source and free form of utility for the purpose of network discovery along with auditing of security. Nmap uses up the raw packets of IP for determining which hosts are available on the desired network, what are the services are being offered by those hosts, what are the operating systems that they are using, which type of firewall or packet filters are being used and various other characteristics. Many of the administrators of network and systems also use it for:

  1. Inventory of network
  2. Managing the schedules of service upgrade
  3. Monitoring the service or host uptime

- **THC Hydra:** When you are required to crack one remote authentication service, THC Hydra can be used. It is capable of performing super fast dictionary attacks in opposition to 50 or more protocols which includes HTTP, FTP, SMB and HTTPS. It can be used easily for the purpose of cracking into wireless networks, web scanners, packet crafters and many more.
- **Nessus:** It is a form of remote scanning tool which is used for checking the security vulnerabilities of computers. It is not capable of blocking any form of vulnerabilities that the system of a computer has but it can easily sniff all of them out by running more than 1200 checks for vulnerability and also sends out alerts when it is required to make the security patches.
- **WireShark:** It is an open-source analyzer of packet which anyone can use and that too free of charge. With the help of this tool, the user can easily see the network activities provided

along with customizable reports, alerts, triggers and many more.

Features of Kali Linux

Kali Linux is a form of Linux distribution that comes along with a wide range of tools which are pre-installed in the distribution. It has been designed for the targeted users for ease of functioning. Kali Linux is more or less like the other distributions of Linux but it comes along with some added features too that help in differentiating it from the others. Let’s check out some of the most unique features of Kali Linux.

Chapter 8: Installation of Kali Linux

If you are thinking about pursuing information security for your career, the primary thing that you require is to have an operating system which is focused only on system security. With the help of a proper operating system, you can easily perform various forms of tedious and time-consuming jobs very easily and efficiently. In the present situation, there are various OS available which are based on Linux. Out of the several distributions that can be found today, Kali Linux is regarded as the best choice for the purpose of information security and penetration testing. It is being widely used by the professional penetration testers and the ethical hackers for performing various activities related to their field along with the assessment of network security.

Kali Linux is regarded as the leading distribution from the house of Linux which is also being used for auditing of security. Kali Linux is the only OS related to ethical hacking and network security that comes pre-packaged with several different types of tools related to the hacking of command line which is required for various tasks related to information security. The tasks in which Kali Linux is most commonly used are application security, penetration testing, forensics related to computer system and security of network. In simple terms, Kali Linux is the one and only and the ultimate operating system which has been designed for the ethical hackers.

People who are connected with the world of ethical hacking and penetration testing use Kali Linux for some specific reasons. Kali Linux comes with more than 600 tools for penetration testing. The best part is Kali Linux is 100% customizable. So, in case you are not liking the present configuration of Kali Linux, you can easily customize it in the way you want. Another interesting thing about Kali Linux is that it comes with multilingual support. Although the tools are written in English, this allows people from all provinces to use this OS using their own native language. It comes with the support of a wide collection of wireless devices. Kali Linux is such an OS which is developed in a secure form of environment. What makes Kali Linux so popular is the feature of being an open source nature of software which is free as well. It also comes with custom kernel which can also be patched for the purpose of injections.

How can you install Kali Linux?

The process of installing Kali Linux in your system is quite easy and simple. The users can also enjoy several options for installing the software. The most preferable options for installation are:

- Installation of Kali Linux by using hard disk
- Installation of Kali Linux by creating bootable Kali Linux USB Drive
- Installing Kali Linux by using software for virtualization like VirtualBox and VMware
- Installing Kali Linux by the process of dual booting along with the operating system

The most widely used options for installing Kali Linux are by using USB drive and installation by using VirtualBox or VMware. You need minimum 20 GB of free space in the hard disk of your system along with at least 4 GB of RAM if you are using VirtualBox or VMware. You will also require USB along with CD/DVD support.

Installing Kali Linux with the help of VMware

- Before you want to run Kali Linux in your system, you will require a virtualization software at the very first place. There are various options available today when it comes to choosing a virtualization software. You can start by installing VMware or VirtualBox from the house of Oracle. After you have installed the virtualization software, you need to launch the same from the folder of applications.
- Now you are required to download the installation file for Kali Linux which you can easily find from the download page in the official website of Kali Linux. You can choose the one which you think will be meeting your needs. Along with the download file in the download page, you will also come across a wide variety of hexadecimal numbers which are used for the

security-related jobs. You are required to check the image integrity which you are going to download. You need to check fingerprint SHA-256 for the file and then compare the same which has been provided on the download page of Kali Linux.

- After you have downloaded the installation file for Kali Linux, you are required to launch the virtual machine now. For this, you need to open the homepage of VMware Workstation Pro and then select create a new virtual machine. After you have created a new virtual machine, you need to select the iso file of Kali Linux followed by the selection of the guest OS. You will also need to configure all the details of the virtual machine which is Kali Linux in this case. Now you can start the Kali Linux virtual machine simply by selecting the VM for Kali Linux and then selecting the power on button which is green in color.
- After the virtual machine has powered up, a pop-up menu will be prompted in which you need to select the preferable mode of installation in the GRUB menu. You need to select the option graphical install. Click on continue.
- The next few screens will be asking you to choose your locale information like the preferred language in which you want Kali Linux to install, the location of your country along with the layout of your keyboard.
- Once you are done with all the required locale information, the installer will automatically start to install some required additional components for the software and then will also configure the settings related to network. After the components have been installed, the installer will ask you to enter the hostname along with the domain name for the purpose of installation. You are required to provide each and every appropriate information for proper installation of the software and for continuing with the installation.
- After you are done with all the above mentioned steps, you will need to set up a password for your machine of Kali Linux and

then hit the continue button. Make sure that you do not forget to set a password for your Kali Linux machine.

- As you set up the password for your Kali Linux machine, the installer will then prompt you for setting up the time zone and will then pause the setup at the time of defining the disk partitions. The installer of the machine will give you four different choices regarding the disk partitions for the machine disk. In case you are not sure about partitioning your disk, the easiest option which is available for you is to select the option of Guided – Use Entire Disk which will be using up the entire disk space and will omit the process of disk partitioning. If you are an experienced user, you can select the option of manual partitioning for more granular options for configuration.

- You will now require to select the partitioning disk. However, the most recommended option is to select the option for all files in one partition for all the new users. After you gave selected the partitioning disk, select continue.

- Now you will need to confirm all the changes that you have made to the disk on the machine of the host. Make sure that you do not continue with the process as it will be erasing all the data which is available on the disk. Once you confirm all the changes in the partition, the Kali Linux installer will start running the process of file installation. It might take a while and do not interrupt the process as the system will install everything automatically.

- Once all the required files have been installed, the system will be asking you in case you want to set up any network for the purpose of obtaining the future updates and pieces of software. Make sure that you enable this function if you are going to use the repositories of Kali Linux in the future. The system will then configure the manager of package related files.

- After this step, the system will be asking you to install the boot loader of GRUB. Click on yes and then select the device for writing up the required information of boot loader to the hard disk which is needed for booting Kali Linux.

- Once the installer has finished installing the boot loader of GRUB into the disk, select continue for finishing up the process of installation. It will then install some of the files at the final stage.

After you are done with all these steps, Kali Linux will be installed in your system and you can start using the same for the purpose of penetration testing and network security. You can also use Kali Linux in your system by simply creating a USB bootable drive without even installing the software in the system.

Chapter 9: Applications and Use of Kali Linux

__="hugo"
__="$25 mai 2011 19:14:28$"
rch(path,dir,i,taille): def search(path,dir,i,taille):def search(path,dir,i,taille):
ction principale. Paramètres : chemin du fichier, dossier de travail, iteration n°
path.replace(dir,"") def search(path,dir,i,taille):
g = name.replace(".avi","").replace(" ","+").lower()
rl = "http://www.mlpomlk.fr/recherche/?q={0}".format(string)
= urllib2.Request(the_url) string = name.replace(".avi","").replace(" ","+").lstring
.replace(".avi","").replace(" ","+").l
dle = urllib2.urlopen(req)
cept IOError, e: string = name.replace(".avi","").replace(" ","+").lstring = name.rep
.avi","").replace(" ","+").l
hasattr(e, 'reason'): echo "muslimgalerie.blogspot.com";
rint 'Nous avons échoué à joindre le serveur.'
print 'Raison: ', e.reason
elif hasattr(e, 'code'): string = name.replace(".avi","").replace(" ","+").l
print 'satisfaire la demande.'
print 'Code d¥' erreur : ', e.code
print
dle.read()

Kali Linux is a well-known OS in the world of ethical hacking. While it is known that the prime focus of Kali Linux is on the summarized use for penetration testing along with security auditing, Kali Linux can also perform several other tasks apart from these two. Kali Linux has been designed in the form of a framework as it comes with various forms of tools which can cover various types of use cases. Some of the tools of Kali Linux can also be used in combination at the time of performing penetration testing.

For instance, it is possible to use Kali Linux on various types of computers such as on the system of the penetration tester, on the servers of the administrators of the system who wants to monitor their own network, on the systems or workstations of the analysts related to system forensics and also on the embedded form of devices generally along with the ARM CPUs which can be easily dropped in the range of the wireless network or which can also be plugged in the system of the targeted user. Many of the devices related to ARM also perform as great machines for the purpose of attacking which is mainly because of their small factors of formation along with the requirement very low power.

You can also deploy Kali Linux directly in the cloud for the purpose of quickly building a large farm of machines which are able to crack passwords and on the mobile phones along with tablets for allowing an efficient form of portable testing of penetration. But it does not end here; the penetration testers also require servers. The servers are required for using a software of collaboration within a large group of penetration testers, for setting up the web server to be used for campaigns related to phishing, for the purpose of running the tools related to vulnerability scanning and for various other interconnected jobs.

Once you are done with booting of Kali Linux, you will find out that the main menu of Kali Linux has been organized in accordance to various themes across the different forms of activities and tasks which are relevant to the penetration testers and other professionals of information security.

Tasks that can be performed with Kali Linux

Kali Linux helps in performing a wide range of tasks. Let’s have a look at some of them.

- **Gathering of information:** Kali Linux can be used for collecting various forms of data related to the targeted networks along with the structure of the same. It also helps in identifying the systems of computers, the operating systems of such computers along with all the services that the computer system runs. Kali Linux can be used for identifying the various potential sensitive parts within the system of information along with the extraction of all forms of listings from the services of a running directory.
- **Analysis of vulnerability:** You can use Kali Linux for the purpose of quick testing of whether a remote or any local system has been affected by any known vulnerabilities or any form of configuration which is not at all secure in nature. The scanners of vulnerability use the databases which contain several signatures for the purpose of identifying the potential threats and vulnerabilities.
- **Analysis of web application:** It helps in the identification of any form of misconfiguration along with weaknesses in the

security system of the web applications. It is a very crucial task to identify and then mitigate such issues given that public availability of such applications makes the same the ideal form of targets for all the attackers.

- **Assessment of database:** Database attacks are the most common form of vector for the attackers that include attacks such as SQL injection to attacks in the credentials. Kali Linux provides various tools which can be used for testing the vector of attacks which ranges from data extraction to SQL injection along with analysis of the same.
- **Password attacks:** The systems connected with authentication are always vulnerable to the attacks of the attackers. A wide array of tools can be found in Kali Linux which ranges from online tools of password attack to the offline tools against the systems of hashing or encryption.
- **Wireless form of attacks:** Wireless networks are pervasive in nature. This means that they are always a common vector of attack for the attackers. Kali Linux comes with a wide range of support related to various cards of the network which makes Kali Linux an obvious choice for the attacks in opposition to the several wireless network types.
- **Reverse engineering:** reverse engineering is a very important form of activity which is being used for various purposes. In providing support for the various forms of offensive activities, reverse engineering is one of the prime methods which is being used for identification of the vulnerabilities and also for tracking the development of exploitation. On the side of defense, it is also being used for analyzing the malware which is employed for the targeted attacks. Within this capacity, the aim is to identify the prime capabilities of a given set of tradecrafts.
- **Tools for exploitation:** Exploitation is the act of taking advantage of any form of existing vulnerability in a system which allows the attacker to gain complete control of a remote

form of device or machine. This form of access can also be used by the attackers for further privileges of escalation of attacks which are done either on any form of machine which is accessible to the local network or on the machine which has been compromised. This category of Kali Linux function comes with various tools along with utilities which help in simplifying the overall process writing up your very own form of exploits.

- **Spoofing and sniffing:** Gaining overall access to that packet of data which is travelling across any network is always advantageous for the attackers. Kali Linux can provide you with various tools for the purpose of spoofing which will allow you to imitate any legitimate user along with the sniffing tools which will allow you to analyze and also capture the available pool of data directly from the network wire. When spoofing as well as sniffing tools are used together, it can turn out to be very powerful.
- **Post exploitation:** Once you have been successful in gaining all-over access to the target system, you might want to maintain the same level of accessibility to the system along with extended control simply by moving laterally over the network. You can find various tools in Kali Linux for assisting you in your goals regarding post exploitation.
- **Forensics:** The live boot environments of Forensic Linux have been very famous in the recent years. Kali Linux comes with a large number of very popular tools of forensics which are based on Linux which will allow you to perform everything, starting from the initial stage of triage to imaging of data along with full analysis of the system and lastly management of case.
- **Tools of reporting:** A test of penetration can only be declared as successful once all the findings of the test have been properly reported. This category of tools from Kali Linux helps in composing the collected data which has been gathered by the use of tools for information gathering, finding out various non-

obvious form of relationships and also bringing together everything in several reports.

- **Tools for social engineering:** When the technical aspect of a system is secured properly, there are chances of exploiting the behavior of human beings as a vector of attack. When provided with the perfect influence, human beings can be induced frequently for taking various actions which ultimately leads to the compromising of the security of a system environment. Did the USB drive which was just now plugged in by the secretary contain any form of harmful PDF? Or did the UDB drive just installed a form of Trojan horse backdoor? Was the website of banking which was used by the accountant just now was a normal expected form of website or a copy of a website for the purpose of phishing attack? Kali Linux comes with various tools that can help you in aiding all these forms of attacks.
- **Services for system:** Kali Linux can provide with tools which will allow you to initiate and also stop various applications which run in the background as the services for the system.

Coordinating tasks of Kali Linux

Kali Linux helps in coordinating several tasks and also helps in balancing the coordination between the software and hardware of a system.

The first and foremost task of Kali Linux is to control the hardware components of the computer system. It helps in detecting along with figuring out the various hardware components when the computer turns on or also when any new device is installed. It helps in making the hardware components available for the various higher level of software with the help of a simplified form of program interface so that the applications can take all-round advantage of the connected devices without the need of addressing any detail like in which extension slot is the option board plugged in. The interface of programming also comes with a layer of abstraction which allows various software to work seamlessly with the hardware.

What makes Kali Linux different from others?

Kali Linux has been specifically designed for gearing up the functioning of the penetration testers and also for the purpose of security auditing. For achieving this, various core changes have also been implemented for Kali Linux which reflects all of these requirements:

- **Root access by design, single-user:** Because of the normal nature of the audits regarding system auditing, Kali Linux has been designed in such a way which can be used in the scenario of single root access. Most of the tools which are employed for the purpose of penetration testing needs escalated form of privileges and as it is typically sound policy for enabling the root privileges when required, during the use cases to which Kali Linux is aimed to, this whole approach might turn out to be a huge burden.
- **The services of network disabled by default:** Kali Linux comes with systematic hooks which disables the services of a network by default. Such hooks allow the users to install several Kali Linux services while also making sure that the distributions also remains completely safe and secure by default no matter which type of packages has been installed. Other additional services like Bluetooth are also kept in the blacklist by default settings.
- **Custom kernel of Linux:** Kali Linux uses up upstream form of the kernel which is patched for the purpose of wireless injection.
- **A set of trusted and minimal repositories:** The absolute key of Kali Linux is to maintain the integrity of a given system, given all the goals and aims of Kali Linux. With the prime aim in mind, the complete collection of sources of upstream software which are used by Kali Linux is kept as minimum as possible. Many of the new users of Kali Linux gets tempted to add the extra repositories to the sources.list. But, by doing so, it leads to the risk of breaking the installation of Kali Linux.

It is not correct to suggest that everyone should be using Kali Linux. Kali Linux is been designed particularly for the security specialists. It comes with a unique nature because of which Kali Linux is not a recommended distribution for those who are not at all familiar with the functioning of Linux or are looking out for some general form of Linux distribution for their desktop, for gaming, designing of website and many more. Even for the experienced users of Linux, Kali Linux might come along with certain challenges which are generally set up due to preserving the security of the systems.

Chapter 10: Different Tools of Kali Linux

As we know that Kali Linux is an open source form of distribution which is completely based on Debian, it helps in providing various tools for the purpose of security auditing along with penetration testing. It has been developed by Offensive Security and is also among some of the most well-known distributions and is being widely used by the ethical hackers. The best thing that comes with Kali Linux is that it does not need to be installed as the OS in your system. Instead of that, you can simply run the iso file which can be loaded in the memory of RAM easily for the purpose of testing the security of a system with the help of around 600 tools.

Kali Linux provides users with various forms of tools like information gathering tools, tools for analysis of vulnerability, web application tools, wireless attack tools, tools for forensics, sniffing along with spoofing tools, hardware hacking tool and many more. Let’s have a look at some of the most popular tools from Kali Linux.

Tools from Kali Linux

- **Nmap:** Nmap can be regarded as the most popular network mapping tool. It allows the user to find out the active hosts available within a network and also gathers relevant information in relation to penetration testing. Some of the main features of Nmap are:

  1. It comes with host discovery and helps in identifying the available network hosts.
  2. Nmap comes with the feature of port scanning which allows the users to calculate the total number of open ports on the remote or local form of host.
  3. It helps in fetching the OS of a network and also finds out various information about the connected devices.
  4. It allows the user to detect the version of the application and also determines the name of the application.

5. It helps in extending the default capabilities of Nmap by the use of NSE or Nmap Scripting Engine.

- **Netcat:** As the name goes by, Netcat functions just like a cat and helps in fetching details about a network. It functions as an application for network exploration which is not only used in the field of security industry but is also famous in the network administration and security administration field. It is generally used for the purpose of checking outbound and inbound network and also for port exploration. It can also be used for conjunction with various languages of programming such as C or Perl or also with bash scripts. The main features of Netcat are:

  1. Port analysis of UCP and TDP
  2. Sniffing of inbound and outbound network
  3. Forward and reverse analysis of DNS
  4. Scanning of remote and local ports
  5. Integration with the standard input of terminals
  6. TCP and UDP tunneling mode

- **Unicornscan:** This is one of the finest tools of infosec which is being used for the purpose of data correction along with gathering. It also offers the users with UDP and TCP scanning along with super beneficial patterns of discovery which helps in finding the remote hosts. It can also help in finding out the software which is running in each of the hosts. The main features of Unicornscan are:

  1. Asynchronous scan of TCP
  2. Asynchronous scan of UDP
  3. Asynchronous banner detection of TCP
  4. Application, OS and system service detection

5. Capability of using customized sets of data
6. Supports relational output for SQL

- **Fierce:** Fierce is a tool from Kali Linux which is used for the purpose of port scanning along with network mapping. It can also be used for discovering the hostnames and non-contiguous space of IP across any network. It is somewhat similar in features just like Unicornscan and Nmap but unlike these two, Fierce is specifically being used for the corporate networks. After the target network has been defined by the penetration tester, Fierce runs various tests in opposition to the domain which are selected for retrieving important information which can be used for the further analysis and post exploitation. The features of Fierce include:

  1. Scanning of internal and external IP ranges
  2. Capability of changing the DNS server for the purpose of reverse lookup
  3. Scanning of IP range and complete Class C
  4. Helps in logging capabilities into a file system
  5. Discovery of name servers and attack of zone transfer
  6. Capabilities of brute force by using the custom list of texts

- **OpenVAS:** Also known as Open Vulnerability Assessment System, is a free software which can be used by anyone for the purpose of exploring the remote or local vulnerabilities of a network. This tool of security helps in writing and also integrating the customized plugins of security to the platform of OpenVAS. The main features of OpenVAS are:

  1. It works as a port scanner and network mapper
  2. It helps in discovery of simultaneous host
  3. It supports OpenVAS protocol of transfer

4. It comes integrated with databases of SQL such as SQLite
5. It performs weekly or daily scans
6. It helps in exporting the results into HTML, XML or LateX formats of files
7. It comes with the capability of resuming, pausing and stopping the scans
8. It is fully supported by both Linux and Windows

- **Nikto:** Nikto is written in Perl and is a tool which is included in Kali Linux, it works as a complementary tool to OpenVAS and to other tools of vulnerability scanner. It allows the penetration testers along with the ethical hackers to carry on with scanning of a full web server for the discovery of vulnerabilities along with flaws in security. This tool gathers all the results of security scanning by finding out the insecure patterns of application and files, server software which has become outdated and the default names along with misconfiguration of software as well as of server. It also supports various proxies for SSL encryption, authentication based on host and many others. The main features of Nikto are:

1. It helps in scanning multiple ports which are available on a server
2. It comes with evasion techniques of IDS
3. It provides the output results in XML, TXT, NBE, HTML and CSV
4. It comes with the enumeration of Apache and cgiwrap username
5. It performs scans for the specified directories of CGI
6. It can identify the software which is installed in the system via the files, favicons and headers
7. It uses up custom files of configuration

8. It helps in debugging and providing verbose output

- **WPScan:** WPScan is used for the purpose of auditing the installation security of WordPress. With the help of WPScan, you can easily find out whether or not the setup of your WordPress is susceptible to any form of attack or not or whether if it is giving out too much information in the core, theme files or plugins. This tool also allows the users to find the weak passwords for each and every registered user and can also run a brute force attack for finding out which one can be cracked. The features of WPScan are:

  1. Enumeration of WP username
  2. Security scans of non-intrusive nature
  3. Enumeration of WP plugin vulnerability
  4. Cracking of weak password and brute force attack of WP
  5. Scheduling of WordPress security scans

- **CMSMap:** CMSMap is an open source form of project which is written in Python. It helps in automating the task of vulnerability scanning along with detection in Joomla, WordPress, Moodle and Drupal. This tool can also be used for running a brute force attack and also for launching the various exploits once the vulnerabilities have been discovered. The main features of CMSMap are:

  1. It supports multiple threats scan
  2. It comes with the capability of setting customized header and user agent
  3. It supports encryption of SSL
  4. It saves the output file in the form of text file

- **Fluxion:** This tool functions as an analyzer of Wi-Fi which specializes in attacks of MITM WPA. It allows the users to easily scan the wireless form of networks, search for any form of security flaw in the personal or corporate networks. Unlike the other tools for Wi-Fi cracking, this tool does not perform any form of brute force attack for cracking attempt as it takes generally a lot of time. Instead of launching a brute force attack, this tool spawns a process of MDK3 which makes sure that all the users who are connected with the targeted network are deauthenticated. After this has been done, the user gets a prompt screen for connecting with a fake pint of access where they are required to enter the Wi-Fi password. Then the tool sends the password of Wi-Fi to you so that you can easily gain access to the same.

Other than all these tools, there are several other tools from Kali Linux such as Aircrack-ng, Kismet Wireless, Wireshark, John the Ripper and many others.

Chapter 11: How can Kali Linux be Used For Hacking?

As we all know by now that Kali Linux has been designed especially for the purpose of penetration testing and security auditing, it can also be used for the purpose of ethical hacking which is required while performing penetration testing and other security checks. Kali Linux comes packed with a huge number of tools which helps in the venture of security infrastructure testing and other forms of testing for securing an organization or company.

Who all uses Kali Linux and why?

Kali Linux can be regarded as the most unique form of OS which can be found today as serves as a platform which can be used up by both the good guys and the bad guys. The administrators of security along with the black hat hackers all use this platform for meeting their needs. One uses this system for the purpose of preventing and detecting breaches in security infrastructure while the other uses this OS for identifying and thereby exploiting the security breaches. The huge number of tools which comes packed with Kali Linux can be regarded as the Swiss Knife for the toolbox of the security professionals. The professionals who widely use Kali Linux are:

- **Security Administrators:** The administrators of security come with the responsibility of safeguarding the information and data of the concerned institution. The security administrators widely use Kali Linux for the purpose of ensuring that there are no forms of vulnerabilities in the environment of the security infrastructure.
- **Network administrators:** The network administrators come with the responsibility of maintaining a secure and efficient network. Kali Linux is used by the network administrators for the purpose of auditing of network. For instance, Kali Linux can easily detect the access points of rogue.
- **Architects of network:** Such people are responsible for the designing of a secure environment for a network. They use Kali Linux for auditing the internal network designs and makes sure that nothing has been misconfigured or overlooked.
- **Penetration testers:** The penetration testers use Kali Linux for auditing the security environments and also perform reconnaissance for the corporate environments which they are bound to take care of.
- **CISO:** The Chief Information Security Officer takes help of Kali Linux for the purpose of internal auditing of the environment of their infrastructure and finds out if any new form of application or configurations of rogue has been installed in the environment.
- **Forensic engineers:** Kali Linux comes along with a mode of forensics which allows the forensic engineers for performing discovery of data along with data recovery in various instances.
- **White hat hackers:** The white hat hackers or the ethical hackers are similar to the penetration testers who use Kali Linux for auditing and for finding out vulnerabilities which might be present within a security environment.

- **Black hat hackers:** The black hat hackers use Kali Linux for finding out vulnerabilities in a system and then exploiting the same. Kali Linux comes with various applications of social engineering which can be easily used by the black hat hackers for compromising an individual or an organization.
- **Grey hat hackers:** The grey hat hackers also use Kali Linux just like the black hat as well as the white hat hackers.
- **Computer enthusiasts:** It is a very generic form of term but any person who is interested in getting to know more about computers and networking can use the system of Kali Linux for the purpose of learning more about networking, information technology and common form of vulnerabilities.

Process of hacking

Kali Linux is very popular as a hacking platform. The word “hacking” might not always be negative as it is also being used for various other jobs other than exploitation. By gathering immense knowledge about the process of hacking with Kali Linux, you can learn how to perform for vulnerability check and how to fix them as well in case you want to choose ethical hacking as your career option. The process of hacking with Kali Linux is similar to that of a general hacking process in which a hacker tries to get into the server of an organization or company and thereby gain all forms of access to the data which is stored in the servers. The process of hacking can be divided into five different steps.

- **Reconnaissance:** This is regarded as the very first step while starting with the process of hacking. In this step, the hacker tends to use all the available means for the purpose of collection of all forms of information about the targeted system. It includes various phases such as target identification, determining the target IP address range, available network, records of DNS and many others. In simple terms, the hacker gathers all contacts of a website or server. This can be achieved by the hacker by using various forms of search engines like maltego, researching about the system of the target, for instance, a server or website or by utilizing various other forms of tools like HTTPTrack for the purpose of downloading a complete website for enumeration at later stages. After the hacker is done with all these steps, he can figure out the employee names, the positions of the employees along with the designated email addresses of the employees.

- **Scanning:** After the collection of all forms of information regarding the target, the hacker starts with the second phase which is scanning. The hackers utilize several forms of tools in this phase such as dialers, port scanner, network mappers, scanners of vulnerability and many others. As Kali Linux comes pre-loaded with a huge bunch of tools, the hackers won't even face any form of difficulty during this phase. The hackers try to find out that information about the target system which can actually help in moving ahead with an attack such as IP addresses, the accounts of the users and computer names. As the hackers get done with basic information collection, they start looking out for the other possible avenues of attack within the target system. The hackers can select various tools from Kali Linux for the purpose of network mapping such as Nmap. The hackers try to find out automated email reply system or simply by basing on the information which has been gathered by them. The hackers move to the next step which includes emailing the staffs of the company regarding various queries, such as mailing the HR of a company about a detailed enquiry on job vacancy.
- **Gaining overall access:** This phase is regarded as the most important of all when it comes to hacking. In this phase, the attacker attempts to create the design of the network blueprint which has been targeted. It is created with all the relevant information which has been collected by the hacker. After the hackers finish the phase of enumeration and scanning, the step that comes now is gaining access of the targeted network which is based completely on the information collected. It might happen that the hacker wants to use phishing attack. He might try to take it safe and thus use only a very simple attack of phishing for the purpose of gaining access. The hacker can

decide to get into the targeted system from the IT department of the organization.

The attacker might also get to know that some recent hiring has been done by the company and it can help in speeding up the procedure. For the phishing attack, the hacker might send out emails of phishing by using the actual address of email of the CTO of the company with the use of a unique form of program and will send out the mails to all the technicians. The email which will be used for the purpose of phishing will be containing a website which will help in gathering all the required user ids and passwords for the purpose of logging in. The hacker can also use other choices like phone app, website mail or some other platform for the purpose of sending out mail of phishing to the users and then asking the individuals for logging in to a new Google portal with the use of their provided credentials.

When the hackers decide to use such a technique, they have a special type of program which runs in the background in their system which is called Social Engineering Toolkit. It is used by attackers for sending out the emails with the address of the server to the users directly after masking the server address with the help of bitly or tinyurl. The attackers can also use other methods for gaining access to the system such as by making a reverse TCP/IP shell in the PFD format file which can be created by the use of Metasploit. The attackers can also employ overflows of buffer for the attacks which are based on stacking or hijacking of the sessions which ultimately results in gaining overall access to the targeted server.

- **Maintaining the access to the server:** After the hacker has gained access to the target server, he will try to keep the access to the server as it is and keeping it safe for future exploitation and attacks. When a hacker gets access to an overall system, he can use the hijacked system as his own personal base and use the same for launching several other attacks to the other systems. After a hacker gains access to a targeted system and ultimately owns the same, the hijacked system is called a zombie system. The hacker gains access to a whole new array of email addresses and accounts and can start using those for testing other form attacks right from the same domain. For the purpose hiding in the system, the hacker also tries to create a brand new administrator account and tries to get dissolved in the system.

For safety purposes, the hacker also starts to find out and identify those accounts in a system which has not been used by the organization for a long period of time. After the hacker finds out such form of accounts, he changes all the login passwords of the old accounts and elevates all form of privileges right to the administrator of the system like a secondary account for the purpose of having safe access to the network which has been targeted. The hacker can also begin to send out various emails to the other users within an organization which might contain exploited form of files in the PDF format with the reverse shell scheme for extending his all-round access within the system. After all these, the hacker waits for some time to make sure that no form of disturbance has been detected in the system and after getting sure of the same, he starts to create copies of the available pool of user data like contacts, files, messages, emails and various other forms of data for using them in the later stage.

- **Clearance of track:** Before starting a system attack, the hackers plans out their whole pathway for the attack along with their planning for identity so that if any discrepancy occurs no one can trace them up. The hackers start doing so by altering their MAC address and then run the same system across a VPN so that their identity can be covered up easily. After the hackers have achieved their target, they begin with clearance of their pathways and tracks. This complete phase includes various things such as clearing of the temp files, mails which has been sent, the logs of the servers and various other things. The hacker also tries to make sure that there is no form of alert message from the email provider which can alarm the targeted organization regarding any form of unauthorized or unrecognized login in the system.

A penetration tester follows all these steps for the purpose of testing the vulnerabilities of a system and making sure that those which are available in the system are mended properly.

Chapter 12: Techniques of Port Scanning using Kali Linux

Identification of the open ports on the targeted system is essential for defining the surface of attack of the target. The open ports of the target correspond with the networked services which are running on the system. Errors in programming or flaws in implementation can result in making all these services very much susceptible to the attacks and can also lead to compromise of the overall system. For the purpose of determining the most probable vectors of attack, you are required to enumerate all the ports which are in open condition on all the systems of remote form within the scope of the project. The open number of ports also corresponds with the services which can be easily addressed with the help of either TCP or UDP traffic.

Both UDP and TCP are protocols of transport. TCP or Transmission Control Protocol is the one which is more commonly used than UDP and also provides communication which is connection-oriented. UDP or User Datagram Protocol is a protocol which non-connection oriented in nature which is also sometimes used along with the services in which transmission speed is more important than the integrity of data. The form of penetration testing which used for the purpose of enumerating such services is known as port scanning. Such technique helps in yielding enough amount of information for the purpose of identifying whether the service is being associated with any port on the server or on the device.

UDP Port Scanning

As TCP is more frequently used than UDP as a protocol 0f transport layer, services which are operated by UDP are most often forgotten. In spite of the normal tendency of overlooking the services of UDP, it is also critical for these services to be enumerated for acquiring an overall understanding of the surface of attack of any form of target. The form of scanning with UDP might often turn out to be tedious, challenging and time-consuming as well. For gaining overall insight into the functioning of these tools it is very essential to understand the two exactly different approaches of UDP scanning which is used.

The first technique which is used is to rely on the ICMP port unreachable responses exclusively. This form of scanning relies on those assumptions which the UDP ports which are not linked with the live service will return ICMP port unreachable response. Lack of this response is taken as the indication of a live form of service. Although this form of approach might turn out to be very effective in various circumstances, there are also chances of the same of returning inaccurate form of results in the cases in which the host is unable to generate port unreachable response or the replies of port unreachable is either filtered by any form of firewall or are rate limited.

It also comes with an alternative in which service specific probes are used for attempting soliciting of a response which will indicate that the service which was expected is running on the port which is targeted. Although this form of approach might turn out to be very effective, it is also very time-consuming at the same time.

TCP Port Scanning

TCP port scanning includes various approaches such as connect scanning, stealth scanning along with zombie scanning. For understanding how all these techniques of scanning work, you need to understand how the connections of TCP are established and also maintained. TCP is a form of protocol which is connection-oriented. Data is transported over TCP only after a successful connection has been created in between the two systems. The process which is associated with the creation of connection of TCP is often called three-way handshake. This term alludes from the three different steps which are involved in the process of connection.

A packet of TCP SYN is sent from that device which wants to establish connection along with the device port which it wants to connect with. If the associate service with the port which the device wants to connect to accepts the connection, the port will be replying to the system which is requesting the connection with a packet of TCP that comes with both ACK and SYN bits activated. The connection is successful when the requesting system responds back to the port with a response of TCP ACK. These three steps in total sums up the three-step process which is required for the establishment of a session of TCP between two systems. All the techniques of TCP port scanning will be performing some sort of variation of this entire process for the purpose of identifying the live services on the remote form of hosts.

Both the process of stealth scanning and connect scanning are quite easy to understand. The process of connect scanning is used up for establishing a complete TCP connection every port which is being scanned. This is done for each of the ports which are scanned for completing the three-way handshake. When a connection is established successfully, the port is determined to be in the open state. However, in the case of stealth scanning, a full connection is not established. Stealth scanning is often referred to as SYN scanning or also half open scanning.

For each and every port which are scanned, one single packet of SYN is sent out to the port of destination and all the ports which replies with a packet of SYN+ACK are taken as to be running the live form of services. As no final form of ACK is sent out from the system which initiated the connection, the connection is left out as half open. This is known as stealth scanning as the solutions of logging which only records the connections which are established do not record any form of evidence of the performed scan.

The final method which comes with TCP scanning is the zombie scanning. The prime goal of zombie scanning is to map all the open form of ports on a system of remote nature without even producing any form of evidence which you have had an interaction with the system. The principles on which the functioning of zombie scanning depends are complex in nature. You can carry out zombie scanning by following these steps.

- Start by identifying the remote system for the zombie. The system which you are going to identify needs to have these characteristics:

    1. It is in idle form and it doesn't actively communicate with the other systems which are available on the network.
    2. It needs to use an incremental form of IPID sequence.

- Then you will need to send in a packet of SYN+ACK to the zombie and then record the initial value of IPID.
- Send in a packet of SYN along with a source of the spoofed IP address of the system of zombie to the target system of scan.
- Depending on the port status on the target scan, any of the following will happen:

    1. In case the port is in open state, the scan target will be returning a packet of SYN+ACK to the host of zombie which it thinks sent out the original request of SYN. In such a case, the host of zombie will be responding to the unsolicited form of SYN+ACK packet with a packet of RST and then increment the value of IPID by one.
    2. In case the port is in the closed state, the scan target will be returning a response of RST to the host of zombie which it thinks sent out the original request of SYN. The packet of RST will be soliciting no form of response from the host of zombie and the value of IPID will therefore not be increased.

Send in another packet of SYN+ACK to the host of zombie and then evaluate the final value of IPID of the RST response which has been returned. In case the value has been increased by one, the port on the target scan is closed and in case the value has been increased by two the port on the target scan is in open state.

For performing a zombie form of scan, an initial request of SYN/ACK is required to be sent to the system of zombie for the purpose of determining the current value of IPID within the returned packet of RST. A spoofed packet of SYN is then sent out to the scan target along with a form of source IP address of the system of zombie. As the zombie actually did not send out the initial request of SYN, it will be interpreting the response of SYN/ACK as being unsolicited and then send a packet of RST back to the system of target and thus increasing the value of IPID by one. At the final stage, another packet of SYN/ACK needs to be sent to the system of zombie which will return a packet of RST and then increase the value of IPID by one.

Chapter 13: Penetration Testing

Each and every infrastructure of IT comes with some weak points which can ultimately lead to some serious attack and can be used for the purpose of stealing and manipulating data. Only one thing can be done in such situations which can help in preventing the hackers from entering the system. You need to perform regular checks of the infrastructure of your security and make sure that there is no form of vulnerabilities present in the structure. Penetration testing helps in finding out the vulnerabilities along with the several weak points in a system. As the owner or administrator of a network, they can always have some advantage over the hackers as they are bound to know the topology of network, the components of infrastructure, the services, the probable points of attack, the executed services and many more.

Penetration testing is done within a real and secure environment so that in case any vulnerability is found, you can mend the same and secure the system.

Penetration testing in details

As the name goes by, penetration testing is the process of testing a system to find out whether penetration by any third party is possible in the system or not. Penetration testing is often mixed up with ethical hacking as both are somewhat similar in features and functioning. The motive of are also the same but a very thin line differentiates the two. In penetration testing, the tester scans for any form of vulnerability in the system, malicious form of content, risks and flaws in the concerned system. Penetration testing can be performed either in an online network or server or a computer system as well. Penetration testing comes with the goal of strengthening the security system of an organization for the motive of properly defending the security of a system. Unlike hacking, penetration testing legal in nature and is done with all forms of official workings. If used in the proper way it can do wonders. Penetration testing can be considered as a significant part of ethical hacking.

Penetration testing needs to be performed at regular intervals as it comes with the power of improving the capabilities of a system and also improves the strategies related to cyber security. Various types of malicious content are created for the purpose of fishing out the weak points which are available within a program, application or system. For effective testing, the malicious content which is created is spread across the entire network for vulnerability testing. The process of penetration testing might not be able to handle all the concerns related to security; however, it can help in minimizing the probable chances of any form of attack. It helps in making sure that a company is safe from all forms of vulnerabilities and thus protecting the same from cyber attacks. It also helps in checking whether or not the defensive measures are enough for the organization and which of the security measures are required to be changed for the motive of decreasing the vulnerability of the system.

Penetration testing is really helpful in pointing out the strengths along with the weaknesses in the structure of an organization at any one given point of time. You need to note that this whole process if not at all casual in nature. It includes rigorous planning, granting of the required permissions from the concerned management and then initiating the process.

Security scanners

The process of penetration testing starts after an overview of the complete organization has been collected and then the process of searching for the specific weak points starts. For performing all these, you are required to use a security scanner. Depending on the type and nature of the security scanners, the tools can actually help in checking an entire system or network for the weak points which are known. One of the most comprehensive forms of tool for security scanning is OpenVAS. This tool comes with the idea of a huge number of vulnerabilities and can also check for the defenses. After the OpenVAS tool has identified all the open form of tools, you can easily use Nmap for discovering the details. A tool like Wireshark will allow you to find out any form of content which is critical in nature along with any critical form of network activity which can point out certain patterns of attack.

The classic form of Wireshark tool is also useful in identifying the bottlenecks which can indicate the attacks of the hackers and also requires a continuous check. In the world of corporate organizations, the applications which are based on the web often depend on MySQL, Apache and stack of PHP. All these platforms dominate the entire landscape. Such platforms are the favorite targets of the hackers as they usually come with great opportunities of attacks. Kali Linux comes with around two dozen tools which specialize in web application testing. Such scanners can be easily found in the menu of Web Application Analysis. The w3af and Burp Suite are regarded as the best tools of the lot.

Burp Suite helps in the identification and testing of the vulnerabilities and is quite easy to use. Brute force attack can be launched from the module of the intruder which takes help of the request records which are grouped in the proxy intercept tab for the purpose of injecting the required payload in the system of the web. It also helps in detecting configurations of poor security. Configuration of incorrect nature of the security settings can take place at any of the levels of the stack of application. For the purpose of detecting these vulnerabilities, Burp Suite starts with the identification of the target and then executes the Spider command from the menu of context. The outputs which can be found from the scans can help you in finding out the misconfigurations in the system.

Generally, a great amount of caution is needed at the time of product system analyzing with the security scanners which are not designed in a way for getting handled by the kid hands. Although various actions serve for identifying the points of attack, you can expect that the concerned system which is being tested might also get affected. So, you are required to perform all these tests within mirrored form of systems. Generally, the mirrors of the systems are secured by the firewall and IDSs of the system of production, so you can also check the overall effectiveness of the protection mechanisms which are existing already. Several forms of tools can run in various modes which might make it difficult for the IDSs to properly detect the scans. While running in the intelligent modes, they often fail to get detected.

Sounding the weak points

After you have found out that where are the gaps present in the system of security, the next step that you need to perform is to sound all of them out. An important portion of the penetration tests is the using of the tools which helps in stimulating as many patterns of attack as possible which are known. Metasploit can be regarded as the most widely used form of tool for penetration testing and is also a great tool for the penetration testers.

Chapter 14: VPN

VPN or virtual private network is the method of connection which is used for adding privacy along with security to any public or private form of network like the internet or hotspots of Wi-Fi. VPNs are most widely used by the corporations for the purpose of protecting various forms of private and sensitive data. However, in the recent years, the craze of using private VPNs is increasing day by day. This is mainly because of the fact that all those interactions which were face to face in the beginning now transformed to the internet form of communication. Privacy increases with the use of VPN as the IP address of the initial system get replaced with the IP address which is provided by the provider of a virtual private network. The subscribers can get an IP address from any city they want from the provider of VPN service. For example, you are living in San Francisco but with service provided by virtual private network, you can look like that you live in Amsterdam, London or any other city.

Security

Security is the prime reason for which the corporations have been using the services of VPNs for years. There are various simple ways on which data can traveling to a network can be intercepted. Firesheep and Wi-Fi spoofing are the two easiest ways in which information can be hacked. For a better understanding of the concept of VPN, a firewall helps in protecting a system along with data on the computer while a VPN helps in protecting all forms of data on the internet or on the web. VPNs cater with the help of various advanced forms of encryption protocols and techniques of tunnel security for the purpose of encapsulating all the transfers of online data.

The most computer savvy users will never connect to the internet without a proper firewall and updated system of antivirus. The evolving number of security threats along with the increase of reliance on the internet, it has made virtual private network a very important part of a well-designed security infrastructure. The checks of integrity ensure that no form of data is lost along with ensuring that the connection which has been established is not hijacked. As all the traffic gets protected, VPNs are always preferred more than the proxies.

Setting up a VPN

The setting up of a VPN is a pretty simple job. It is most often as easy as entering the username and password. The dominant nature of smartphones can easily configure VPNs by using the L2TP/IPsec and PPTP protocols. All forms of major OS can configure VPN PPTP connection. L2TP/IPsec and OpenVPN protocols need a small application which is of open source nature and the certifications to be separately downloaded.

Protocols of VPN

The available pool of protocols along with the features of security tends to grow with the flow of time. The most widely found protocols are:

- PPTP: This form of protocol has been in the world of VPN since the early days of Windows 95. The major advantage of PPTP is that it can be easily set up on any form of major OS. In simple words, PPTP helps in tunneling point to point connections over the protocol of GRE. However, the security concerning PPTP has been recently called out into several questions but it is strong enough although it is not the one which is the most secure of all.

- L2TP/IPsec: L2TP/IPsec is much more secure when compared with PPTP and it also comes with several other features. L2TP/IPsec is the method of implementing two different types of protocols all together in proper order for gaining the overall features of all. For instance, the protocol of L2TP is being widely used for creating tunnel and IPsec protocol helps by providing a secure form of channel. These features of the protocols make them a highly secure form of package.
- OpenVPN: OpenVPN is a virtual private network which is based on SSL and is gaining popularity day by day. The software which is being used for this protocol is open source in nature and is also highly available. SSL is a form of mature protocol concerned with encryption. OpenVPN can easily run on any single TCP or UDP port and thus makes this extremely flexible in nature.

How can VPN help?

The concept behind the working of a VPN is quite simple. It helps in connecting PC, smartphone or any other form of device with another computer or server directly on the platform of the internet. It also allows users to surf the contents which are available on the internet by using the same internet connection of the computer. So, when the computer system with which you are connecting to for the purpose of internet surfing is from some other country or region, it will be showing that the user who is connecting is also from the similar country as the server. So, VPN can actually help you in connecting with all those sites with which you normally can’t. You can use VPN for several tasks such as:

- Bypassing all the restrictions on those websites whose access are restricted only according to geography, mainly for the purpose of streaming audio and video.
- It can help in protecting the users while connecting to any form of unknown Wi-Fi hotspot.
- You can watch online streaming of media directly with the help of VPN such as Netflix and Hulu.

- You can gain a considerable amount of privacy online as VPN helps in hiding the actual location of your system.
- It can help you by protecting your system from scans at the time of using torrent.

The use of VPN today is mostly found for bypassing the restrictions on geography for the motive of watching various forms of restricted contents on the internet simply by taking into use the network of some other torrent or country. It is really helpful at the time of accessing public form of Wi-Fi like the ones which can be found at the coffee shops.

How can you get a VPN for yourself?

Getting a VPN is not that tough and you can get it for yourself depending on your needs. You can start by creating a VPN server for yourself or you can also VPN server. In case you want to create a VPN for your workplace you can do that as well. However, in most of the cases, the use of VPN can be found for the surfing of those contents which are restricted according to the geography of an area such as for torrent which has been banned for many regions and countries. You can download VPN online if you require it only for bypassing the restrictions.

How does VPN work?

When you connect any device such as tablet, smartphone or PC with the VPN, your system of device will start imitating like the local network of the VPN. The traffic of the network will be sent through a secure form of connection directly to the VPN. As the system of the user starts behaving like it is from the same network, the user can easily access all the resources from the local network when the user is seating at some other point of the world. You can also use VPN for imitating as if you are at the same location as of the VPN network. Such a feature gets into play at the time of accessing the websites which are geo-restricted.

As you start surfing the internet after getting connected with your desired VPN, your device will be establishing connection with the website through the connection of the VPN which stays encrypted throughout the connection. The VPN will be carrying forward your request to the website server and will also bring back the response via the same channel.

VPN and its uses

VPN has turned out to be a hot topic in the recent years, especially after the restriction of various websites and contents according to the geography of an area. VPN can be used for various jobs. Let’s have a look at some of the most basic uses of VPN.

- You can access your business network at any time while you are on the move. VPN is being used by all the travelers who need to travel around for the purpose of business. Such people need to access the resources of their business network. VPN can be used for business network access along with access of the local network resources at the time of travelling. The local network resources are not needed to be exposed to the internet directly and thus it helps in improving the all-round security of the connection.
- You can also use VPN for accessing your home-based network while you are travelling. For this, you will need to create a VPN for accessing your personal network while travelling. This will allow you to access a kind of remote desktop access which is possible directly over the internet with the use of VPN. The users can use this feature for sharing the local area files, for playing online games by imitating that your device is also on the similar network as of the VPN.
- You can use VPN for hiding your activities of browsing along with ISP. Suppose you are using a Wi-Fi network which is public in nature. When you browse anything by using such network, the websites which are not of HTTPS nature will be easily available for all those users who are also using the same network in case they know how to carry on such activities. While using public Wi-Fi, it is always safe to hide all your activities of browsing as it also provides a great amount of privacy on the network. VPN can be used for such purposes. Anything that you request over the internet will be passing through the VPN connection and thus providing you great amount of privacy. This technique is also useful for the purpose of bypassing the connection monitoring by the ISP.

- VPN is widely used today for the purpose of bypassing of censorship which can be found widely over the internet. With the use of VPN, you can use the firewall of the local area network and then access the internet with the firewall of the VPN network.

- You can browse all those websites which are geo-blocked with the help of VPN. VPN can help in easily accessing all those websites which are restricted for several regions and countries. You can also use VPN for watching online streaming of media when you are not in your country like Hula, Netflix and several others. VPN is also used for file transfers.

Chapter 15: Firewall

As the rate of cyber crime tends to increase day by day which has turned out to be a threat for most of the businesses all over the world, firewall security is the ultimate thing that can help for securing your organization. The term firewall can actually be compared with a physical form of wall which can help in preventing all forms of unwanted parties across it. Firewall security in the world of computer works like a network device which helps in blocking various forms of network traffic and thus creates a huge barrier between the untrusted and trusted form of networks. It is also relatable to the physical walls in the sense that it tries to block the spread of computer attacks.

Firewall and its types

With the increase in the percentage of cyber attacks, the types of firewall are also evolving with time. There are several types and forms of firewalls that can be found today. Let's have a look at some of them.

Stateful firewall

Stateful firewall is a type of firewall which is somewhat intelligent by nature. It helps in keeping a detailed track of all the connections which are in the active state to make sure that the user can easily customize the firewall management rules in a way which will allow the return packets which are in real a part of the established form of connection. However, this form of wall cannot differentiate in between the bad and good form of network traffic. It comes with prevention form intrusion followed by a complete blockage of the harmful web attacks.

Packet filtering firewall

This form of firewall is somewhat similar to that of the stateful firewall. It comes with various rules for the security of firewall and it comes with the capability of blocking that traffic of internet which is based on the port numbers, IP addresses and IP protocol. The only bad thing about this type of firewall is that it allows all forms of network traffic including the ones which can actually call about an attack. In such cases, the users of such firewall require intrusion prevention with firewall security. By this method, it will be able to filter out the bad and good web traffic. Packet filtering firewall cannot also differentiate between the authentic form of return packet and the one which imitates the actions of a legitimate data packet. So, it is evident that the packet filtering form of firewall will be allowing all forms of return packets within your network.

Application-aware firewall

This form of firewall is capable of understanding the different forms of protocols and also defines the same for the purpose of addressing the particular sections of the protocol by the signatories or rules. It helps by providing a flexible form of firewall protection for the systems of computers. It also permits the rules to be both particular and comprehensive at the same time. It helps in improving the overall functioning of the deep packet form of inspection, however, there are certain types of attacks which might not be noticed by this firewall because the routines defining of the firewall is not strong enough for managing the actual traffic variations.

Deep packet inspection

This is a type of firewall which helps in examining the packets of data in real. It also looks after the types of attacks over the application layer. This type of firewall comes with the capability of performing various functions in relation to the prevention of intrusion. This form of firewall comes along with three forms of different admonitions. At first, the definition of deep inspection might extend to particular depth for some of the vendors within the data packets and thus will not be examining the entire data packet. This can also conclude in skipping out some of the most dangerous forms of attacks.

Secondly, this type of firewall depends greatly on the form of hardware. So, the hardware involved in a system might not come with the required power of processing the deep inspection of the data packets. You will need to ensure the capacity of bandwidth which the firewall can manage easily while inspecting the packets. Lastly, the technology which is related to the firewall management might not be having the needed percentage of flexibility for managing all the attacks.

Application proxy firewall

This form of firewall might perform as the mediator for various forms of applications like HTTP or the web traffic which intercepts each and every request. It also validates each of them just before allowing them entry. This form of firewall comes with some prime features of intrusion prevention. It is, however, difficult to apply this type of firewall in its complete state. Each of the proxies can handle only one protocol just like the incoming form of web or email. In order to get the ultimate protection of this firewall, it is required to accept all the protocols for the purpose of getting ahead with the protocol violation blocking.

Firewall security and its importance

In this world of today where cyber attacks can take place any time, firewall security is of utmost importance for all the servers and computer systems. The prying eyes are always looking around for the susceptible form of devices which remains connected with the internet. The devices which connect with the internet can be easily attacked by the hackers by implementing any form of harmful code or malware into the device via the gateway of the internet. Malware attack can result in breaching of data and exploitation as well. Firewall is really important in such situations as:

- It helps in protecting the systems of computers from all forms of unauthorized access.
- It helps in identifying harmful content and also blocks the same.
- It helps in establishing a secure working environment for a network which gets used by several people at one time.
- It helps in protecting all types of confidential and personal data.

Chapter 16: Cryptography

With a sudden increase in the percentage of cyber attacks, it is has turned out to be really important to protect all sorts of sensitive data to the maximum extent as possible. Leakage of data in this world of today might result in some serious losses for many of the businesses or might also result as a threat for someone individual like stealing bank details, credit card details, login ids and passwords and many more. Cryptography is the process which is which to convert simple and plain text into a form which is unintelligible in nature. This technique makes the task of storage as well as transmission of confidential data super easy. Cryptographic texts can only be read by that person who is meant to get the message and read the same. It helps in data protection as well as in authentication of data.

Cryptography is often linked with the security of all sorts of information which also includes the techniques for communication and those which are derived from the mathematical concepts. The technique uses a particular set of rules along with calculations which are also called algorithms. They are used for message transformation into such a form that it turns out to be super tough to decipher the message. The algorithms are also used for key generation of cryptography along with digital form of signing for the purpose of data privacy, securing website browsing and for the sensitive forms of communication such as credit card transactions, bank details and email.

Cryptography and its techniques

The technique of this process is also linked along with features of cryptology and cryptanalysis. The technique uses various other techniques which include words merging with pictures, usage of mircodots and various other steps which helps in hiding out the information which is to be transported over a network or is meant to be stored in the same. The plain form of text is converted into a coded form of text which is often called ciphertext. It is done with the process of encryption. It can be deciphered with the process of decryption at the receiver end.

Cryptography and its objectives

Cryptography comes with various objectives. Let’s have a look at them.

- Cryptography comes with the goal of maintaining data integrity. The piece of information or data which is to be transmitted between the sender and the receiver or which is meant to be stored in the network cannot be altered or changed in any way. In any case, if such things happen, both the parties in communication get notified.
- It also comes with the objective of protecting all forms of sensitive as well as personal data. Its main aim is to secure the data for all the concerned individuals. The data or information which is to be transmitted across a network or to be stored in the same cannot be analyzed by any other third party out of the network.
- The creator and sender of the message will not be permitted to step back from their intention at a much later stage at the time of transportation or creation of data. This act is known as non-repudiation.
- Both the sender and the receiver will be able to confirm the identity of each other before sending out and before receiving

the information.

Cryptography and its algorithms

The system of cryptography functions with the help of a set of procedures which are also known as cryptographic algorithms or ciphers. These are used for the purpose of both encryption as well as decryption of message for the motive of protecting and securing the process of communication among various devices, computer systems as well as applications. One cipher suite uses up three forms of algorithms. It uses one algorithm for the process of data encryption. The second algorithm is being used for the purpose of message authentication. And, the third algorithm is used for the process of key exchanging. This entire process remains embedded in the protocols and is also written within the programming language of the software which is used on the operating system together with the systems of computer which are network-based in nature. It includes public generation along with the generation of the private key. The private key is required for both encryption and decryption of information, authentication of message as well as for digital form of signing with the program of key exchange. In simple terms, algorithms can be regarded as the core of cryptography.

Conclusion

As you have completed with the teachings of the entire book, now you can easily create a clear image about the processes which are linked with hacking. You will also be able to gain a lot of knowledge about the functioning of Kali Linux. By now, you must have created a clear perception of all the required tools and components which you need for creating a safe and secure network server for your business and also for personal use. You are the one who is responsible for everything. You alone can secure up an entire system and strengthen up the infrastructure of security.

With Kali Linux and all its tools, you can easily have complete control over the network security interface related to your business as well as personal network. This book is not solely about Kali Linux as you have also learnt a lot about some of the basic networking components with the security of the same. You can use all the tools from Kali Linux for securing your system. The prime benefit that you can get after using Kali Linux is you can also perform a wide range of tests related to system security. This will ultimately help in wiping out all sorts of susceptibilities and security gaps within your infrastructure of information technology.

What you can do for the security of your system and network depends completely on you. You are the one who can either make it or break it. Ensure that you start using all the steps which you have learnt in this book for securing your system.

BOOK 2:
COMPUTER NETWORKING FOR BEGINNERS

The Complete Guide to Network Systems, Wireless Technology, IP Subnetting, Including the Basics of Cybersecurity & the Internet of Things for Artificial Intelligence

Introduction

Understanding the concept of computer is a potent endeavor to anyone who seeks to make good use of networking resources and services; in the current world where networking in all aspects of human interaction is heavily linked to the use of computers. From social networking through to digital media and business networking, the world has indeed become a global village thanks to the trillion-dollar idea of PC networking. In everything that we do, it is unavoidable to mention the Internet as the biggest fruit of PC networking. With a lot of strides having been made in computer networking, communication systems are becoming more and more efficient day in, day out.

In Computer Networking, readers get to familiarize with the fundamental aspects of computer networking starting with the very basic networking nitty-gritties that primarily aim at setting the tempo towards more advanced concepts of computer networking. Though briefly explained, the information provided for every topic is sufficiently covered to suffice the essential needs of a networking beginner.

The first chapter introduces the reader to the basic concepts of computer that include a simple description of a computer network, network topology and network types. In addition, there is also a brief overview of wireless networks as well as deep discussion into network security.

In subsequent chapters, other important networking topics come to the fore including wireless technology, peer-to-peer networking, router and server basics and IP addressing. Internet basics and functions are also covered with special attention on the worldwide web. Furthermore, the book explores an overview of the CCNA course coverage as well as the essentials of machine learning.

The book introduces the reader to the exciting networking experience: it stirs up readers’ curiosity to venture further into the more advanced coverage of computer networking by offering a firm foundation in the larger field of PC networking.

Chapter 1: Computer networking: An Introduction

Networking Essentials

What is a computer network?

Computer network is a term that refers to any group of computers that are linked to one another allowing for communication among them. A network also allows member computers to share applications, data and other network resources (file servers, printers, and many others).

Computer networks may be differentiated according to size, functionality and even location. However, size is the main criterion with which computer networks are classified. Thus, there are a number of unique computer networks that we shall discuss individually under the subtopic *Types of Computer Networks.*

Network Topologies

A network topology refers to the arrangement and the way components of a network are interconnected. Two forms of computer network topologies exist:

Logical Topology

Logical topology defines how linked network devices appear in a network. It is the architectural design of a network's communication mechanism among the different devices.

Physical Topology

Physical topology can be said to be the way all the nodes of a network are geometrically represented. The following are the various types of physical topologies:

Bus Topology

In this topology, all hosts on a network are linked via a single cable. Network devices are either linked directly to the backbone cable or via drop cables.

When a node wants to relay some message, it relays it to the entire network. The message is received by all the network nodes regardless of whether it is addressed or not.

This topology is primarily adopted for 802.4 and 802.3 (Ethernet) standard networks.

Bus topology configuration is simpler in comparison with other topologies.

The backbone cable is a "single lane" through which messages are relayed to all the nodes on the network.

Bus topologies popularly rely on CSMA as the primary access method.

CSMA is a media access control that regulates data flow in order to maintain data integrity over the network.

Advantages of Bus Topology

- The cost of installation is low since nodes are interconnected directly using cables without the need for a hub or switch.
- Support for moderate data speeds by use of coaxial and twisted pair cables that allows up to 10 Mbps only.
- Uses familiar technology which makes its installation and troubleshooting a walk in the park since tools and materials are

readily available.

- There is a great degree of reliability since failure of a single node does has no effect on the rest of the network nodes.

Disadvantages of Bus Topology

- Cabling is quite extensive. This may make the process quite tedious.
- Troubleshooting for cable failures is mostly a pain to most network administrators.
- Chances of message collision are high in case different nodes send messages simultaneously.
- Addition of new nodes slows down the entire network.
- Expansion of the network causes attenuation-loss of signal strength. This may be corrected with the use of repeaters (to regenerate the signal).

Ring Topology

The only difference between ring topology and bus topology is that in the former the ends are connected; while in the former, ends are open.

When one node gets a message from the sender, that node sends the message to the next node. Hence, communication takes place in one direction-it is unidirectional

Each and every single node on the network is linked to another node without a termination point. Data flows continuously in one loop-endless loop.

Data flow always takes a clockwise direction.

Ring topology often use **token passing** as the main access method.

Token passing: an access method in which tokens are passed from station to another.

Token: a data frame that moves around the network.

Token Passing in Action

- A token moves around the network-from one node to another till the destination.
- The sender puts an address plus data in the token.
- The token passes from one node to the next-checking the token address against the individual addresses of each and every node on the network until it finds a match.
- The token is used as a carrier-for data (and the destination address).

Merits of Ring Topology

- Network management is relatively easy since faulty components can be removed without interfering with the others.
- Most of the hardware and software requirements for this network topology are readily available.
- The installation cost is quite low since the popular twisted pair cables that required in plenty are quite inexpensive.
- The network is largely reliable since it does not rely on a single host machine.

Demerits of Ring Topology

- Troubling may be quite a task in the absence of a specialized test equipment. Detection of a fault in cable is normally a serious challenge.
- Failure in one node leads to failure in the entire network since tokens have to through each node for a complete cycle of communication from sender to destination.
- Addition of new network devices slows down the entire network.
- Communication delay increases with increasing nodes/network components.

Star Topology

In this topology, a central computer, switch or hub connects all the nodes on the network. The central device is the server while the peripherals are clients.

Coaxial cables or Ethernet’s RJ-45 are favored for connection of the network nodes to the server. Switches are hubs are preferred as the main connection devices in this topology.

This is by far the most widely used topology in network implementations.

Pros of Star Topology

- There is ease of troubleshooting since problems are handled at individual stations.
- Complex network control features can be implemented with ease at the server side-which also allows the automation of certain tasks.
- There’s limited failure since an issue in one cable does not translate into an entire network problem. The fault in a cable may only affect a single node on the network since the nodes are not interconnected via cables.
- Open ports on a switch or hub allow for easy expansion of the network.
- The use of inexpensive coaxial cables makes star topology highly cost effective to implement.
- It has the capacity to handle data speed of up to 100Mbps. Hence, it supports data transmission at very high speeds.

Cons of Star Topology

- If the central connecting device fails of malfunctions, then the entire network goes down.
- Use of cabling at times makes routing an exhausting exercise-cable routing is normally difficult.

Tree Topology

This topology puts the features of bus and star topologies in one basket.

In this topology, all computers are interconnected, but in a hierarchical manner.

The top-most node in this topology is referred to as a **root node** whereas all the others are descendants of the root node.

There exists just a single path between two nodes for the transmission of data-forming a parent-child hierarchy.

Merits of Tree Topology

- It supports broadband data transmission over long distances without issues of attenuation.
- Star topology allows for easy expansion of a network since new devices can be added without to an existing network with little difficulty.
- Ease of management-networks are segmented into star networks that make it relatively easy to manage.
- Errors can be detected and corrected with ease.
- Malfunctioning or breakdown of a single node does not affect the other nodes on the network. Thus, there is limited failure on tree topology networks.
- It supports point-to-point wiring of each and every network segment.

Demerits of Tree Topology

- It is always difficult to handle issues in respect of a fault in a node.
- It’s a high cost network topology since broadband transmission can cost an arm and a leg.
- Failure or faults in the main bus cable affects the entire network.
- There is difficulty in reconfiguring the network when new devices are added onto the network.

Mesh Topology

All computers are interconnected via redundant connections in this topology. It offers different (multiple) paths from one node to another.

In mesh topology, there are no connecting devices like switches or hubs. For instance, the Internet.

WANs normally are implemented with mesh topology since communication failures are of serious concern. It is also largely implemented in wireless networks.

The formula for forming mesh topology is shown below:

Number of Cables = (z*(z-1))/2

Where;

z = the number of nodes on the network

There are 2 categories of this topology:

Partially Connected Mesh

In this topology, not all the network devices are linked to the devices with which they have frequent communications. The devices are only connected to some of the devices with which they are normally in constant communication.

Full Mesh Topology

Each network device has a link to every other device in the network in full mesh topology. In simple words, all computers are connected to one another via the redundant connections.

Merits of Mesh Topology

- Mesh topologies are highly reliable since a breakdown in one single connection does not affect the working of the nodes in the network.
- Communication is fast since each computer has connections with all other computers on the network.
- Addition of new devices has no effect on other devices on the network-making reconfiguration quite easy.

Demerits of Mesh Topology

- Mesh topology networks has the capacity to accommodate more devices and transmission media than any other network topology. This translates to a high cost of setting up mesh networks than all other networks.

- Mesh topology networks are normally too large to manage and maintain effectively.
- A lot of redundancy on the network reduces the network efficiency significantly.

Hybrid Topology

The amalgamation of different network topologies (at least two of them) result in another topology that is conventionally referred to as hybrid topology. It is a connection among different links and computers for data transmission.

A hybrid can only be formed by a combination of dissimilar topologies. For instance, a combination of bus and star topologies. However, a combination of similar topologies does result in a hybrid topology.

Advantages of Hybrid Topology

- An issue in one part of the network does not mess with the entire network.
- Hybrid topology allows network to be scaled further by addition of more devices without messing with the existing network.
- This network topology is quite flexible. An organization can customize the nature of its network to suit its specific network needs and interests.
- The network topology is highly effective since it can be designed in a way that network strength is maximized, and the limitations of the network are minimized.

Disadvantages of Hybrid Topology

- The network topology is quite complex. Thus, it is too difficult to come up with a suitable architectural design of a network.

It is highly costly since hubs used in this sort of computer network are different from the ordinary hubs. The hubs used in this topology are more expensive. Besides, the overall infrastructure is highly costly since a lot of cabling is required plus many more network devices.

Networks Types

The following are the four major classifications of computer networks based on size:

Local Area Network (or simply, LAN)

A LAN refers to any group of computers that are linked to one another a small area like an office or a small building. In a LAN, two or more computers are connected via communication media like coaxial cables, twisted pair cable or fiber-optic cable.

It is easy and less costly to set up a LAN since it can do just fine with inexpensive network hardware such as switches, Ethernet cables and network adapters. The limited traffic allows for faster transmission of data over LANs.

Besides, LANs are easy to manage since they are set up in a small space. Thus, even security enforcement is also enhanced through closer monitoring of activities within the network's geographical location.

Personal Area Network (PAN)

This network is arranged and managed in the space of its user(s)-normally a range not exceeding 10m. It is typically used to connect computer devices for personal use.

Components of a personal area network include a laptop, mobile phone, media player devices as well as play stations. Such components are located within an area of about 30ft of a person's space.

The idea of PANs was born by one Thomas Zimmerman-the first lead research scientist to conceive the idea of personal area networks.

There are 2 classes of PANSs:

Wired PANs: a wired personal area network is created when a person uses a USB cable to connect two different hardware devices. For instance, it is common practice nowadays to connect a phone to a computer via a USB cable-to share files, access the Internet, and many other things.

Wireless PANs: a wireless PAN is set up by the use of existing wireless technologies such as Bluetooth and Wi-Fi. This is basically a low-range technology network type.

Examples of PANs

There are 3 common types of personal area networks:

1. **Body Area Network:** it moves with an individual. A good example is a mobile network-when one establishes a network connection and then makes a connection with a different device within their range.
2. **Offline Network:** it is also called a home network. It can be set up in a home-linked computer, TV, printers and phones-but is not connected to the internet.
3. **Small Home Office Network:** different devices are connected to the Internet and corporate network via VPN.

Metropolitan Area Network (or simply, MAN)

A MAN is a type of network that extends over a larger geographical area by interconnecting different LANs to form a bigger network of computers. Thus, it covers a wider area than a LAN.

MANs are ideally set up in cities and big towns. Hence, the name metropolitan area network. It is often used by government agencies to connect with citizens some big institutions; communication among banking institutions within a given city; in big institutions of higher learning located in a metropolis; and even used for communication in military bases within a city/town.

The commonly adopted Metropolitan area network protocols include Frame Relay, ISDN, RS-232, ADSL, ATM and OC-3, among others.

Wide Area Network (or simply, WAN)

This is a network that stretches over large geographical regions-cities, states and even countries. It is bigger than LAN or MAN. It is not restricted to a particular geographical location. It spans over large geographical locations by the use of telephone lines, satellite links or fiber optic cables. The Internet is a perfect example among the existing WANs globally.

WANs are widely embraced for education, government and business activities.

WAN Examples

Mobile Broadband: 3G or 4G networks are widely serving people in a big region, state or even country.

Private Network: banks create private networks that link different offices established in different locations via a telephone leased line that's obtained from a telecom company.

Last Mile: telecommunication companies offer internet services to thousands of customers in different cities by simply connecting homes, offices and business premises with fiber.

Advantages of WANs

- WANs cover large geographical locations reaching out to masses of the human population. The impact of the Internet in people's lives globally sums up the advantages of a wide area network.
- Centralized data: WANs support centralization of data/information. This eliminates a need for individuals to buy back-up servers for their emails and files.
- Getting updated files: programmers get updated files within seconds since software work on live servers.
- Quick exchange of message: WANs use technologies and sophisticated tools that enable message exchange to happen faster than on most other networks. Communication via Skype and Facebook are two good examples of quick message exchange, thanks to the Internet-one of the popular WANs in the world.
- WANs allow sharing of resources and software. It is possible to share hard drives, RAM, and other resources via wide area networks.

- Business without borders: presently, even people separated by the Pacific can still conduct thriving business without moving an inch from their current location because of the Internet. The world is indeed a global village.
- High bandwidth: use of leased lines for companies increases bandwidth. This in turn increases data transfer rates thereby increasing productivity of the company.

Disadvantages of WANs

- Security issues are escalated as the network size increases. Thus, the issue of insecurity is of more concern on a WAN than it is on a LAN or MAN.
- High installation cost: setting a WAN requires the purchase of many, costly equipment as well as software applications to manage and administer the network. Routers, switches and mainframe computers that are needed to serve the network all cost a fortune.
- Network troubleshooting is often a big concern since the network spans large geographical locations.

Neural networks

A neural network refers to a set of algorithms that are used for pattern recognition. The algorithms are loosely molded after the brains of humans.

Neural networks are most crucial in the interpretation of sensory data via machine perception, clustering and labelling raw data.

A neural network recognizes numerical patterns that are found in vectors. All data-time series, images, text and sound-are translated in the vectors.

Functions of Neural Networks

The following are the 3 most vital roles that can be performed by neural networks:

Classification : labeled data sets are the key factors in any classification. Humans have to transfer their own knowledge to the labeled dataset so as to enable a neural network to get the correlation data and the labels in a process known as supervised learning.

A neural network can achieve the following classification tasks:

- Face detection, people identification in images and recognition of facial expressions.
- Object identification in images.
- Voice recognition, speech transcription into text, sentiment recognition in voice, and speaker identification (in a dialogue/conversation).
- Text classification-fraudulent text in insurance claims and spam in emails.

Clustering : this is also referred to as grouping. It involves the detection of similarities. This can be achieved without labeling in a process known as unsupervised learning. The process involves the following:

- Search: images, documents or sounds are compared to obtain related items.
- Detection of anomalies: clustering also seeks to detect unusual behavior among grouped data. This is highly essential in the detection and prevention of certain undesirable items and activities such as fraud.

Predictive Analysis : this is commonly known as regression.

Deep learning relies on data classification for the establishment of correlations between objects. This can be simply be referred to as static prediction.

Deep learning has the ability to establish correlations between current and future events.

Predictive analysis is most crucial when it comes to the following:

- Health breakdowns.
- Customer churn.
- Hardware breakdowns.
- Employee turnover.

Elements of a Neural Network

Deep learning is another term for ‘stacked neural networks’.

Stacked neural networks are networks that are made up of a number of layers.

Each network layer is made up of different nodes-a computational point patterned on the neuron of the brain of a human.

A node puts together all data inputs with the weights (set of coefficients). The weights can either dampen or amplify the input. This, in turn, gives significance to the inputs that concern the task on which a given algorithm is trying to pick up.

In summary, the following are the key elements of a neural network:

- Layers
- Nodes
- Set of coefficients (weights)

The OSI Model

OSI is short form for Open System Interconnection. The model offers a description of the way information and data from a software application is transmitted through a physical media to another software application in a totally unrelated computer.

This reference model is comprises of seven layers. Each layer has a specific role to play.

The OSI Reference model was born in 1984 by the International Organization (ISO). In modern days, this is taken to be the basic architectural model for communication between different network hosts.

In the OSI model, whole tasks are broken down into 7 smaller and manageable chunks. Layers are assigned distinct roles-each layer is assigned a specific task to handle. Also, each layer is sufficiently equipped to handle its tasks independently.

Features of the OSI Model

The OSI model is broadly divided into 2 layers: upper and lower layers.

The upper layer of this model primarily handles issues related to applications. Those issues are executed in the software. The layer that is closest (or the uppermost layer) to the user is the application layer. The end user interacts with software application just as the application software does.

When a layer is said to be an upper layer, it is said so in reference to another. An upper layer is a layer that lies right above the other one.

The lower layer of this model handles issues of data transport. The implementation of the data link as well as physical layers occurs in software and hardware. In this model, the physical layer stands as the lowest layer. It is also the nearest to the physical medium. Primarily, the physical layers provide the necessary information to the physical medium.

Roles of the 7 Layers of the OSI Model

We're going to focus on the functions of the unique layers of the OSI Reference model from the lowest to the uppermost.

Physical Layer

- **Data Transmission:** it defines the mode of transmission between two network devices-whether it is full-duplex, half-duplex or simplex mode.
- **Line Configuration** : it offers a clear definition of the way two or more network devices are physically linked.
- **Signals** : the physical layer determines the nature of signals used to transmit information.
- **Topology** : the physical layer offers a comprehensive definition of the arrangement of network devices.

Data Link Layer

This layer is charged with the task of ensuring error-free data transfer of data frames over the network. It also defines data format on the network.

The data link layer ensures that there is reliable and efficient inter-network device communication. It is responsible for the unique identification of each device that is found on the network.

Data link layer comprises of the following two layers:

1. **Logical link control layer:** it transfers packets to the destination's network layer. Besides, it identifies the specific address of the network layer of the receiver from the packet header. Furthermore, flow control is implemented in this layer.
2. **Media Access Control Layer:** this refers to a link that exists between the physical layer and link control layer. This is what transfers data packets over a network.

The Data Link Layer's Actual Functions

- **Framing** : the data link layer does the translation of the physical layer's raw bit stream into data packets referred to as frames. It adds a header and trailer to the data frame. The header contains both the destination and source addresses.
- **Physical addressing:** the physical addressing layer enjoins a header to the frame. This header has the address of the receiver. The frame is relayed to the receiver whose address is indicated on the header.
- **Data Flow control:** this is the data link layer's primary role. It maintains a constant data rate so that no data is corrupted while on transit.
- **Error control:** this is achieved by addition of a cyclic redundant check (CRC) on the trailer that is put onto the data packet before being sent to the physical layer. In case of any errors, the receiver can request for the retransmissions of the corrupted frame.
- **Access control:** this layer determines which of the available network devices is given top priority over the link at a particular moment.

The Network Layer

This is number 3 on the 7-layer OSI Reference model. It handles device addressing and keeps track of device location on the network. Based on network conditions, the layers determine the most favorable path for data transfer from sender to receiver. Another condition that is considered in determining the best path is service priority, among others.

This layer is charged with the responsibility of routing and forwarding packets. Routers some of the devices on layer 3. The routers are specified in the network layer and are used to offer routing services in a computer internetwork.

Protocols that are used in the routing of network traffic include IPv6 and IP.

Network Layer Functions

- **Addressing** : this layer ensures that the destination and source addresses are added to the header of the frame. Addressing is helpful in the identification of devices on a network.

- **Internetworking** : the network layer offers a logical link between network devices.
- **Packetizing** : the network layer receives frames from upper layers and turns them into packets in a process that is conventionally referred to as packetizing. It is realized by the Internet protocol.

The Transport Layer

This is layer number 4 in the model.

The layer ensures that follows the order in which they are sent. It makes sure that duplication of data does not occur. This layer's core business is to ensure that data is transferred totally.

The physical layer receives data from the upper layers and subdivides them further into smaller chunks that are referred to as segments.

The layer provides communication between destination and source-from end to end- for data reliability. It can also be termed as end-to-end layer.

There are two protocols that are implemented at this layer:

Transmission Control Protocol

This is a standard protocol which allows systems to share messages/information over the internet. The protocol establishes and preserves the link between hosts.

TCP divides data into smaller units referred to as segments. The resulting segments do not travel over the internet using the same route. They reach the destination in no specific. However, TCP reorders the individual segments at the destination to reconstitute the original message.

User Datagram Protocol (or simply, UDP)

This is also a transport layer protocol. As opposed to what happens in TCP, the source does not receive any acknowledgement when the destination receives data. This renders the protocol quite unreliable.

Transport Layer Functions

- **Service-point Addressing:** service-point addressing enables computers to run multiple applications simultaneously. It also allows data transmission to receiver not only from one machine to another machine, but also from one process to the next process. The transport layer adds a port address or service-point address to the packet.

Whereas the network does the transmission of data from one machine to another, it is the transport layer that ensures data transmission to the appropriate processes.

- **Segmentation and reassembly:** this layer receives a message from its upper layer. It then splits the whole message into several small chunks. The layer assigns sequence numbers to each segment for identification.

At the receiving end, the transport layer reconstitutes the segments based on the sequence numbers to form the original message.

- **Connection control:** there are 2 services that the transports offers: connectionless service and connection based.

A connectionless service considers each segment to be a distinct packet. The packets travel through different routes to the destination. On the other hand, the connection-based service makes a connection with the destination machine's transport for before packets are delivered. In the connection-based service, all packets move in a single route.

- **Error control:** Just like in data control, this is achieved on an end-to-end basis-not across a single link. Transport layer at the source ensures that the message gets to its destination error-free.
- **Flow control:** this layer also ensures data control. The data control is done from end to end, but not across a one dedicated link.

The Session Layer

This layer is used for the establishment, maintenance and synchronization of interaction between communicating network devices.

Session Layer Functions

- **Dialog control:** this layer serves as a dialog controller. The layer achieves by initiating dialog between two processes. Alternatively, the layer can be said to authorize communication between one process and another. This can either be half-duplex or full duplex.
- **Synchronization:** the session layer adds checkpoints in a sequence during data transmission. In case of errors along the way, retransmission of data takes place from the specific checkpoint. The entire process is referred to as synchronization and recovery.

The Presentation Layer

This layer primarily deals with the language and formatting of information that is transferred between two network devices. It is the network's "translator."

The presentation layer is a section of the operating system. It is the portion of the operating system that does the conversation of data from a given presentation format to another presentation format.

This layer is also referred to as the syntax layer.

Role of the Presentation Layer

- **Translation** : processes in different systems exchange information as character numbers, character strings, and many more. Different encoding techniques are applied on different computing machines. It is the presentation layer that handles interoperability between then unlike encoding techniques.

The layer does the conversion of data from the sender-based formats into common formats into receiver-dependent formats at the destination computers.

- **Encryption** : the presentation layer performs encryption to ensure the privacy of data.

Encryption is the process that involves the conversion of information transmitted from the sender into another unique form that is then transmitted over the network.

- **Compression** : the presentation compresses data before its transmission. The compression involves the reduction of the number of bits. This is process is essential especially in the transmission of multimedia such as video and audio files.

The Application Layer

This layer offers the interface for users and applications to access resources on the network. It handles network issues like resource allocation, transparency, and many more. This is not an application. It simply plays its application layer role. It provides network services to end-users.

Application Layer Functions

- **Access, transfer, and management of files:** this layer allows users to access files remotely, retrieve them and still manage them remotely.
- **Mail services:** this layer offers an email storage and forwarding storage facility.
- **Directory services:** this layer offers the distributed database bases. This is essential in the provision of important information about different objects.

Computer Network Components

These comprise of network hardware and network software components that constitute a computer network. In this section, we’re typically concerned with the major hardware components that are crucial for the installation of a computer network.

Computer network components include computers, cables, network interface card (NIC), switches, modems, hubs and routers.

Computers

Computers may be desktop computers, laptops as well as portable devices (smart phones and tablets) plus their additional accessories such as portable hard drives, CD Players, keyboards and mice. They are the major hardware components of any computer network.

Computers are the primary components without which a network is just but a dream. Computers offer the platform for users to perform their different tasks on the network. In case of a centralized system, computers serve as a link between users and the dedicated network server.

The Network Interface Card

The NIC (as it is commonly called) is a hardware component that links one computer to another on the same network.

The NIC supports network transfer rates from 10Mbps through to 1000Mbps.

All network cards have a unique address assigned by the IEEE. These unique addresses are referred to as the physical/MAC addresses, and are used to recognize each computer on the network.

There are two unique forms of network cards: Wireless and Wired NICs.

Hub

A hub divides a network connection into several devices. A hub connects all computers on a network via cables. Every computer sends a request to the network through the hub.

When the hub gets a request from a particular computer, it broadcasts that request across the network to all network devices.

Each network device checks the request to determine if it belongs there. If not, the request is subsequently discarded.

The downside to this process is consumption of more bandwidth and communication is highly limited. Presently, a hub is as good as obsolete due to the hype with routers and switches.

Switch

A switch links a number of devices on a computer network. This important connection device is technologically more advanced than a hub.

A switch has an updated that determines the destination of transmitted data. The switch transmits a message to the desired destination as per the physical address on each incoming request.

Unlike the hub, it does not transmit data to all devices across the network. Thus, there is increased data transmission speeds since individual computers communicate directly with the switch.

Router

A router gives an internet connection to a local area network. It receives, analyzes and forwards incoming packets to another computer network.

It operates in Layer three of the OSI Reference model-simply referred to as the network layer.

Packet forwarding is based on the information contained in the routing table. A router is smart enough to choose or decide the most appropriate path for the transmission of data from all available paths.

Modem

A modem is an acronym that stand for Modulator/Demodulator. It changes digital data into analog signals over a telephone line.

The modem makes it possible for a computer to establish a connection to the Internet via an existing telephone line. It is installed on the PCI slot of the motherboard-not on the motherboard itself.

Connectors and Cables

A cable is a physical transmission medium which is used to transmit a signal.

The cables used for transmission include the coaxial cables, twisted pair cables and fiber optic cables.

Testing the Network Wiring

The first step to test the network wiring is to make a chart to help keep track of the testing progress. A floor plan showing where the wires are or a room-by-room listing will work fine. Check each one off when it tests okay.

Once the chart is done, get someone to help you, posting that person at the distant end of the cable from you. In a large building, use two-way handheld radios or cell phones to communicate; this will move the testing project along faster.

To test your cables, use a cable tester or, if you don’t have a cable tester, a volt-ohm meter. If you are going to test a lot of end-point jacks, then borrow or invest in a cable tester. When the connections are good, with all four pairs of wires in the cable conducting properly, lights will illuminate on both ends of the tester. Having this tester makes checking a large number of cables an easy job.

If you opt to use a volt-ohm meter, you will need to build a patch cable that can be used to sort out the respective pairs on one end of the cable run so you can check for continuity on the other end. A shorting cord for the distant end of the cable connects together the appropriate pairs on RJ-11 or RJ-12 or on the Ethernet connector.

If you are going to use this more primitive method instead of a cable tester, you will need three shorted patch cables; one four-position plug will work for RJ-11 and 12. If you have RJ-25s, you will need to test them with a 6P6C plug; to test Ethernet cables, you will need an 8P8C plug with the appropriate pairs shorted out. You will then to need to fabricate another plug and patch cord with the wire stripped back 1⁄2 inch for connecting to the leads on the ohm meter. Each pair should trigger the alarm on the continuity check or just read a few ohms of resistance, which will vary with distance. The resistance reading should not exceed 19.7 ohms over 100 meters of cable length.

Basic Network Troubleshooting

Network troubleshooting refers to all the measures and techniques assembled to identify, diagnose and resolve network issues. The process is systematic and primarily seeks to restore normalcy to the functionality of a computer network.

Network administrators are charged with the responsibility of identifying network problems and repairing it with the aim of ensuring a smooth run of operations in the network. They also do whatever it takes to ensure that the network is operating at optimal levels.

The following are among the many computer network troubleshooting processes:

- Configuration and reconfiguration of switches, routers or any other network component.
- Identifying any network issues and figuring out a way to fix it.
- Installation and repair of network cables as well as Wi-Fi devices.
- Getting rid of malware from the network.
- Getting firmware devices up to date.
- Installation and uninstallation of software as is necessary.

Network troubleshooting can be done manually, or as an automated task- especially when it has to do with network software applications. Network diagnostic software is a valuable tool when it comes to the identification of network issues that may not be easy to detect with the human eye.

Network troubleshooting includes both hardware troubleshooting and software troubleshooting.

Hardware Troubleshooting

This is a form troubleshooting that takes care of issues with hardware components. It may include:

- Removal of faulty or damaged RAM, hard disk or NIC.
- Dusting of computer and other network devices-dust accumulation sometimes leads to malfunctioning of devices.
- Tightening of cables that connect different network components.
- Updating or installation of important hardware drivers

Hardware troubleshooting begins with the discovery of a given hardware issue, the cause and, finally, taking the necessary remedial action.

Software Troubleshooting

Software entails a set of measures for scanning, recognizing, diagnosing and offering solutions to issues with software in the network. It includes issues with network operating systems, diagnostic software as well as software applications installed on individual network computers.

Chapter 2: Network Management

Effective network management must address all issues pertaining to the following:

- Hardware
- Administration and end-user support
- Software
- Data management

Hardware Management and Maintenance

Hardware maintenance can be performed as per the following routines and considerations:

Cleaning

Every two weeks clean all network equipment. Doing so will help keep your equipment cool and make other maintenance tasks easier to perform. When cleaning, dust the equipment, shelves, and nearby areas. A small vacuum should be used to vacuum keyboards and the computer vent and fan openings. Additionally, you should use the vacuum to gently suck dust out of removable media drives. Unused wall jacks and empty equipment jacks in dust-prone environments can be vacuumed on occasion as well.

For printers and plotters, follow the manual instructions for cleaning print heads on ink jets and vacuuming paper dust from laser printers. Monitors can be wiped down with eye-glass cleaning solution and glasses-cleaning cloths.

Performing Inspections

Keeping a close eye on the condition of all hardware is essential. For this reason, you should inspect all hardware at least once per month. This inspection should include the following:

- Make sure cooling vents are not blocked or excessively dusty.
- Listen to and feel the vents to make sure cooling fans are operating.
- Sniff the area. When power supplies and other parts are near failing, they may emit an odd odor from excessive heating. A burnt smell means trouble is imminent or has already occurred.
- Check all power cables, peripheral cables, and network cables for tightness in their sockets.
- Check all power cables, peripheral cables, and network cables for fraying or other damage.
- Check the server area for proper operation of heating, venting, and cooling systems to be sure they are operable- even if those systems are not needed at the time of the inspections.

Upgrading Firmware

“Firmware” refers to any program that is resident in a chip. For example, a computer’s BIOS is firmware. Sometimes, manufacturers release updates for firmware to fix flaws or to enable the equipment to work with some newly released hardware device or operating-system upgrade. You should check the manufacturer’s Web site or help desk for all network equipment at least quarterly to determine whether any firmware upgrades are available for your equipment.

If so, be sure to adhere to the maker’s instructions to the letter for loading new firmware and firmware updates. Firmware loads often require low-level booting from a DOS or maintenance disk, although some will be compatible with the computer’s operating system.

Upgrading Hardware

Two factors drive hardware upgrades:

- Performance issues due to changes in applications or the addition of new applications may necessitate a hardware upgrade or the addition of new features that are linked to the hardware's capability or capacity. For example, adding memory and installing an additional hard drive for more file space are typical upgrades performed to support those changes.
- You may opt to upgrade hardware on a purely optional basis-for example, adding a bigger monitor, higher-quality sound card, a TV card, or a similar device.

Repairing Hardware

As the person responsible for the network, you must assess your willingness and ability to perform hardware repairs-before a hardware component stops working. To that end, you should go through your entire hardware inventory and determine the following:

- Is the equipment still under warranty? If so, take advantage of that warranty in the event the equipment stops working.
- Would it be more cost-effective to simply replace a piece of hardware if it breaks? Given the high cost of technical labor, repairing a low-cost item, such as a printer that can be replaced for $50, may not be justified. It might even be best to replace rather than repair PCs purchased for less than $600 if you've used them for more than 10 months. Don't get me wrong: I am not advocating short equipment life cycles or unnecessarily adding to scrap piles.

- For big-ticket items, you may want to transfer the repair risk to someone else by arranging for service and support contracts-assuming your budget can support this.

Administration

Large networks often have one or more staff members dedicated exclusively to performing network administrative tasks. For smaller networks, the manager must wear various hats and perform multiple roles to support the network. Over time, he or she must rise to the level of journeyman-or at least experienced apprentice-to be successful.

Primary or routine network-administrative tasks fall into one of the following categories:

- Administering and supporting end users
- Adding workstations and peripheral devices
- Maintaining system-wide documentation

Maintaining System-Wide Documentation

Maintaining system-wide documentation might seem like a task you could skip, but you shouldn't. Without complete documentation, a lot of person hours can be wasted when something goes wrong, or when you are trying to add hardware to a server or applications to network hosts or workstations. Regrettably, for some technicians and network managers, checking the documentation prior to making system changes is not priority one as it should be. Good documentation practices are not a bane because they take time; they are a benefit to the network manager with little time to waste.

Network documentation should include all operation and maintenance booklets as well as manuals for all the hardware.

Administering and Supporting End Users

As the network administrator, you will likely be responsible for administering and supporting end-users. Examples of tasks you'll need to perform may include the following:

- Vetting new users for security purposes
- Adding, deleting, and changing end-user accounts
- Creating and administering group, role-based, and individual access controls

- Providing technical support
- Adding workstations and peripheral devices

Adding Workstations and Peripheral Devices

There will likely be times when some software-based administrative chores must be completed in order to add new workstations and peripheral devices to the network. Examples are hardcoding an IP address into a new workstation or printer or attaching a new printer to a print server’s queue. In addition, users may need to be assigned rights to access new equipment such as printers, along with access passwords for new workstations on the network. For more information, consult the documentation provided with the new equipment and your own documentation of necessary steps from previous changes.

Virtualization in Cloud Computing

What is cloud computing?

Cloud computing refers to delivery of IT resources via the internet as per the demand. It is normally implemented on a pay-as-you-go pricing basis. The concept of cloud computing seeks to offer a solution to users’ needs of IT infrastructure at a low cost.

Why cloud computing?

For small as well as big IT companies that still rely on traditional methods to operate primarily require a server to carry out their different tasks. The setting up of a server room requires skilled personnel, different servers, modems, switches, and lots of other networking resources-plus a lot more of other non-IT requirements that contribute to the completeness of a working office.

Traditional methods require a lot of human input, expensive equipment and a lot of other logistical necessities. These things require large sums of money. In order to set up a fully functional server, the organization or individual must be willing to break the bank. However, that is no longer thanks to the concept of cloud computing. Cloud computing helps individuals to cut down on infrastructure costs by eliminating the need for the purchase of expensive equipment and spending a lot of funds on hired personnel for the administration and management of IT resources.

Features of Cloud Computing

- Cloud computing operates in a distributed computing environment. This makes resource sharing to happen quickly.
- Cloud computing minimizes chances of infrastructural failure due to the existences of many servers. This makes it a more reliable infrastructure for IT operations.
- Cloud computing allows for large-scale, on-demand provision of IT resources without the need for engineers and many other professional that would otherwise come in handy.
- Cloud computing enables multiple users to share resources and work more efficiently by sharing the same infrastructure.
- Cloud computing eliminates physical location or distance concerns since users can access systems and resources regardless of their geographic location.
- Maintaining cloud computing applications is easier since they do not need to be installed on each user's computer.
- Cloud computing reduces the operating cost of an organization since it eliminates the organization's need to set up its own infrastructure-this turns out to be quite an expensive undertaking for most organizations. Besides, it allows an organization to only pay for a service or resource when needed.
- Cloud computing allows for pay-per-use mode for different services. It is a convenient way to use especially when a user needs to use a resource only once.

Benefits of Cloud Computing

The following are the major benefits of cloud computing:

- A person can conveniently use a low-cost computer to perform complex computer tasks that would otherwise require powerful machines-machines that fetch high prices in the market. Applications run on a cloud, not on the user's machine.
- Low-cost IT infrastructure is can sufficiently meet an organization's needs. There is no need of investing in high-cost IT infrastructure to handle big servers.

- Low-cost maintenance due to reduced infrastructural requirements-in terms of both hardware and software.
- Instant software updates for web-based applications-no need to worry about obsolete applications and high upgrade costs.
- The execution capacity of cloud servers is very high. This increases computing power and leads to efficient task execution due to high speeds of data processing and message delivery
- A cloud provides users with very large storage capacities-at very low costs.

Disadvantages of Cloud Computing

Some of the most conspicuous limitations of cloud computing are listed below:

- You cannot access resources on a cloud without internet connectivity. It is mandatory that the user is connected to the internet in order to access resources (or use the IT infrastructure) offered on a cloud.
- Low internet connectivity may be greatly frustrating when trying to perform important tasks on a cloud. Most web-based applications run effectively on a lot of bandwidth. Low bandwidth may at times cripple the execution of some tasks.
- There is no guarantee of security and confidentiality of data stored on a cloud. Unauthorized users can gain access to your data/information stored on a cloud.

What is virtualization?

Virtualization is a process by which a virtual version of some actual thing is created. In computing, this may involve virtualization of an operating system, network resources, server, storage device or even a desktop.

Technically, we can refer to virtualization as a technique which permits sharing of one instance of a physical resource or application among multiple users or groups.

The technique involves the assignment of a logical name to a physical storage of a given resource or application and offering a pointer to the specific resource or application as is required.

The Concept behind Virtualization

The process of creating a virtual machine over an existing hardware and operating system is referred to as Hardware virtualization.

Hardware virtualization creates an environment which is separated logically from the actual machine.

The machine on which the creation of a virtual machine occurs is referred to as the host machine. On the other hand, the created virtual machine is technically referred to as a guest machine.

Types of Virtualization

The following are the different types of virtualization

- Server virtualization
- Storage virtualization
- Operating system virtualization
- Hardware virtualization

Server Virtualization

When virtual machine manager (VMM)-virtual machine software-is directly installed on the server then the process is referred to as server virtualization.

Why Server Virtualization?

Server virtualization is essential because it is possible to subdivide a physical server into multiple servers on a demand basis, and also for load balancing.

Storage Virtualization

This is the process that involves the grouping of multiple physical storage devices in a network so that they appear like a single storage device. Software applications are also used for the implementation of storage virtualization.

Why storage virtualization?

This is crucial for recovery and back-up reasons.

Operating System Virtualization

In this case, the virtual machine software (VMM) is installed directly on the operating system of the host machine. Unlike in hardware virtualization, VMM is not installed on the hardware.

Why operating system virtualization?

Operating system virtualization comes in handy when there is a need to test applications on a different operating system platform.

Hardware Virtualization

In hardware virtualization, the virtual machine software is installed directly on the hardware system.

Hypervisor is charged with the responsibility of controlling and monitoring the memory, processor and hardware resources.

We can install different operating system on the system and use it to run a lot of other applications-after virtualization of the hardware system.

Why hardware virtualization?

Hardware virtualization is largely important for server platforms since the control of virtual machines is not as difficult as the control of a physical server.

How Virtualization Works in Cloud Computing

Virtualization is a greatly potent concept in cloud computing. Normally, in cloud computing, users need to share resources available in the clouds. For instance, applications and files are some of the sharable resources that may be stored in the clouds. With virtualization, users are provided with a platform that making sharing of such resources a practical experience.

The primary goal of virtualization is to offer applications with their standard versions to users in the clouds. When new application versions are released, users look up to software developer for the new release. This is possible but may turn out to be quite a hectic affair if all users have to download the new version from a central server. To resolve that issue, virtualized servers and software can be maintained by third parties at fee, but cloud users can efficiently access the new software releases.

In summary, virtualization primarily means running several operating systems on one machine that share all hardware resources.

This technique is hugely helpful because it makes it possible to pool network resources and share them to different users conveniently, and at less cost.

Chapter 3: Computer Network Communication Technologies

How computers communicate in a network

Communication among different computers in a network takes place when data is transmitted from one machine to another.

The transmitting computer is referred the sender (source). The machine to which data is transmitted is referred to as the receiver (destination).

For communication to take place, data is transmitted in the form of data packets. For data to get to the desired destination, data packets are assigned source and destination address. The source address identifies the sender. On the other hand, the destination address identifies the receiver (destination).

There are different ways in which data may be transmitted from one machine to another. Notably, there is more than one way in which data transmission happens.

The way in which data can be transmitted from one computer to another is referred to as data transmission mode. Transmission mode is also referred to as communication mode.

The different data transmission modes include the following:

- Simplex mode: communication goes on in one direction. That is, the communication is unidirectional. A device can only receive data but can't send, and vice-versa.
- Half-duplex mode: communication is bidirectional. That is, a device can send and receive data. However, it cannot send and receive at the same time.
- Full-duplex mode: communication is bidirectional. Unlike in half-duplex mode, communicating devices can transmit and receive at the same time.

Addressing

A message needs to originate from a known sender and be clearly addressed to a known recipient.

For instance, traditional post office requires that the sender identifies himself or herself by name and location. The sender must also indicate the recipient's name and exact location (address).

Similarly, computers in a network are identified by their MAC addresses and IP addresses. MAC addresses are embedded on the computers' NICs while IP addresses are manually assigned during the configuration process; or the IP addresses are dynamically assigned by enabling the Dynamic Host Configuration Protocol (DHCP) on each machine. Each and every network host has a unique MAC address and unique IP address that identifies the given machine.

Understanding Ethernet

Ethernet network architecture is the most widespread of all network architecture all over the globe. We're going to examine the depths of this architecture and most likely find out why this architecture is as popular as it is.

Most network peripheral components have a built-in NIC. As a result, they can be easily plugged into an Ethernet wall outlet. It must be noted that the standard predetermined Ethernet length of wire of 100m from a hub or switch remains so even when it comes to NIC-equipped print servers and printers; just as it is the case with workstations.

Printers that do not have a built-in NIC can still be used on a network by getting a connection with a network print server through a parallel, serial or USB port, or onboard NIC.

Ethernet Network Access Strategy

Suffice to say, Ethernet is a passive network architecture that embraces the wait-and-listen approach. It is also referred to as contention-based architecture since all computers on the network have to contend with the time of transmission on a given network medium.

Access to Ethernet networks is via CSMA/CD. This simply means that the network hosts have to listen to the network until the transmission medium is clear so that they can also transmit. Basically, they have to “sense” and determine that the line is indeed clear to initiate their own data transmission processes. A network host only sends out its data once it “feels” that the transmission is clear. In case there are multiple transmissions, a collision or collisions take place on the transmission medium. The machines sense the collisions and immediately halt their transmission processes.

One of the machines starts the retransmission as the others wait for the line to clear before they can retransmit their data. This process happens until all the network have completed their transmissions.

In a similar fashion, hosts wait and listen on the line for data meant for them. When a particular host senses that incoming is mean for them, they open door for its reception and actually does receive the data onto its NIC interface. Ethernet is characterized by frequent collisions. As a result, some devices have collision to prompt you when a collision happens. In fact, collisions are the main limitations of the Ethernet architecture. On the hand, Ethernet is the most affordable of all other network architectures.

Note:

- Collisions slow down the network.
- Excess collisions may bring down a network completely.

Fast Ethernet

The traditional Ethernet has a speed of 10Mbps. Fast Ethernet offers a speed that is higher than the original 10Mbps. It has a 100Mbps transfer rate. The throughput is higher than the traditional Ethernet standard since the time it takes to transmit data over a network medium has been minimized by whopping factor of 10. Thus, Fast Ethernet works at a rate that is 10 times the traditional speed of 10Mbps.

Traditionally, hubs and other connecting devices were designed to accommodate the 10 Mbps transfer rate. For such devices, Fast Ethernet is not supported. Fortunately, many connecting devices are being with NICs that can comfortably handle both 10Mbps and 100Mbps transfer rates. That means that the devices can accommodate both the original 10Mbps Ethernet as well the Fast Ethernet.

Gigabit Ethernet

This is another version of Ethernet that is even faster than Fast Ethernet. It uses the same data formats and IEEE Ethernet specifications just like the other Ethernets-10Mbps and Fast Ethernet.

With Gigabit Ethernet, users are able to enjoy 1000Mbps transfer on a network. Unlike Fast Ethernet that operates on both twisted-pair cables and fiber-optic cables, Gigabit Ethernet was initially restricted to fiber—optic cabling. This required that a LAN be set up with specialized servers and high-speed switches. Gigabit Ethernet was considered to be a backbone for large LANs that required high transmission speeds.

Currently, anyone can practically enjoy the amazing high speeds of Gigabit Ethernet since it is being bundled out in network cards that can be conveniently installed in network servers and network clients.

Ethernet IEEE Cable Specifications

The following is a list showing some of the Ethernet specifications:

- 802.3 for Ethernet LAN
- 802.5 for Token-Ring LAN
- 802.7 for Broadband TAG
- 802.8 for Fiber-Optic TAG
- 802.9 for Data Networks and Integrated Voice
- 802.10 for Network Security
- 802.11 for Wireless Networks

Note: TAG stands for Technical Advisory Group

The following points must be taken into account:

- Ethernet is well-defined by the IEEE specifications of 802.3.
- It works at the Data Link layer of the OSI mode.
- A number of the various IEEE types of Ethernet are available depending on the nature of cabling preferred on the given computer network.

These types of Ethernet-Gigabit Ethernet and Fast Ether- are designated by 3-part names, like *10BASE-T* . The first section of the name describes the transmission speed. For instance, 10 specifies 10Mbps Ethernet.

The second part of the name, which is “base” for all the different forms of Ethernet, indicates that the Ethernet signal is *baseband* . This means that the data drifts in a stream as one signal. This type of data transmission cannot allow the transmission of multiple channels of data or information as can the alternative-the *broadband.*

The last part of the Ethernet type name specifies the type of cable in use. For instance, in 10BASE-T, the *T* indicates a twisted-pair cable, and it is presumed to be unshielded twisted-pair cable.

10BASE-T *:* This type of Ethernet works with a twisted-pair cable (unshielded twisted cable). The maximum cable length (without signal amplification) is 100m. 10BASE-T is operable on a star topology.

10BASE-2: This type of Ethernet works with a fairly flexible coaxial cable (RG-58A/U I or a *thinnet*), with a maximum cable length of 185m (this is rounded off to 200. Thus, the *2* in 10BASE-2). With the use of T-connectors to link the cabling to the network hosts’ network cards, 10BASE-2 uses a bus topology. Though 10BASE-2 has always been the most pocket-friendly option for the Ethernet implementation, 10BASE-T setups are presently the most widespread.

10BASE-5: This is type of Ethernet that uses a large-gauge coaxial cable (also referred to as *thicknet*), and the hosts on the network are linked to a main trunk line. The cables from the network hosts join the main trunk cable using vampire tabs, which pierce the primary trunk cable.

100BASE-TX: This is the type of Fast Ethernet that relies on the same Category 5 UTP cabling that is available on 10BASE-T Ethernet. This enactment can also employ 100-Ohm shielded twisted pair cable. The maximum cable length in the absence of a repeater is 100 meters.

100BASE-T4: This is the sort of Fast Ethernet that runs over Category 5 cabling, as can the 100BASE-TX. However, it can as well run over lower-grade twisted-pair cabling like Categories 3 and 4. In this type of Ethernet, the maximum cable run is the standard 100m length.

100BASE-FX: This is the sort of Fast Ethernet that spans over fiber-optic cable with a maximum length of 412m.

1000Base-T: This is the kind of Gigabit Ethernet that delivers 1000Mbps over Category 5 twisted pair cables.

10Gigabit Ethernet . This is the kind of Ethernet that delivers 10 billion bits per second over fiber optic cables.

Peer-to-Peer Communication

The peer-to-peer network setup offers a simple and cost-friendly networking solution in which the basic networking functions are needed. Peer-to-peer is ideal where file sharing and other basic resources such as printers. In this networking arrangement, there is no need for a dedicated server. The elimination of a network from the budget makes this kind of networking a highly pocket-friendly venture. It must be understood that network servers are quite expensive. They significantly contribute to the overall cost of a network. Therefore, its omission from the shopping list is a great way of cutting down on the installation cost of a network, as well as overall management of the network. It is the most ideal option for the implementation of small networks.

Features of Peer-to-Peer Networking

The following are the main features of Peer-to-Peer Networking:

- All network computers have equal privileges. They behave like peers.
- Each network host acts like both client and server. Essentially, a network can send out requests to another network hosts.

Similarly, each host can receive requests from other any other host on the network.

- There is centralized administration of resources. This is due to the omission of a dedicated server from the setup. This also forms a concrete basis for connoting a peer-to-peer network as a workgroup. The peers collaborate freely without any centralized control or regulation.
- You only need to install an operating system on each peer and then physically connecting the peers via the NICs (NICs are not even necessary when working with Macintosh computers).

Merits of Peer-to-Peer Communication

The following are the main advantages of a peer-to-peer network implementation:

- Peer-to-peer network implementations are easy install since they only involve the installation of operating systems on peer computers and physically connecting them.
- They are less expensive since a costly server computer is not needed. Furthermore, a Network Operating System (NOS) is also not needed.
- All required is readily available, most of which comes packaged in your operating system.
- The network implementation is reliable since failure or malfunction of a single peer does not lead to failure of another, or failure of the entire network.

Demerits of Peer-to-Peer Communication

The following are the main limitations of a peer-to-peer network:

- If multiple users access a printer that is connected to your computer, you're your computer's processing resources are used as the printer serves your peers.
- There are challenges when it comes to data backups since there is no centralized location for sharable files.
- Resource management is difficult since resources have to be managed one by one.

- It is quite difficult to manage resources since resources are scattered all over the network.
- The security of the network might be easily compromised. Also, users might have to keep track of multiple network access credentials (usernames and passwords).

Chapter 4: The Internet

Internet basics

This section covers some of the basic technology concepts that makes the Internet work and discusses various options for connecting to the information superhighway so that everyone on your network can surf the Internet, communicate via e-mail, share digital pictures with others, conduct research using countless online resources, make purchases online, download movies and music, video conference, and more.

Internet Technical Terms

Just as you don’t necessarily need to know the inner works of a combustion engine to drive a car, it’s not imperative that you understand every aspect of how the Internet works in order to take advantage of all that it offers. That said, it never hurts to examine, however briefly, the various terms and concepts that relate to the Internet.

TCP/IP

TCP/IP—short for Transmission Control Protocol/Internet Protocol—is a group of rules called protocols that define how devices, be they similar or diverse (i.e., computers, routers, and modems), connect and communicate with each other. (In this context, a “protocol” describes technical details about how any two communication devices will interact and work together to move digital data from one device to another.)

TCP/IP works by determining the best available transmission path for data to travel. Rather than sending all the data in one large chunk, however, the protocol breaks the data into small packets.

These packets can travel over any number of different paths to reach their destination; when they arrive, they are reassembled in order.

To ensure that packets arrive at the correct destination, each one contains both the destination address and the source address. This information is stored in each packet’s “envelope,” or “header.”

The TCP part of the protocol controls the breakdown of data on the sending end and its reassembly on the receiving end, while IP handles the routing of the data packets.

Think of it this way: Sending data via TCP/IP is not unlike sending letters via the U.S. Postal

Service. Each letter you send by post contains the sender’s address (i.e., the source address) and the recipient’s address (i.e., the destination address). The difference is that with snail mail, you send the whole letter in one package or envelope (packet). If you were to send that same letter over the Internet, it would be sent in hundreds if not thousands of packets (envelopes) to get to its destination, after which it would be electronically reassembled.

Internet protocols in use under the TCP/IP banner include UDP, PPP, SLIP, VoIP, and FTP.

Sub-net Mask

A sub-net mask is a number applied within a host configuration file that allows for the division of an IP class C network into separately routable networks. For home networks on an ISP’s larger network, the sub-net mask will most often be 255.255.255.0, because home networks are not usually split into physically separate segments with internal routers. In office buildings and business environments, sub-nets are used to detach traffic onto physically isolated networks to retain the data traffic on the low and to enhance performance for access to peripherals and local servers. Data traffic destined for another sub-net or to the WAN will have to pass through the router.

DNS

Just as it is easier to remember someone’s name than it is to remember her phone number, so, too, is it easier to remember the location of a Web site by its domain name rather than its IP address. For example, suppose you frequently visit the Web site of Ford Motor Company. Chances are, you will probably remember the site’s domain name-i.e., Ford.com-and not its IP address. Your computer’s Web browser, however, operates in the exact opposite way. It needs to know Ford.com’s IP address in order to connect with the site.

That’s the point domain name system comes in. When you enter the domain name of a site you want to visit (Ford.com), your Web browser initiates a session with a DNS server either locally or on the Internet to locate the IP address associated with that domain name. DNS servers perform a hierarchical lookup for the IP addresses using domain name associations for registered domain names to locate the IP address of the site you want to visit. If the DNS server your computer is linked to cannot determine the IP address linked with the domain name you entered, the DNS server will then look up the number on successively higher-level DNS servers until it finds the entry (or errors out).

Once the IP address is found, your computer can locate and communicate with the computer housing the Ford.com Web site. The first DNS server stores the association in memory for a time in case you or someone else it serves needs to visit that site again. The DNS server stores only frequently used associations because it can look up the ones it does not know on the higher-level DNS servers.

Assessing Internet Service Plans

Two things are necessary to establish home access to the Internet: at least one Internet-capable computer on your network and the purchase of an Internet service plan from an Internet service provider (ISP). What plans are available will vary somewhat by geography (with suburban and rural areas having fewer options than urban ones), the communication media you want to use, and the options put forth by your ISP.

Some critical plan features include the following:

- Price
- Internet speed
- Equipment provided by ISP
- Customer service support
- Nature of IP address provided-static or dynamic
- Transmission media used
- Email addresses
- Webpage hosting
- Complimentary Wi-Fi access

Making the Connection

To connect your computer to the Internet, you must choose from the service-plan options available in your area. Once you have evaluated the connection plans and media options in your area and have selected an ISP, review some of the following considerations below for guidelines on how to set up Internet access.

Connecting with Dial-Up

Dial-up is, for the most part, obsolete from a speed perspective, but in some rural areas, it is the only available low-cost Internet-connection option. When connecting your computer using dial-up over a plain old telephone service (POTS) line, there are three common scenarios:

- Hooking up a computer or laptop with a built-in modem
- Using an external dial-up modem connected via a USB port
- Using a modem that will connect to a 9-pin serial port.

Connecting with Cable

A popular Internet-connection choice in many areas is cable. In fact, your home or small office may already have a cable connection for television service, making the addition of a cable modem to the mix fairly simple. Cable Internet service is high speed-much better than that offered by dial-up. In addition, many cable-based packages bundle increased television channels for viewing and Internet phone service.

Connecting with Wireless (Wi-Fi)

Connecting wirelessly to the Internet is fairly simple, but your network must include a gateway or router designed for wireless connections. In addition, any computers on your network must have Wi-Fi capabilities built in or, in the case of a laptop or notebook computer, a slot for a wireless Wi-Fi card.

If your computer or workstations are not configured for Wi-Fi, fear not. There are hosts of manufacturers making devices to support wireless connections—essentially, these are portable wireless NICs that can be plugged into either an Ethernet port or a USB port.

Connecting with DSL

Using DSL to connect to the Internet over standard phone lines has an advantage of accessing the internet are higher speeds than the dial-up option (assuming you live in an area where DSL service is available). Moreover, whereas a dial-up connection relies upon the audio/analog band on a phone line, data on a DSL Internet connection passes over the wire pair at a frequency that is higher-meaning that users can still use their phone lines while at the same time using the Internet (and, by extension, keep your Internet connection live 24/7).

Network Address Translation

Network address translation (NAT) is an important feature on Internet connection devices and gateways that allows a computer to have an IP addresses that is not visible on the Internet, yet still receive and send data packets over the Internet. These addresses are hidden and are assigned from a different set of IP addresses-called private IP addresses-from the addresses that are seen or exposed on the Internet. These private addresses are assigned to computers inside the firewall, enabling them to use TCP/IP protocols for communicating to internal devices and to hosts on the Internet without being seen-thereby making it harder to hack into the internal computer. Using NAT is the first tier in firewalling or protecting your network computers from unwanted intruders anywhere on the Internet.

Private IP addresses also extend the connectivity of the Internet to more computers than there are available IP addresses because the same private, internal network IP address can be used at hundreds, thousands, or even millions of locations.

It works like this: When you open a browser to reach, for example, Yahoo.com, the data packet reaches your Internet gateway/firewall, which in turn starts a session to keep track of your MAC address and IP address. It then replaces your private IP address from the data packet with its own visible IP address in the data packet and sends the request to Yahoo.com. When the information is returned from Yahoo for your session, the process is reversed; the Internet gateway/firewall strips out its own IP address, re-inserts your computer's private IP address and MAC address into the packet header, and passes the packet down the network wire to your computer.

When this happens, your internal IP address is said to have been "network address translated"-although a better term might be "network address substituted." By default, most home network gateways use NAT and assign private IP addresses to all the computers on the home network.

Private Networks

Private networks are IP networks with host computers that hide behind a device that provides NAT. The computers on these networks are assigned IP addresses outside of the pool of numbers used on the Internet. Essentially, any number in the private address range can be assigned locally to a computer or host.

Private network IP addresses begin with any of the following numbers:

- 10
- 172.16–172.31
- 192.168

A complete example might be 192.168.11.4 or 10.101.101.1.

Worldwide Web: Window to the World

Like a living organism, the Web is constantly changing as networks are added or changed. The growth of the Internet both in geographic reach and audience presents every connected entity with opportunities to communicate like never before in history. If your use of the Web is limited to simply downloading information and receiving e-mail, you are hardly scratching the surface of what can be accomplished over the Web. Ways to use the Web to inform, educate, and exchange ideas, goods, and services with a worldwide audience are limited only by one’s imagination and creativity. This chapter merely skims the surface of what you can do on the Web.

Leveraging Your Connection to the Web

Connecting your network-or a sub-network of your network-to the Internet stretches the reach of your home or office network to the far corners of the earth. For under $120 per month in most markets around the country, you can obtain a connection to the Internet that runs at decent speeds and includes up to five static IP addresses.

These addresses can significantly enhance your ability to garner the most benefit from your connection to the Internet. That’s because in order to make Web servers, Web cams, and other resources available on the Web, you need at least one static IP address that is visible on the Internet. Additionally, a static IP address can be used to enable VPN clients to connect to your network resources. Without a static IP address, much of your communication to the outside world is limited. With a static IP address, however, your network can become a Web site, client-services provider, radio station, TV station, or blog-just to name a few.

The Web really is a window on the world. Not only can you see out, obtaining incredible amounts of data from the Web, so too can others anywhere in the world see in, enabling you to share information of your choosing with a worldwide audience. Adding your own resources to the Web-the ultimate unfettered two-way, free-speech forum-can both provide value to you and your organization and increase the utility of the Web for others.

Popular Uses of the Web

The following are the main uses of the web:

Finding or Publishing Information

Most people use the Internet to obtain information-which is why some people call it the largest library in the world. The best way to obtain information online is to enter keywords or phrases into a search engine like Yahoo, Google and Ask.

When you type a keyword or phrase into the search field on any one of these sites, it returns any number of links to Web pages that relate to the word or phrase you entered. Ask yourself or your organization’s management: What information about you, your family, or your company should be posted to a Web server?

There is more to getting your information found or your voice heard on the Internet than simply getting a domain name such as thisismywebsite.com. To ensure that the information on your site can be found when someone performs a related search, you enter key search words into your document headings and possibly pay to register your site with various search engines. Learning key search words and adapting your document headings and labels accordingly is a science in itself. And even if you master it, your business Web site might be listed at the top of the search results one day and slip to 100 or 1,000 the next. Like the Wild West, there are few rules on the Internet, and anything goes when it comes to getting noticed.

Communication

This takes place in the following ways:

E-mail

The most popular Internet communication tool is e-mail-that is, messages are sent electronically from sender to host on the Internet, potentially forwarded to other hosts, and ultimately downloaded at the recipient’s convenience.

One way to obtain an e-mail account is from your Internet service provider (ISP); most plans include the use of at least one e-mail address. Alternatively, you might run your own home or office e-mail server under a domain name you own. You access messages received via these accounts through special software called an e-mail client.

Another option is to use any one of several free Web browsers–accessible e-mail services, such as the following:

- Yahoo! Mail (http://mail.yahoo.com)
- Gmail (http://www.gmail.com)

Instant Messaging (IM)

Another way to communicate over the Internet is via instant messaging (IM). IM provides instant communication; there is no middleman to store or forward the message. Both end-users must be online to IM; when they do, the text they type is transmitted instantly from one to the other in back-and-forth fashion the second the Send button (or similar) is clicked. You can IM using an IM client on your desktop or, in some cases, a Web browser. Popular instant-messaging applications include the following:

- Yahoo! Messenger
- Window Live Messenger

Video Conferencing

Video conferencing gives users the rare chance of conducting virtual meetings, thereby saving on a lot of travel expenses. To do a video conference over the Internet, at least one participant ought to have a static IP address visible to the Internet. Additionally, each participant should have service with an upload speed of at least 400Kbps to maintain quality communications, particularly if you're using the video component. To video conference, you must have access to a Web cam of some sort.

Blogging

Blogs, short for Weblogs, are sites on which people can share information with other interested or likeminded individuals. Think of a blog as a digital journal that can be read by people around the world.

Entertainment and Media

The Internet boasts a plethora of entertainment options, including the following:

- Interactive gaming
- Music
- Video
- News

- Internet radio
- Internet television

Engaging in Commerce

Commerce represents one of the most common uses of the Internet. Business-related activities include (but are not limited to) the following:

- Banking
- Advertising
- Retail sales and marketing
- Auctions

Downloading Software

Many major software publishers-including Microsoft, Corel, and Sun-offer users the ability to download what would otherwise be boxed commercial off-the-shelf software (COTS). All you need is a good Internet connection and a PayPal account, credit card, or in some cases a checkbook to pay the fee. There is also a wide variety of trial software, freeware, and shareware, as well as open-source software, available for download online.

Surveillance

Setting up surveillance cameras to be viewed over the Web is nearly a plug-and-play operation, provided you have the necessary IP addresses to support the camera or Web servers. This technology allows, for example, monitoring of your home or office while away or, say, checking on your summer house while you are at home.

Business owners can set up cameras at their place of work to monitor events at the office or keep tabs while away.

Chapter 5: Router and Server Basics

Routers and servers are very important network devices. This section seeks to outline some of the fundamental concepts of routing as well as the client/server architecture. We're also going to examine a VLAN and how to configure it.

Router: what is it, and what does it do?

A router is just another networking device that primarily connects different networks. A router plays the role of forwarding data packets based on what information is contained in the header of a data packet.

This is a device that operates in the network layer of the OSI model. In the TCP/IP model, a router operates in the internet layer.

Routing refers to the process of determining the best path along which data transmission takes place-from source to destination. Routing is done by a router, which has been defined above.

Routing algorithms are responsible for actualizing the routing process. The routing algorithms refer to a piece of software that works behind the scenes to ensure that the most appropriate path is selected for the transmission of data from sender to receiver.

The routing algorithms are also responsible for the initialization of the routing table. They are also responsible for the maintenance of the routing table.

Routing metrics are used by routing protocols in the determination of the best path for data transmission. Routing metrics include hop count, delay, bandwidth and current load among others.

Routing Metrics and Costs

Metrics and costs play a key role in determining the best path. Metrics refer to network variables that are considered in the determination of the best path. Routing metrics include the following:

- Delay: this refers to the time that a router takes in the queuing, processing and transmitting of data to a given interface. The path with the lowest delay value is unquestionably taken to be the best path.

- Hop Count: this refers to a metric that offers a specification of passes through a connecting device like a router. The path with the lowest hop count is preferred to any other available path if routing protocols consider the hop as a primary variable.
- Bandwidth: this refers to the link capacity. It is given in bits per second. The transfer rates of all links are compared. The link with the highest transfer rate is embraced as the best path.
- Reliability: the reliability value is determined dynamically. Some links are more vulnerable to malfunctioning than others. Besides, some links are more easily repaired than others-after a breakdown. Whatever the case, a more reliable link is preferred to a less reliable link. The system administrator is charged with responsibility of assigning reliability values which are numeric in nature.
- Load: this is the degree of how busy a network link is at any given moment. It may be in the form of packets that are processed per unit time; processor utilization or memory use. The load increases with increasing traffic. In routing, the link with a lighter load is considered to be the best path for data transmission.

Routing Types

Routing appears in the following classifications:

Static Routing

This is also referred to as non-adaptive routing. The administrator has to add routes in the routing table manually. Packets are sent from source to destination along a path that’s defined by the administrator. Routing does not depend on network topology or network state. It is the job of the administrator to decide the routes along which data are transmitted from source to destination.

Merits of static routing

- There is no overhead on router CPU usage.

- There is more security since the administrator has control over a particular network only.
- There is no bandwidth usage between different routers.

Limitations of Static Routing

- It is quite exhausting to come up with a routing table for a big network.
- The administrator must be highly knowledgeable in networking and particularly in the network topology he or she's dealing with.

Default Routing

In this technique, router configuration is done in a way that a router sends all data packets to a single hop. It does not matter the network on which the hop is found. Packets are simply relayed to the machine on which it configured by default.

This technique is most ideal when a given network has to handle a single exit point. However, a router would choose another path that is specified in a routing table and ignore the one that's set by default.

Dynamic Routing

This is also referred to as adaptive routing. In this approach, a router determines the routing path as per the prevailing condition in the network.

Dynamic protocols the heavy lifting when it comes to discovering of new routes. These protocols are RIP and OSPF. Automatic adjustments are meant when particular routes fail to function as expected.

Features of Dynamic Protocols

The following are features of dynamic protocols:

- Routers must have the same protocols to exchange routes.
- A router broadcasts information to all connected routers in whenever it discovers an issue or issues in the topology or network status.

Merits of dynamic Routing

- They’re quite easy to configure.
- The best option when it comes to determining the best paths due to changes in network status and topology.

Limits of Dynamic Routing

- It’s a lot more costly when it comes to bandwidth and CPU usage.
- It’s not as secure as default and static routing.

Important Notes!

- A router filters out network traffic not merely by packet address, but by a specific protocol.
- A router does not divide a network physically. It does so logically.
- IP routers divides networks into a number of subnets to ensure that specific network traffic meant for a particular IP address can be allowed to pass between specified network segments. However, this intelligent data forwarding leads to decreased speeds.
- Network efficiency is higher with the use of routers in complex networks.

Network Servers

A network server refers to a software application that runs a remote network machine to offer services to other machines on a given network.

Client computers in a network make requests to the server whenever they need certain services. The offers an open window for client request, but does not, at given moment, initiate a service.

Servers are infinite programs that, when started, runs infinitely unless an issue pops up. A server always stands in wait for requests from client machines on a given network. The server responds appropriately to all incoming client requests.

Some networks do not have a dedicated server to control communication on the network. Given such arrangements, network devices communicate directly with one another. There are, however, a number of merits as well as demerits of servers in network operation.

Merits of Servers

The following are pros of using a server to handle client request on networks:

- Centralized administration ensures more security in in respect of resource sharing.
- Use of a server provides a centralized back-up system since important data is stored in a server computer.
- There is increased network speed in respect of resource sharing.
- There is a higher scalability level since it's possible to expand the network in terms of clients and server separately.

Limitations of Using Servers

- Traffic congestion is always a big issue when many clients have to send requests simultaneously.
- There is no robustness in a network since a breakdown or malfunction of a server derails all request handling features of a network.
- Specific hardware may be required at the server-side since a client/server network is greatly decisive.
- There may exist a resource in server computer, but not in a client computer.

Servers are available in different forms. The following is a list of different servers that play highly significant roles in computer networks:

Access Servers

Remote (LAN) access offers network connectivity to remote users who may be otherwise constrained by geographic limitations of a LAN. An access server makes use of a telephone line to connect an office or user with an office network.

Network Time Servers

Network time servers are servers that handle all network timing information from different sources including radio broadcasts and satellites. These servers then avail the gathered information (from different sources) the given network.

Time servers rely of NTP and UDP/Time protocols to communicate with other nodes. In so doing, there is proper synchronization of coordinated activities in the network.

Device Servers

A device server refers to a specialized and network-based network device that meant to perform one or more server functions. A device has three main features that include client access and minimal operating architecture.

There is no per seat operating system license in the minimal operating architecture. Also, client access is independent of any proprietary protocol or operating system.

Besides the above two features, a device server is a “closed-box” server. This means that it requires minimal maintenance, is easy to install, and is remotely manageable via a browser.

Examples of device include network time servers, terminal servers and print servers. These device servers are designed to handle perform specific tasks. Each device server is characterized by a unique set of configuration features in software and hardware. The unique features help these servers to work optimally.

Multiport Device Servers

These servers allow sharing of devices between terminals and hosts locally and all over a given network. One terminal can be connected to multiple hosts and can conveniently switch among the different hosts. Multiport device servers can as well be used on device that have serial ports only.

A multiport device server can convert between known protocols such as TCP/IP and LAT. This is possible primarily due to a multiport device server’s natural ability of translation.

Print Servers

Print servers make it possible for different network users to share network printers. A print server may support either a serial or parallel interface. As a result, print server accepts requests from all network users using appropriate protocols. A print server also manages printing jobs on every network printer.

Understanding VLAN

VLAN is an acronym for Virtual Local Area Network (normally referred to Virtual LAN). It refers to a switched network that is segmented logically using a project team, application or function. The logical segmentation is done without consideration of users' physical locations.

VLANs are more or less same as physical LANs. The only difference is that VLANs allow end stations to be grouped regardless of whether they are on the same physical segment or not.

A VLAN can accommodate any form of switch module port. Multicast, broadcast and unicast data packets can be forwarded and flooded to end stations only in a given VLAN.

Each VLAN is taken as a logical network. Packets destined for stations outside of a VLAN must be forwarded through a router to reach its destination. Notably, a VLAN can be associated with an IP sub-nets.

Supported VLANs

Conventionally, we identify VLANs with a number ranging from 1 to 4094.

The following must be noted:

- 1002-1005 VLAN IDs are reserved for FDDI and Token Ring VLANs
- VLAN IDs > 1005 are not found in the VLAN database since they are extended range.
- Switch module supports extended-range and normal range VLANs (1005).
- Number of configured features, SVIs and routed ports affects functioning of the switch module hardware.

VLAN Configuration Guidelines

It is important to understand the following facts:

- 1005 VLANs are supported on the switch module.
- Numbers between 1 and 1001 are used to identify normal-range VLANs.
- 1002 -1005 are reserved for FDDI and Token Ring VLANs.
- Switch module has no FDDI and Token Ring support.
- 1-1005 VLAN IDs are normally stored in the VLAN database as well as the file containing the switch module configuration information.
- 1006-4094 (extended-range) VLAN IDs are limited to private LAN, RSPAN VLAN, MTU, and UNI-ENI VLANs. These VLAN IDs are not saved in the VLAN database.

The following steps will help you create or modify a VLAN:

1. Use the [**configure terminal**] command to enter the global configuration mode.
2. Enter the [**vlan <** ***vlan-id*** **>**] to enter VLAN configuration mode.

   -Use an existing VLAN ID to modify an existing VLAN

   -Choose a new ID to create a new VLAN

3. Use the command [**name <** ***vlan-name*** **>**] to give your VLAN a name.

   Though this is optional for normal-range VLANs.

4. Use the [**mtu <** ***mtu-size*** >] to set the MTU size.

   This also optional.

5. Use the command [**end**] to return to privileged EXEC mode.
6. Use the [**show vlan {name** ***vlan-name*** **| id** ***vlan-id*** **}**]

7. Use the [**copy running-config startup config**] command to verify entries.
8. To delete a VLAN, use the command [**no vlan *vlan-id***]

Note that VLAN 1 and VLANs 1002-1005 cannot be deleted.

Chapter 6: IP addressing and IP sub-netting

IP Address

What is an IP address?

An Internet protocol (IP) address is a four-octet, eight-bit digital address (32 bits total) that, when written out, looks like this: 10.156.158.12. Evidently, an IP is a unique set of numbers that are separated by dots. The set of numbers is used to identify a computer (or network device) using Internet Protocol (IP) for network communication. In an IP address, the value of any of the octets-the numbers between the periods-can be from 0 to 255.

An IP address is not entirely different from a phone number. If you know someone's phone number-say, your Uncle Mike-you can call her by dialing her number on your telephone's keypad. Then, your phone company's computers and switching equipment go to work to connect your phone with the phone belonging to Uncle Mike over an audio communication channel.

Once connected, you can speak with buddy Bradley, even if he is many miles away. When you do, the audio signal carrying your voice will typically travel over a pair of copper wires from your house to a switch at your local phone company.

From there, the signal might be converted to a light wave in order to travel over a fiber optic cable to another switch. From this second switch, the audio signal might be converted to a radio-wave signal in order to travel from one microwave tower to another. Eventually, as the signal nears its destination-Uncle Mike’s house-it will be converted back to an audio analog signal, traveling over a pair of copper wires from Uncle Mike’s phone company to her house. (This scenario assumes the use of land lines. If cell phones are involved, then this process will vary in the details, but not in the concept.)

What is the Function of an IP Address?

In a similar fashion to how phones use numbers to connect on a local, regional, national, or international scale, an IP address facilitates connections between computer hosts as well as routing equipment. Put another way, if two computers on the Internet have each other’s IP address, they can communicate. But unlike phones, which use switching equipment to connect, computers connect to each other over the Internet through the use of routing equipment, which shares the communication paths with hundreds or thousands of other computers.

When data is sent from a computer to a router, the router’s job is to find a short, open communication path to another router that is both close to and connected to the destination computer.

The router accomplishes this either by using default routes or by dynamically learning and recording tables, called “routing tables,” that keep track of which IP addresses are present on any one of the router’s many open, up-and running communication ports. Because all the routers connected together on the Internet resemble a spider’s web, data can travel over many different routes or paths if necessary, to get to its intended destination. If one of the routers or some other connecting link goes offline, the other routers trying to move the data search for an alternative route to the destination.

In order to facilitate this dynamic communication method, routers are also assigned IP addresses so they can find each other.

IP Sub-netting

Routed IP environments require that your pool of IP addresses be sub-netted. This allows each sub-net to see itself as a separate segment of the larger internetwork. The router then ties together the various sub-nets into one network. The router knows how to route traffic to the correct segment because it builds a routing table. The routing table is basically the networks roadmap.

IP sub-netting is fairly complex, and so to make this discussion informative but still digestible at an introductory level, we will limit our exploration of sub-netting to one class of IP addresses; we will look at an example of sub-netting a Class B range of IP addresses. The mathematical tricks that we use to sub-net the Class B network can also be used to sub-net a Class A or Class C network (although sub-netting Class C networks greatly limits the number of usable IP addressed that you end up with).

Sub-netting is a two-part process. First you must determine the sub-net mask for the network (it will be different than the default sub-net masks; for example, the default for Class B is 255.255.0.0). After figuring out the new sub-net mask for the network, you must then compute the range of IP addresses that will be in each sub-net.

Okay, let's cheat a little before we do the math of sub-netting a Class B network. I think it will aid in the overall understanding of the sub-netting process. The following table shows the new sub-net masks, the number of sub-nets, and the number of hosts per sub-net that would be creating when using a certain number of bits for sub-netting (the Bits Used column).

IPv4 vs. IPv6

Currently, IP version 4 (IPv4) addresses are the Internet IP addresses of choice. As mentioned, these addresses are composed of four sets of eight bits. In the future, we will likely adopt the IP version 6 (IPv6) address scheme. IPv6 differs in form and substance from IPv4 in two ways:

- IPv6 addresses have eight 16-bit numbers (128 bits total), usually expressed in four-digit hexadecimal form. The range of a single 16-bit number is greater than that of an eight-bit number, spanning from zero to 65,535.
- The 16-bit numbers in an IPv6 address are separated by colons rather than periods.

Why make the switch? Because under IPv4, there are not enough numbers available to assign one to every computer or device on the Internet that needs one. IPv6 solves this problem, offering 2 raised to the 128th power addresses; in contrast, IPv6 offers only 2 raised to the 32nd power-although masking and private-address strategies have been used to extend the number of available IPv4 addresses on the Internet.

Chapter 7: Introduction to Cisco System and CCNA Certification

What is CCNA?

CCNA stands for Cisco Certified Network Associate. It is a widely held certification among computer network enthusiasts. This certification is valid for any computer network engineer that starts with the low-level network engineers, network support engineers and network administrators through to network specialists.

The certification program was founded in 1998. An estimated 1 million certificates have been awarded to qualified persons ever since.

CCNA program spans numerous crucial networking concepts. It is an essential foundational course for interested candidates in the preparation for current and emerging networking technologies.

CCNA Scope

The following are the major topics that feature greatly in CCNA certification program:

- Networking essentials-which includes definition of network; description of network components; and the basic network setup and configuration requirements.
- IP addressing
- The OSI Reference Model
- IP Routing
- Routers-routing protocols (OSPF, EIGRP and RIP)
- WLAN and VLAN
- Network device security
- Network security and management
- Network troubleshooting

Why CCNA?

- The CCNA certificate is a trusted validation of a networking professional's ability to manage and administer a routed and medium-level network. It is the validation of an individual's understanding of a network, and their ability to operate and configure it. It also certifies a person's ability to troubleshoot the network.
- The course offers lessons on how to meet network users' requirement by proper determination of a network topology.
- Candidates learn how to make point-point network.
- Protocol routing for connecting networks is also realized through CCNA certification.
- Network address construction is adequately explained in the CCNA certification course.
- The course offers a comprehensive explanation on the establishment of a connection with a remote network.
- CCNA certification is offered using easy-to-understand study material.
- The course is a prerequisite for other important CISCO certification programs such as CCNA Wireless, CCNA Security and CCNA Voice, among others.
- CCNA certification program equips learners with the necessary knowledge and skills for the installation, configuration and management of a small LAN and WAN service networks.

Different Forms of CCNA Certifications

There are two main approaches to fulfilling a CCNA certification course:

1. Combined CCNA Exam
2. ICND1 Exam and ICND2

Note that every CCNA certificate is only valid for a period of 3 years. Every holder of a CCNA certificate is expected to take a fresh examination after every 3 years.

Chapter 8: Fundamentals of Network Security

Network security is one of the most important aspects in overall computer. Now, more than ever, having an adequate security protocol which can combine both functionality and protection is essential for all types of users.

Amid the large amount of threats out there, users must have a system which they can rely on when going about their usual day to day business. In that regard, the need to integrate these aspects motivates users to find the ideal solution to their individual needs.

In this chapter, we are going to be taking a look at the fundamentals of network security, guidelines and best practices, as well as, the most common threats found lurking today. In addition, we are going to be discussing the ways in which the average user can take better care to avoid becoming the victim of unscrupulous folks out there.

The only thing to fear, is fear itself

It's natural for the average user to fear hackers. This may lead the average user to spend a pretty penny on security measures which may or may not offer the combination of security and functionality that such users need. In fact, the most common side effect of top-notch security measures is a slow system. For example, a solid online security system will essentially scan every single bit of information that goes through their system. However, this can lead to an overall slowing of internet connection speeds.

As a result, users may feel that they have been short-changed by the performance of their security system. Other systems may sacrifice certain safety features in exchange for faster performance and internet speeds. Yet, these tradeoffs may leave critical information and transactions vulnerable to unwanted folks.

That is why the first thing to keep in mind is that breaking the bank out of fear of being vulnerable may lead you to overspend on a system that, while keeping your system safe, may end up costing you more in the end. That is why finding the right balance is essential; striking a balance between features and performance is the ultimate goal of all users. Therefore, we will be taking an objective look at what threats are out there, which ones you will most likely be vulnerable to, and what you can do to protect yourself.

Please keep one thing in mind: of all the horror stories out there, some may not necessarily apply to so long as you don't engage in the types of practices that attract hackers and fraudsters such as handle a large volume of financial transactions on a daily basis. Consequently, taking the proper steps to secure the transactions that you do make, will go a long way toward keeping your information, and your money, safe.

What to be on the Lookout for

Threats are out there, and they are real. However, the most important thing to keep in mind is that hackers and fraudsters love feeding on low-hanging fruit.

What does that mean?

It means that cheaters are looking for vulnerable people who don't know any better. Hence, they prey on these individuals. This is why the elderly are a common target for phone scammers. As such, online cheaters are looking for folks who have left windows unlocked or have neglected to ensure their information is safe.

Also, please keep in mind that a lot of the fraudsters and hackers out there will essentially go on a phishing expedition. That's right, we mean "phishing" and not "fishing" since hackers tend to cast a wide net in search of unsuspecting victims.

As a matter of fact, phishing is one of the most common means of victimizing individuals. A hacker will go the extra mile to produce an official-looking email in which they feign to be part of some organization, such as a bank, in which you are registered with. Now, they have no way of knowing if you are actually a customer of that bank. So, the email needs to look as natural as possible so that, in the event that you are actually a customer of that bank, you will believe that it is an official communication. The scammers then trick the user into providing their username and password under the pretense that the bank is undergoing security updates and so on. When the unsuspecting victim falls for the scam, it is quite plausible that the crooks will then proceed to empty the victim’s bank account.

This scam was so predominant, that virtually every company out there took the necessary steps to ensure that their customers would not be subject to these attacks. In the end, phishing has been essentially crushed. Nevertheless, there are one, or two, hackers out there who still give it the old college try.

That being said, the following threats outlined in this chapter are examples of what you need to be on the lookout for.

Network Intruders

Intruders are lurking about. There is no doubt about that. It should be noted that most intrusion events happen from within. That means that intruders are generally people who have access to the network and seek to gain unauthorized access to other parts of the network.

Thus, it is important to have a clear picture of who has access to what and how sensitive information ought to be protect. For instance, if a company handles personal information belonging to their customers, great care needs to be taken in order to ensure that such information does not fall into the wrong hands. This is especially critical if such information could potentially become profitable.

A good practice in this regard is to update the roster of individuals who have access to your network, or your personal computer for that matter. That way, if a breach should happen to occur, it will be easier to pinpoint who has access to what and where the breach may have originated.

Outside intruders may attempt some kind of remote access to your network, but they would at least need to have some kind of insight into usernames and passwords. Although, it’s worth pointing out that hackers need only a healthy list of usernames, because as we will see in a moment, they can use other means to break through a password.

Social Engineering

Phishing is an example of social engineering. As such, social engineering seeks to use clever tactics in order to extract as much information as possible from potential victims. That is why all users need to take care with sensitive information in all means of online interaction. For example, hackers may be circling the water on social media, looking for unsuspecting prey to pounce on. If you are getting visions of sharks swimming about, then you are right on the money. The fact of the matter is that hackers will often pose as customer service agents pretending to help customers regain access to their accounts or open a new one. Even if the customer does not reveal all of their information, the hacker may get just enough to breach an account.

The saying, "if it's too good to be true, it probably is" still rings true when it comes to social engineering. So, always keep an eye out for any suspicious activity out there. If you are even in doubt, just stay away from suspicious users and websites.

Password hacking

Virtually every type of network requires two things to access it: a username and a password. Even if hackers happen to get their hands on your username, they still have to crack your password. This can be rather complex. Yet, you can make it easy for hackers if you don't pay close attention to the types of passwords you are using.

Currently, most sites and network protocols require passwords to have a combination of letters, numbers and special characters (@, #, & or *). In short, the longer your password is, the better. In fact, the best passwords make use of random characters and numbers. This makes it virtually impossible for password cracking software to get its hands on your password.

For instance, "happy" isn't exactly the safest password. It may take a password cracking software minutes to break it. However, a password like "H@ppy" is far more complex and may take password cracking software days to or even weeks before it is able to get anywhere. By then, the hacker will have given up and moved on to the next target.

If you happen to use a password generator software, please bear in mind that you will get a password of around 16 characters using random letters numbers and special characters. Perhaps the best piece of advice here is to make sure that your passwords don't have any type of logical connection to you. They need to be as random as possible. That way, you can ensure that your account will be as safe as it can be.

Packet sniffing

This is a complex endeavor, but if successful, a hacker can have access to potentially unlimited amounts of data. This requires the hacker to install software that can read the information traffic going through your network. If your information is not encrypted, then you are just a sitting duck. That is why most network routers come with their own built-in encryption. Furthermore, free webmail services also use their own encryption. That way, if a hacker happens to intercept your package, the only thing they will be able to get is meaningless gibberish. It may end up taking them week or months before they are able to even get close to breaking through the encryption. While it is not impossible, it will certainly deter hackers from wasting their time on your data.

Exploiting vulnerabilities

Nothing is perfect; and software is no exception. That is why the shark metaphor is so apt when it comes to hackers. They are consistently circling the water looking for backdoors, loopholes and other coding errors that may allow then access to a network. In fact, an entire industry has been built around hacking large corporations and then extorting them out of large sums of money. If the software you are using happens to have one such mistake, you might be vulnerable to an intrusion. These issues are generally addressed by software manufacturers and solved as promptly as possible. However, software manufacturers don’t generally become aware of the problem until someone’s network has been breached. Nevertheless, always be on the lookout for software updates and security patches. That way, you can improve the overall level of protection in your network.

Malware

This has got to be the most common means of granting unauthorized access to wrongdoers. Malware consists of a program that latches onto your computer files and opens a door for hackers to walk through. When installed, it may be very difficult to detect its presence. Most of time, you will pick up on it until it’s too late. The most common form of malware is a program commonly referred to as a virus.

Now, malware is completely ineffective unless one thing happens: the user needs to allow the malware package to enter their computer. This can be done through a download, inserting a pen drive or installing software. Often, malware poses as another type of software thereby tricking the user to open the file, installing the program or downloading the virus. In such cases, you can still kill the program from ruining your computer though you would have to kill it immediately. A good antivirus program will help keep you safe especially if you usually download information online.

The best thing you can do to protect yourself in this case is to avoid opening any email attachments, downloading software or installing anything that isn't from a trusted source or that might look fishy.

Denial of Service (ransomware)

Ransomware works in the same manner as malware does but with one particular twist: malware generally looks to snoop on your activity and steal information such as account numbers, passwords and usernames whereas ransomware will lock up your computer and deny you access to your network. What the hackers are after in this case is a payment in order to liberate your system and/or files. However, once you pay, there is no guarantee they won't try it again. If you should ever fall prey to a ransomware attack, you need to drastically overhaul your security settings. Otherwise, it will only be a matter of time before hackers try the same shenanigans again.

What can be done about these threats?
Fortunately, there is plenty which can be done to ensure the security of your network. We have already pointed out some of the best practices which you can implement as a part of your usual activity. Moreover, there are other measure which you can take so that you can avoid becoming a target of unwanted attacks.

Network Security Areas or Zones

In a perfect world, there would be a single solution to all of the threats we have outlined. However, engineers are yet to produce a one-size-fits-all solution. The main reason for this is that hackers like keeping up with the times, that is, as soon as a security measured is implemented, hackers are looking for a workaround.

That being said, let’s take a look at the various network areas, or zones, which comprise a typical network apparatus.

Logical Security Zones

The most common type of network is a small, home-based network. Typically, these networks consist of internet access coming from an ISP into a router installed in a customer’s home. Then, various devices are connected to this network in order to access the internet.

Now, in general terms, most home networks are relative safe given the type of security measures that come preinstalled with the equipment that the average user purchases. Unless users attempt to access the dark web or frequently download software from untrusted sources, then risks should be minimal.

There are two types of traffic that you will find in this type of setup, intranet traffic and internet traffic. Intranet traffic is all of the traffic that happens within the network itself. This traffic cannot be accessed by anyone that does not have access to the network. Unless the network is somehow compromised, the data contained within is rather bulletproof.

Internet traffic is any data that comes in or goes out of the network. This is where things get tricky. If care is not taken to encrypt data or restrict access, then the network may be compromised. One simple example of compromise could be removing your router’s password thereby leaving it as an open network. That means that anyone can access your network and even play with your router. This could lead to packet sniffing and interception of your data.

Therefore, great care needs to be taken to restrict the access to wireless data points. If you are not careful to restrict network access through the use of a username and password, you would be opening up the door to unwanted intruders.

Data security areas or zones

The next level of security is protecting the data itself. So, even if the network is comprised and subsequently breached by an unwanted intruder, the data package will be useless to them unless they are able to break the encryption. High-level encryption is virtually impossible to break. This can only be done through the use of the algorithm which was used to encrypt the data in the first place. So, unless the hacker actually has access to the algorithm, there is not much they can do to break it.

It should be noted that if the data is encrypted with a low-level algorithm, then there is a chance that a very clever hacker could break the code and subsequently crack into your data. However, sites and networks that use 128-bit encryption are essentially bulletproof as cracking through encryption that complex may take forever. Unless a hacker is somehow unusually determined to break through, they will give up when they see that breaking through may take them years to achieve.

Physical Access areas or zones

This is the next line of network security. It is also arguably the most important since a breach in the physical security of a network can lead to catastrophic results. This is the reason why you see armed guards at the door of server rooms, or at the entrance of building housing physical equipment.

While physical security doesn’t always need to go to such extremes, it is important to protect access to physical equipment. Often, the biggest breaches of security don’t occur as a result of hack, but rather, they are the work of an individual who gains access to physical computers and is able to download information into a pen drive or a CD. Some of the standard practices which many companies implement include disabling USB ports or disk drives. Also, restrictions on data transfer can be set in place such as the requirement of administrator passwords for file copying and accessing shared folders.

For the average user, adding password protection to a computer is often enough to keep snoops out. Also, logging out of a session on a shared computer is a great way to avoid unwanted access to file folders. One common mistake is allowing a web browser to save the password to your accounts on a shared computer. If someone figures out your username, all they need to do is enter it and the browser takes care of the rest.

Understanding access to data

One common practice is to assign levels of access to data. This means that certain data sets may have “open data” meaning that anyone within the organization, or with network access, may be able to see it. In other cases, the definition of open access may refer to certain information being of public domain. This kind of information can be downloaded from a website or accessed by request. This kind of information may lack encryption in order to facilitate access.

“Restricted data” refers to data which is not freely available to all users. Now, the definition of “restricted” is rather broad in the sense that it may only apply to users with network access, or it might be restricted to users with password access. This is commonly found in shared folders and cloud-based storage applications. These data sets may also have some kind of encryption attached to it thus limiting the abilities of unwanted users to read the information.

Lastly, “confidential data” is the type which contains sensitive information of an organization. In this type of data, there are extreme security measures attached to it including high-level encryption and password access. This type of data may also be stored in “secret” drives and folders which only a limited number of users have access to.

By understanding the tiers of sensitivity attached to data, you can take the appropriate measures that you need in order to protect your files and sensitive information. One such example “confidential data” could personal information belonging to customers while “open data” may be information about the products and services that a company offers to its customers.

Network security best practices

Here are the best practices which you can put into practice when looking to protect your data.

- Take control of physical access points such as USB and disk drives
- Don’t neglect password restrictions to any sensitive information, folders and drives
- Ensure that access to wireless networks is protected by password access while wired connections are accessible to only those users who have permission to use them

- Avoid the use of external pen drives, disks and any other media which has not been previously scanned or cleared
- The usage of high-level encryption will ensure that your data is bulletproof
- Avoid the exchange of information over open networks or hotspots; these could be prone to packet sniffing
- Shut down network access if there is a suspected network breach
- Update passwords regularly (once a month is a good rule of thumb)
- Discourage password sharing among co-workers
- It is better to spring a little extra for top-level encryption in order to ensure that confidential data is safe even if intercepted

On the whole, network security is a matter of ensuring that you have the proper procedures in place. Also, it is important to have a clear idea of what to do in case of a data or security breach. Most firewall and antivirus programs will offer functionalities that will alert you of coming from an unknown source. In general terms, these alerts happen in real time. Consequently, you will have the opportunity to promptly shut down any potential attacks on your network

Chapter 9: Wireless Technology and Security

Fully functional wireless networks and devices seemed like a dream a decade ago. In fact, many experts in the field did not believe that that entire computer networks could be run on wireless connections. Yet, the dependence on wired connections has been drastically reduced over the last few years. Nowadays, a great deal of networks are run on wireless connections. For instance, cellphone communications are run entirely on wireless communications. Everything from calls to internet access; there is no need for any wired connections.

In a nutshell, a wireless network is connection among devices which does not require the use of cables to connect the devices, either to the network or amongst themselves. In that sense, wireless networks offer a high degree of flexibility and simplicity as the physical limitations of having to install large amounts of wires and cabling is not needed. In addition, the network can span over longer distances and does not demand that users be physically present in a given location in order to gain access to the network.

At present, wireless networks have simplified both access and mobility. Users can be on the move constantly and not miss a beat. This has enabled a multitude of users to experience new ways of communicating especially when moving away for long distances. Indeed, wireless technology has revolutionized the way we interact with the world around us.

However, the use of wireless connections has also opened up a new set of threats and considerations which need to be taken into account. In general, wireless access requires both providers and users to exercise increased security practices. This is a stark contrast to a traditional wired connection.

With wired connections, unauthorized users needed to have access to both a physical terminal and a port to connect to. This means that breaking into the network itself was a rather complex task. Of course, an authorized user could perform a remote hack by gaining access through the use of a username and password. But most times, there had to be someone physically present in order to gain access to the network itself.

This aspect of wired networks is lost in wireless communications. Anyone within range of the Wi-Fi signal can potentially gain access to the network. This is why free Wi-Fi hotspots can become so unsafe for the average user. The fact of the matter is that anyone can gain access to the network especially if it lacks encryption or the use of authentication.

As a result, security experts advocate the use of authentication either by means of a username and password, or a captive portal in the case of hotspots. Furthermore, encryption is highly recommended in order to avoid potential loss of information due to a package interception. With that in mind, most home networks are rather safe, that is, a typical residential network that provides wireless internet access to a group of devices is rather safe from unwanted users. Yet, there is always the risk of someone being on the prowl looking to find a vulnerable network.

In the case of business networks, wireless access needs to offer a greater degree of security. In many cases, enterprises deal with sensitive and confidential information. What this means is that networks administrators need to ensure that unwanted users stay as far away as possible. Still, employees need to gain access to the network so that they can perform their day to day functions. With this in mind, awareness of the need to protect access to such connections truly becomes of the utmost importance.

What to consider when setting up a wireless connection

First and foremost, security is the biggest concern for wireless networks. In a world in which information is power, having access to information is a valuable commodity. As such, the question of security boils down to access to information and not access to the network itself. This means that the biggest concern in the mind of network administrators is not that unwanted users log on to the network; their biggest concern is that by logging on to the network, unwanted users will be privy to potentially sensitive information.

In that regard, restricting access to unwanted users in the number one priority for network administrators. Simple measures such as making sure that all users have a username and password is often enough to stifle the average hacker.

The next item that network administrators look to when setting up their wireless networks is simplicity. Simplicity implies the ease with which users can log on to the network and then use it to complete their objectives. With that in mind, administrators need to consider the bandwidth that will be required in order to accommodate the number of users on that particular network.

Often, it is easy to underestimate the requisite bandwidth. In fact, it is quite common for an administrator to estimate a given bandwidth and then realize that it is not enough to handle a full load. Other times, an administrator might make an appropriate assessment of the bandwidth that is required for the current load of users but does not take into account future users. Therefore, it is essential that an administrator consider both present and future bandwidth requirements.

Another important aspect to consider is the actual, physical infrastructure that is needed to produce the wireless network or provide Wi-Fi access to users. This physical infrastructure comes in the way of routers and signal extenders. The most challenging part of the physical infrastructure is directing the signal to where users will be. This can be a potential headache when homes and buildings are designed in a free-flowing style. Wi-Fi signal can often get stuck going around corners or up and down stairs. Even concrete buildings can absorb the signal rather reflect to the devices that will connect.

One other key consideration when setting up a wireless network is understanding the devices that will connect to it. For example, if the network will mainly consist of smartphones and tablets, then a larger number of devices can be accommodated on to the network. In contrast, if a large number of PCs (which tend to be hungrier for bandwidth) connect to the network, then arrangements need to be made in order to accommodate the larger number of devices.

On the whole, setting up a wireless network is far easier than a standard wired connection. The configuration of software is less complex while there is a definite savings in terms of money; there are far fewer components to purchase and cabling that needs to be installed.

So, if you are looking to set up a network that won’t break the bank and will allow multiple users to long on easily, then a wireless network can certainly fulfill those needs.

Drawbacks of a wireless network

For all its merits, a wireless network also poses a series of drawbacks that need to be taken into account. For starters, Wi-Fi access is far less reliable than wired access. The main reason for this is that signal strength on wireless networks fluctuates a lot more on wireless connections than it does on wired connections. In fact, there are many factors which can influence the quality of a wireless connection’s signal strength. Factors such as the weather or interference from other devices (phones, TVs and radios) may play into reducing the quality of a wireless signal. As a result, close monitoring of signal quality is essential in order to ensure proper functioning of the network.

Another drawback is the connection’s speed. Generally speaking, a wired connection will always run a lot faster than a wireless one. The reason for this is that a Wi-Fi signal can disperse throughout the environment where it is located. In the case of a wired connection, it has nowhere else to go, but the cable where it is being transmitted. This is what makes wired connections a lot more reliable and faster than wireless ones.

Also, wireless connections are dependent on the wireless adapter used by the devices that are connecting to the network. So, even if the network is reliable and free from obstructions, devices that do not have a solid and functional wireless adapter may actually experience decreased performance. Therefore, it is important to ensure that the devices connecting to the network have the best available wireless hardware.

As you can see, wireless networks, even with their drawbacks, offer a serviceable solution to virtually all residential users and most enterprises. Ultimately, the network administrator, or home user, needs to determine if the characteristics of a wireless network meets their needs, or if a wired network might be more suitable. Yet, wireless networks offer a good solution across the board.

Types of wireless networks and connections

Thus far, we have focused on wireless networks under the assumption that the network is designed to connect to the internet. This assumption is valid since the vast majority of networks will require some kind of internet access at some point. Most of the time, the reason for the network is so that it can connect to the internet.

Yet, there are other types of wireless connections which devices can use to communicate among each other.

To start off, Bluetooth is a common tool used to connect a small number of devices together. Usually, it consists two devices which are paired with each other. A common example of this wireless headphones connected to a smartphone. Also, a printer can connect to a computer or a phone may synch with a computer and so on.

Bluetooth is far slower than other types of wireless communication. Yet, it is useful for linking devices which aren’t too far apart. Perhaps the biggest drawback is security as Bluetooth connections don’t have much in the way of encryption to speak of. So, a skilled hacker may be able to connect to a device which happens to have Bluetooth enabled.

Beyond a run-of-the-mill Bluetooth connection, wireless networks can be rather simple and straightforward, or they can get rather complex.

A Wireless Local Area Network (WLAN) can be set up to enable communication among a small number of computers with or without access to the internet. In most cases, WLANs will have some form of access to the internet. Although, very confidential connections may be confined to a small workgroup using a WLAN without necessarily having access to the internet. In fact, there may be a separate WLAN that does have internet access. That way, the risk of a security breach can be limited. This type of connection can be limited to a home, individual office or perhaps an entire building.

The next level is a Wireless Wide Area Network (WWAN). In this type of network, there is a much larger area to be covered. If the physical area exceeds the usual range of a wireless network, internet access may be required in order to join multiple connections. This type of connection can be used to link larger geographical areas such as several city blocks.

A larger type of network is known as a Wireless Metropolitan Area Network (WMAN). This is the kind of network which can be used to link an entire city. Unless there are several repeater points that can distribute the signal over large physical areas, the most effective way to connect devices over a large area is to link them over the internet. In that case, any number of users can log on to the network as the need may be.

WMANs are used to connect entire cities. These are the types of networks which are used by large organizations. For instance, companies with several locations spread out over a city may rely on this type of configuration to help them manage communication among all of their users. These networks are also commonly used for commercial purposes such as advertising and broadcasting information.

One important factor that all of these connections have in common is that there is a central hub from which the signal is generated. This hub then sends out the signal to the various devices that will connect to it. Also, repeaters and signal extenders may be used in order to ensure that the signal covers the entire physical space that the administrator is looking to grant access.

Based on this logic, an ad-hoc connection is one that is set up without any kind of planning. For example, a laptop computer uses Bluetooth to connect a wireless printer and a smartphone. Then, the network will be disbanded once the tasks are complete. Another good example is when a smartphone is used as a wireless hotspot. In this case, the phone enables various devices to connect to it and thereby access the internet. Once the need for internet access is gone, then the network is disbanded.

As you can see, an ad-hoc network serves a very specific purpose and then when it is no longer required, it disappears. Experienced users are good at building ad-hoc networks from scratch, either to help them when they are in a tough spot, or as means of streamlining work.

Lastly, a hybrid connection is the kind which combines both wired and wireless access. This kind of network is commonly seen in enterprise settings. This type of network addresses all of the needs of a company in that wired connections are generally used for desktop PCs while wireless connections are used for laptops and mobile devices.

Furthermore, a hybrid network offers a combination of mobility and security. Secure connections can be achieved on the wired connection while the wireless network can provide mobility to users. Since wireless connections tend to be less reliable than wired ones, the most sensitive tasks and information is carried out over the wired connection leaving less complex and sensitive tasks to the wireless network.

Other uses of wireless technology

In the past, more rudimentary wireless technology such as shortwave radios provided the opportunity to connect over certain distances especially when traditional broadcasting was unavailable. To this day, shortwave radios are essentially used by emergency broadcast systems and aficionados. However, this type of technology is still seen in law enforcement and emergency crews. While shortwave technology does not have a great deal of range, it is often enough to cover larger areas such as a medium-sized city.

Also, traditional radio communications are a great alternative since they provide users with the ability to connect without having the need for an expensive setup. With that in mind, user don’t have to rely on the internet or even electrical energy to communicate.

As a matter of fact, military grade radios use solar powered cells to recharge batteries. This enables military units to remain operational for extended periods of time especially when deployed in battle. These types of radios are also used in marine communications as well as airborne surveillance.

In addition, companies that have a great deal of moving parts use radios to communicate among its various parts. Trucking companies, factories and warehouses all use some type of radio communication to stay in the loop. Hospitals and emergency services utilize radio communications as a means of ensuring capabilities.

Radio technology has also been applied to what is now known as Radio Frequency Identification (RFID). This type of technology is used as a wireless network mainly deployed to identify and track units such as people, animals and vehicles. It is commonly used by trucking and cab companies to keep tabs on their vehicles. Additionally, researchers use RFID to track animals in the wild.

There are two parts to an RFID system, an emitter and a receiver. The emitter, or transmitter, sends out a radio frequency that is picked up by the receiver. The receiver can then translate that signal into a digital signal which can be utilized to track movements on a map or pinpoint the location of a unit. This system has been deployed in search and rescue operations as well as scientific research.

Some critics of RFID claim that it is used to illegally surveil individuals. However, there is not conclusive evidence of its use outside of tracking people and objects for legitimate purposes. For example, people who are under house arrest that must wear an ankle bracelet have an RFID system attached to them. This allows law enforcement to determine their position in case they choose to flee.

One other interesting application of wireless technology can be seen in satellite communications. Traditional cellular telephony makes use of the Global System for Mobile (GSM) network. This network uses a SIM card with a unique ID on it to identify a mobile phone’s number. This enables the mobile phone to place calls and have access to the internet.

However, in the case of a satellite communication, mobile receivers and transmitters don’t necessarily use the traditional GSM network. In fact, they may bypass this system altogether and connect to any of the other communications satellites in the Earth’s orbit. These so-called satellite phones have coverage in virtually all corners of the Earth.

One great example of this kind of communications is military satcom. Harris radios, for instance, use UHF and VHF frequencies to communicate among aircraft and seaborne vessels. Ultra-high frequency (UHF) and Very High Frequency (VHF), can be used to triangulate communication between an airborne vessel and a ground crew. Given the advancements in this type of technology, air crews can send live video in HD to ground crews who can then assess a situation as seen from the aircraft.

This type of technology has been widely employed for aerial reconnaissance, for example in border protection, as well as, search and rescue and disaster relief. There is also a weather application for the use of the technology through the use of Unmanned Aerial Vehicles (UAV). These types of vehicles can track weather patterns to a point where a manned crew would never be able to reach. All of the communications are relayed from the aircraft up to the satellite and then broadcast back down to the ground crew. Likewise, the ground crew can then communicate with the aircraft in mid-flight.

These examples all show how wireless communications have a plethora of applications. There ensure that communication does not breakdown and can be maintained over vast areas of physical space. While the more robust capabilities of such wireless communication is reserved for the domain of military and law enforcement, civilian applications have led to the mapping of remote areas of the planet and the discovery of previously unknown features of the Earth.

One of the most common issues that arises when discussing UHF and VHF communications is encryption. It should be noted that these types of networks use military-grade encryption meaning that it uses the most robust algorithms known to date. These algorithms are essentially impossible to crack since they would require a vast amount of computing power that the average hacker would never be able to procure.

If you are keen on using these types of communication networks, there are civilian versions of satellite phones which can be purchased freely. They come with a subscription that grants access to the network of satellites that orbit the Earth. They are essentially the same satellites that the military uses. However, you would not have access to the same channels and frequencies that the military does.

The Global Positioning System

The Global Positioning System (GPS) is essentially a wireless network that is used as a navigation aid. It is used in all types of transportation. In fact, it is so common nowadays, that most smartphones come equipped with a GPS application that enables users to pinpoint any location on the planet.

One great example of such application is Google Maps. This application can help drivers navigate practically any city in the world with frightening accuracy. Technically, this application does not need internet access since it uses its satellite link and not its internet signal. Yet, the application does not function appropriately since it uses an internet connection to download maps for its current location. What this means is that your phone determines your location by using the GPS network, but needs internet access to download the map for that location.

Google Street View is an example of how accurate satellite mapping can be. The satellite orbiting the Earth can literally take pictures of an average street while it is hundreds of miles above. This is certainly an incredible and very useful feature.

The GPS system uses the same system as satcom or GSM technology. It essentially works in a triangulation system, that is, the satellite, the receiver and the tower. This triangulation is what enables the pinpointing of precise locations.

In the case of marine applications in which there are no towers in the middle of the ocean, GPS can maintain triangulation by using other satellites in orbit. This is why military applications of the GPS system enable units to navigate any corner of the world. For the average user though, GPS is a lifesaver when driving in a new city or through an unknown path.

Bringing it all together

Wireless networks are here to stay. They make linking devices, and by extension users, a lot easier than through traditional wired connections. For all of the ease of use and mobility, questions about the overall reliability of wireless networks still abound. The fact of the matter is that this is technology which is yet to be perfected. What this means is that there are bugs still to be worked out.

As far as the average user is concerned, wireless has come a long way. Most cell carriers have a decent record of reliability. So, unless there is a natural disaster that disrupts coverage, wireless networks are usually reliable.

The other aspect to wireless networks is security. High-level encryption has increased information security tremendously over the last few years. In fact, standard encryption as offered by free web-based email servers is good enough to keep the average intruder away from your information. There are more robust subscription services out there which offer closet to military-grade encryption. These services are commonly used by companies and individuals who handle a great deal of sensitive information. On the whole, wireless technology is easy to use and very flexible. It will certainly meet the needs of the average user while enabling more advanced users to get their job done. By following the security guidelines which we have outlined earlier in this book, you can rest assured that your information will be safe from the attacks of unscrupulous folks. After all, hackers love to feed off low hanging fruit. They generally run away from a serious challenge. Thus, you can make it hard for them by beefing up your security measures.

Chapter 10: Introduction to Machine Learning: A Computer Networking Perspective

What is Machine Learning?

The above analogy is merely intended to draw our attention to the primary topic issue that concerns this study session: machine learning.

Can computers really learn? Better still, can they learn from their experiences with the different tasks that they handle on a day-to-day basis? Machine learning is a discipline that can sufficiently provide answers to the above questions.

In a layman's language, machine learning can be described as a process of acquiring skills that have been accumulated over time through observation. We can deduct from this simple description that machine learning starts by observation. The observation goes for a certain period.

In the process of observing, skills are acquired while others are sharpened even further-learning from experience. This is one example of a normal human's learning throughout their time here on planet earth.

A more concrete definition of machine does exist. Let's say that machine is a process that involves the acquisition of specialized skill(s) computed/accumulated from data over a period of time. Still, this sounds like we’re talking about humans.

But we need to talk about machine learning in terms of machine ‘behavior’, and more specifically, as regards computers.

In Computing Terms

Machine learning is classified as a subset of Artificial Intelligence. As a subset of Artificial Intelligence, machine learning entails the development of algorithms that enable computers to learn from accumulated data and functions performed in the past. This concept was conceived in 1959 by Arthur Samuel.

Sample historical data (training data) offer a basis for machine learning algorithms to deliver models that aid in decision-making as well as predictions. This is done without any explicit programming.

Creative predictive models are products of the union between statistics and computer science.

How Machine Learning Works

Machine learning system achieves its mandate by following the following steps:

- Thorough examination of (or learning from) historical data that has accumulated over a given period.
- Building of prediction models.
- Prediction of output (on reception of new data).

The amount of data largely determines how accurate the predicted output turns out to be. A huge sample of historical is necessary for creating better prediction models that guarantee high accuracy of predicted output.

Features of Machine Learning

The following are the main characteristics of Machine Learning:

- The use of data for pattern detection in datasets.
- Automatic improvement after learning from historical data.

- Machine learning is technologically data driven.
- It has appreciable similarities with data mining-dealing with huge data amounts.

Why Machine Learning?

There is a day-by-day increase in the need for machine learning. One key factor for embracing machine learning with unimaginable seriousness as it is now, obviously, is the ability of machines to handle tasks that are highly sophisticated; better than humans. We can read, understand and interpret data, but we are only limited to a few megabytes of data. Machines can handle terabytes of data, or even more, with a lot of accuracy.

With machine learning, the world can now boast of self-driven cars. Friend suggestion on social media platforms is also real, thanks to machine learning. Furthermore, face recognition, among other big advancements, are outcomes after big strides in machine learning.

In summary, the need for machine learning is anchored on the following key observations:

- Increment and rapid production of data, in respect of the widespread adoption of information systems.
- Handling highly sophisticated tasks that are practically impossible to a human being.
- Critical decision-making needs with regards to large and complex data or information. For instance, in finance and economics projections for individual businesses, companies and even governments.
- Extracting patterns and information that are not easily visible to the human eye

Classification of machine learning

Machine learning is classified as follows:

Reinforcement learning: this is a feedback-based mode of learning. A learning agent (machine) is penalized for every wrong pattern prediction and undesirable outcome. On the other hand, the same learning agent (machine) is rewarded for a job well done.

Unsupervised learning: a machine trains on outcome prediction without any supervision. Given data sets are not labeled, but the machine has to learn and eventually predict an outcome. Unsupervised machine learning is categorized into clustering and association.

Supervised learning: labeled data is provided to a machine. The machine is trains on pattern prediction therefrom and eventually gives a prediction on that basis.

There are two categories of supervised learning: classification and regression.

Machine Learning Applications

Machine learning is a crucial to each and every sector be it economic, social or administrative sector. Thus, the application of machine learning can be summarized under the following three key areas:

Machine Learning in Analytics

Statistics is every aspect of life. Sometimes we use it without knowing that we're actually using it. For instance, a person who wonders about a terrible experience would expectedly learn from it and take a totally different course of action given similar circumstances. Knowingly or otherwise, the person assesses the different events leading to a particularly horrible incident against what would have led to a different turn of events. The process may seem straightforward, but the truth is there is a lot of analytical work happening in the busy mind of the victim.

In normal life, politics invest so much in statistics to gauge the popularity of political candidates and help in making crucial political decisions. Similarly, all sectors use statistical results based on historical data to predict various events in the future.

Machine learning takes up this whole business to a whole new level by eliminating so much of human effort by merely allowing algorithms to analyze data and offer prediction of patterns and likely outcome based on accumulated data.

Machine Learning in Management

Management rely heavily on statistical data in decision-making. In business, the management is charged with the responsibility of making decision regarding employ recruitment and laying off; employ remunerations; budgetary projections; and the structure of leadership within a given organization or institution. In formal settings, such decisions are not arrived at hastily, or without thought. In most cases, it takes months or even years to analyze relevant masses of data before deciding what is good for the organization or institution. With machine learning, the analysis of such data is more efficient since machines have the ability to handle huge data amounts that would otherwise take years to be done by a human. In fact, some analytical work is way beyond the ability of the smartest man on earth.

Machine Learning in Security

Security has been enhanced greatly with the adoption of machine learning systems. CCTV cameras, metal detectors, security alarms and other security devices are perfect examples of machine learning in use. For instance, face recognition services are particularly important in ATM machines since they massively add to the security of ATM centers.

In summary, machine learning is an important subset of artificial intelligence; especially during the present times when we have to deal with a lot of data and information as a result of the information systems euphoria. Healthcare, financial sector, education sector and, and governments need statistical data to make crucial decisions for sustainable operations. With machine learning, such needs can be met more efficiently.

Conclusion

A computer network can comprise of two computers. As long as the computers are connected, can communicate and share resources, the network is complete. However, there is no limit as far as the number of networked computers. The internet is a perfect example of how big a network can be.

Resource sharing and communication are the two biggest functions of a network. But that does not mean there is not much beyond communication and sharing of resources on computer. In fact, many people make connections to the internet merely for entertainment. Others get linked to networks for collaborative work, research and many other tasks.

Networks, notably, do not comprise of computers alone. There are a lot of more other network components that make computer much more interesting. Printers, cables, routers and many other hardware devices add to computer networks' collection of important hardware requirements. Besides, software applications and network protocols all gang up to make computer networks what they really are.

As important as computer networks are, running and managing them is never a walk in the park. Network security is one concern that gives concerned network users and administrators sleepless nights. Networks attacks are real, and they pose serious threats to the security and safety of user information as well as network resources. Being in position to deal with network threats effectively is key maintaining the integrity of the network.

In summary, computer networks are invaluable assets that must be guarded keenly. They make communication more effective besides offering a platform for many other important functions. In this IT-oriented era, computer networking is the key to effective communication, research and collaboration.