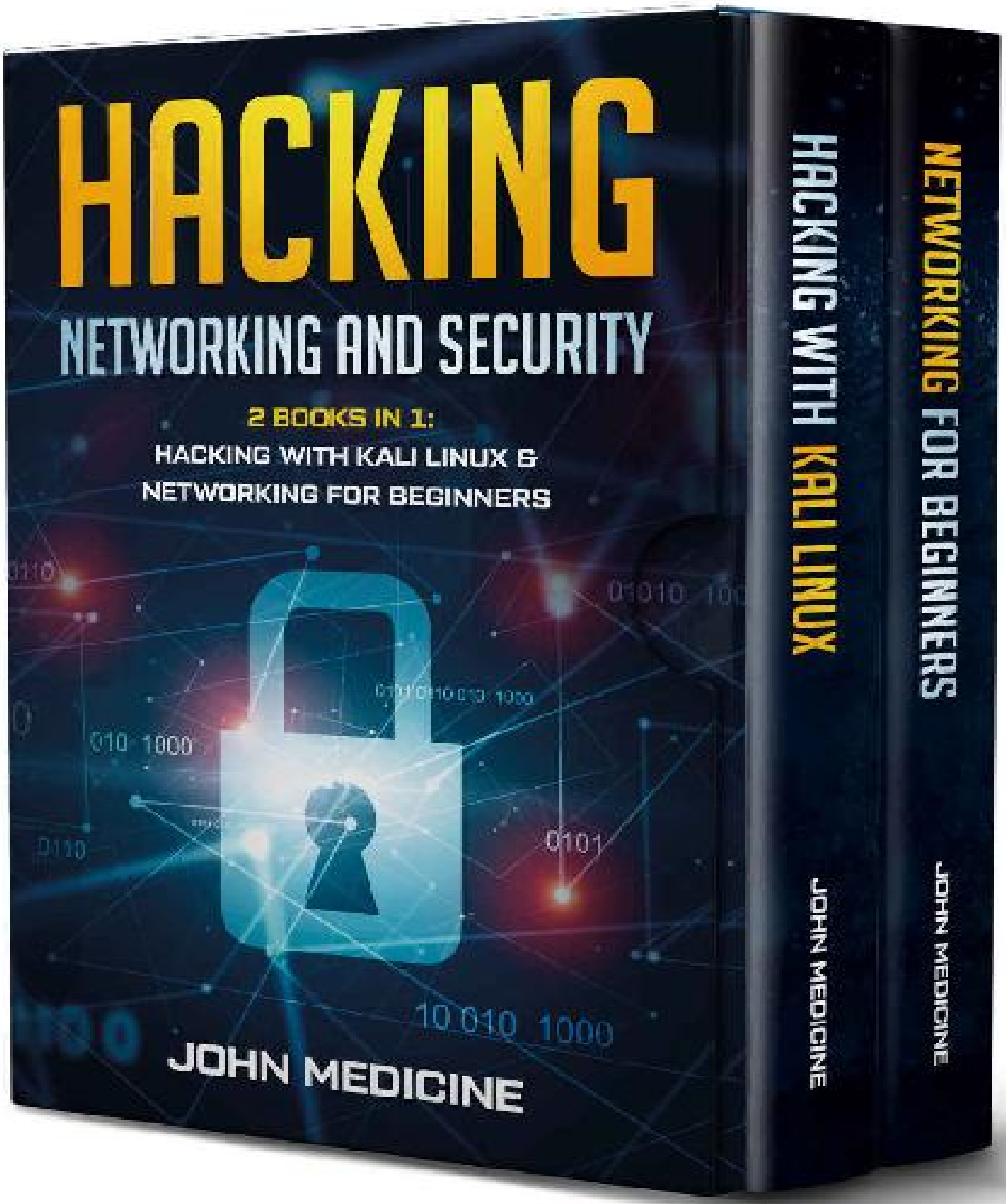

HACKING
NETWORKING AND SECURITY
2 BOOKS IN 1:
HACKING WITH KALI LINUX &
NETWORKING FOR BEGINNERS
JOHN MEDICINE
HACKING WITH KALI LINUX
JOHN MEDICINE
NETWORKING FOR BEGINNERS
JOHN MEDICINE

Hacking

Networking and Security
2 Books in 1
Hacking with Kali Linux & Networking
for Beginners

John Medicine

Table of Contents

Networking for Beginners:

The Complete Guide to Computer Network Basics, Wireless Technology and Network Security

John Medicine

Introduction

Congratulations on downloading your eBook copy of the *Networking for Beginners*. I am very much delighted that you all have shown so much interest in learning about the basics of networking and the functioning of each and every component of the same. Networking can also be regarded as the main component of every organization as without proper networking it is not possible to set up a proper business.

Networking is the technique which is used for transferring various forms of data from one end to another with the use of intermediary systems. Networking is not only about the design, use or construction of its structure. It also comes with management, operation and maintenance of each and every component that builds up the network. It can also be said that a properly structured network can help in transferring data and information in lightning speed from one system to another. Networking allows various devices and systems to be connected with each other via various networking systems that you will learn more about in this eBook. The various components of networking make it possible for the human world to send uninterrupted messages from any corner of the world. Not only that but with the various types of networking, the organizations can server their function in a better way.

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

Chapter 1: Logic of Computer Networking

In this world of today, where nothing is possible without the touch of technology in it, computer networking is also such a thing without which setting up an organization or business cannot be imagined at all. It helps in connecting various related devices to the endpoints with the help of various networking systems. Networking serves a very essential function for all the service providers, consumers and businesses all over the world for the purpose of sharing, using and offering various services and also for communicating at the same time. Networking comes with everything, from text messages to telephone calling and ending with video streaming and IoT. Network operation requires some serious skills that depend completely on the network complexity. For instance, in a very large enterprise, it might have millions of nodes along with several other requirements of network security like encryption, administrator functioning and many more.

On the other side, a normal person who uses internet and networking daily at his home can easily set up along with troubleshooting of various basic problems in the wireless network at their home. Both the examples given require the basics of networking to some extent.

Computer Network Basics

For understanding the prime functioning and components of networking, you need to learn about the basics first. A computer network is made up of various components that help in its overall functioning. Let's have a look at the basics of networking.

Networking and its types

Computer networking can be divided into two different types: wired network and wireless network. In the case of a wired network, it needs a physical medium for the purpose of transporting information between the nodes. For the purpose of digital communication in homes and in businesses, Ethernet cables are used for its durability and low cost as well. Optical fiber is also being now for data transportation to great distances and also at a much faster speed. However, whenever it comes to costing, Ethernet cables are much more cheaper than optical fibers.

In wireless networking, the radio waves are used for transporting data around the air in which the devices in the network are connected with each other without any form of cables in between. WLAN or wireless LAN is the most widely used and well-known version which is used for wireless networking. There are also several alternatives in the market today such as satellite, Bluetooth, microwave, cellular any many more.

It has been found that when it comes to networking, wired networking provides better speed, security along with reliability when it is compared with wireless form of networking. However, wireless networking provides much more mobility, scalability and flexibility that wired networking.

Wired and wireless networking is classified according to the networking physical layer. However, networking can also be differentiated in accordance with the design and built of the network, approaches of encompassing like SDN or overlay network. It can also be classified according to the scale, environment like campus, LAN, WAN, storage area network, data center network and many more.

Types of networking systems

There are two types of networking system: open and closed. In an open system, the system is connected with the network and is also ready for communication. However, in the case of a closed system, the system is not linked with the network and it is not possible to connect with the same.

Networking components

Computer networking comes with the requirement of the infrastructure of physical network. It includes various components such as routers, switches, access points along with the basic firmware which will help in operating the other components. When it comes to the other components, it includes the necessary software for the purpose of monitoring, securing and managing the network. All forms of networking rely largely on the standards of protocols for performing uniformly various discrete jobs or for communicating with various types of data. Protocol is nothing but a set of algorithms or rules which helps in defining the various ways in which two different entities communicate with each other across a network.

There are various types of protocols that can be found within a network such as IP, ARP, DHCP, TCP, FTP and many more.

VoIP or voice over IP is used for the transportation of IP telephonic traffic to the endpoint which also supports the protocol. TCP/IP is known as the internet protocol suite which is responsible for data transportation over a network based on IP.

An IP address is the logical address which acts as the network address for the systems in a network. It helps in creating a unique identification for all the devices across the network. The IP addresses are in 32 bits. IANA or Internet Assigned Numbers Authority assigns a unique IPV4 for each and every system or device in a network.

MAC address is regarded as the physical address for every host in a network. It is linked with the NIC or network interface card. The MAC addresses can be found in 48 bits or 6 bytes or 12 nibble. Each MAC address is assigned to the system NIC while manufacturing of the system or device.

Chapter 2: Internet Communication

The world today has completely changed from which it was a few years back. It is changing every day. With the advancement of digital technology, the pace of change has also become very fast. There were times when a simple message used to take a few months to deliver and now it takes just a few seconds. Internet communication has evolved so much that it can now connect people seamlessly from every corner of the world.

Internet Communication

Internet communication is a very simple thing. It is the sharing of ideas, information or just mere words over the internet or World Wide Web. Internet is composed of a huge string of worldwide connected networks which helps in exchanging information and data with the help of packet switching by using the TCP/IP.

Internet communication comes with a bunch of advantages that can help us in a lot of ways.

Internet communication and its advantages

Communication system on the internet comes with more number of advantages than disadvantages. For a business person, he/she can be at the

comfort their home, drinking tea or coffee and having a conference call with the clients as well at the same time. It can help in saving a lot of time, money along with growth in business.

- **Versatility:** Internet communication is versatile in nature. It is available 24*7. Internet communication will keep on working as long as you are connected with the web. Internet communication can also be regarded as a boon for the businesses, especially at the time of emergency incidents such as in the sector of social media advertising, bad publicity of even one second can lead to a disaster. In such case, internet communication helps in mending it all up.
- **Leveling:** It is a fact that everyone cannot in front of everybody at once. Also, there are many people around us who do not like to talk that much. Such people always love to express their feeling by writing. Some people feel more comfortable while talking from behind the keyboards. In that case, internet communication helps in building up a communication line for such people.
- **Well documented:** Face to face communication is not much documented whereas, internet communication is well documented. It helps in various situations especially when people need to be accounted for the words they speak. Thus, internet communication helps in establishing a very responsible environment.
- **Fast communication:** Internet communication is fast. It transfers messages in blazing fast speed that makes it possible

to send out messages at the time of emergency.

Tools for internet communication

Internet communication has provided the human world with a wide range of tools for the purpose 0f communication. Let's have a look at them.

Email

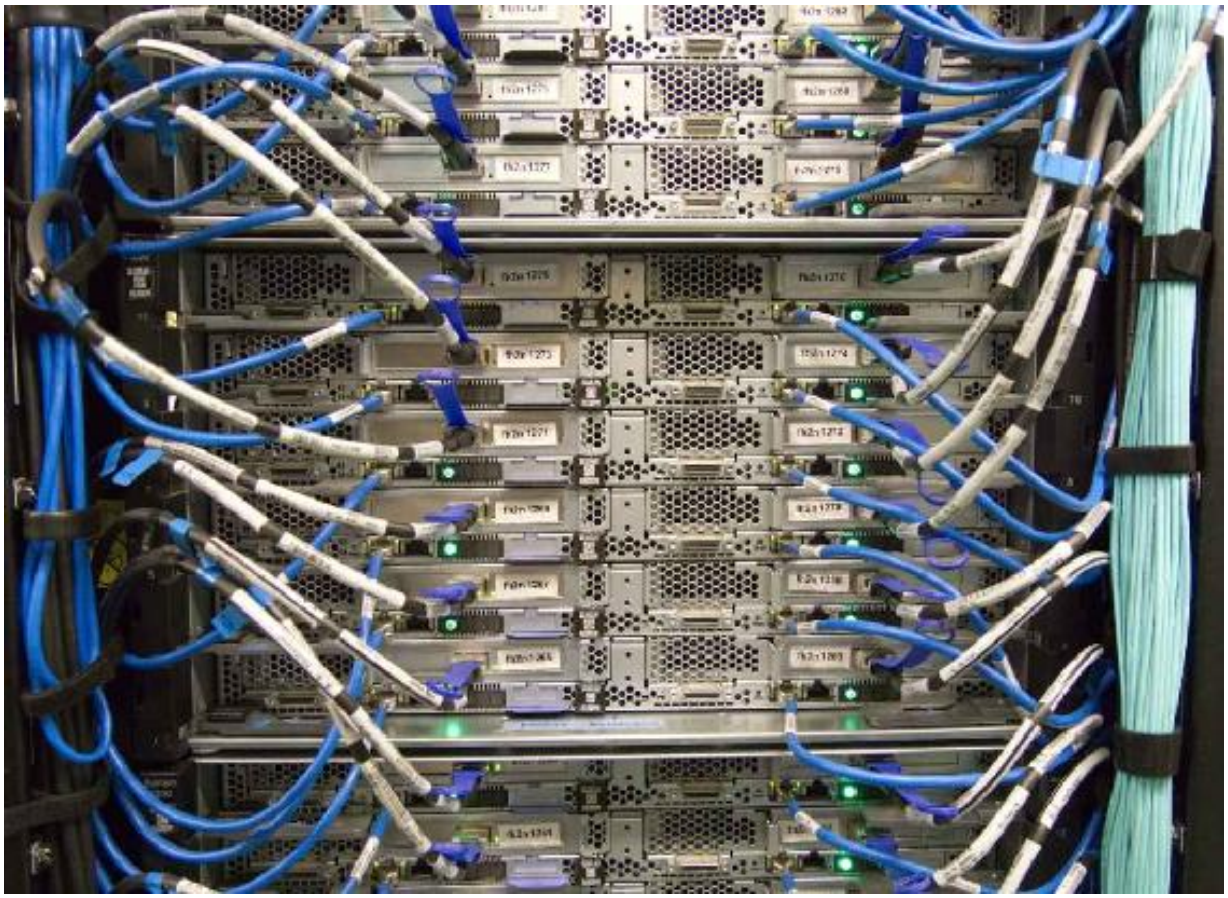
Email is regarded as one of the fundamental tools for internet communication. Today, email addresses are required in almost all forms of services today and it is also believed that everyone who is active on the internet has at least one single email address. Email addresses can be taken from various free services such as Google and Microsoft. Email is most widely used for the purpose of sending out official or confidential information. However, in this world of today, it is also being used for various harmful activities such as spreading malware or scams with the use of phishing emails. In the case of phishing, a third party tricks the victim into sharing his/her sensitive data such as bank or credit card details, account numbers etc. So, it is always better to be a little cautious while fetching any form of email from unrecognized sources.

Social media

One of the trending tools of today, it is being used for seamlessly connecting millions of people from all over the world without any kind of delay in transmitting the messages. It is also being used for spreading awareness or alert in case of any emergency situation, share important information with anyone you want and many more. But, the case of fraudsters in social media today is increasing day by day. Also, social media is used for spreading various information which is being used by the fraudsters at times for spreading hoax.

World Wide Web

World Wide Web is the most dominant form for internet communication. It is being used for everything, starting from online shopping to checking out the weather. It also helps in communicating online such as using digital messaging board or email. The users need to have a web browser in order to access the web. There are various types of browsers available today both for computers and smart devices. Each website is built with the use of HTML which is the website language, CSS which defines each and every element on the screen and JavaScript which is used for processing of data and also provides logic for programming. Every other form of internet communication such as VoIP or voice over internet protocol also relies on the web. VoIP helps in internet-based systems of calling. Using VoIP systems is regarded to be much cheaper as well as faster than traditional mobile phones. It also allows international calls with no form of delay in transmission.



Chapter 3: Client-Server Approach

The client-server approach is the architecture of computer networking in which various clients or the remote processors requests for a service and receives the same from the host or server computer. The computers of the clients come with an interface for the purpose of allowing the user of a computer for requesting various services from a server and then display the requested result which is returned by the server. All the servers in a network wait for the arrival of the requests from the clients and then only respond to each of the requests. Generally, a network server comes with a transparent standardized interface for the clients so that all the clients are aware of the system specifications such as software and hardware which is responsible for providing the services.

The clients typically are on their PCs or at their workstations and the servers are located right on the network i.e. on much powerful systems than the clients. The client-server approach is the most effective when both the server and the clients have some specific job to perform regularly. For example, in data processing of hospitals, the computer which acts as the client system runs a program for entering all the patient information and the server system helps in managing the patient database in which all form of information is stored permanently. All the clients on the network can access the information which is given out by the server and the client system can also perform various other jobs like sending out emails.

Both the client and the server in the networking approach are regarded as intelligent devices. So, the client-server model is also completely different and much more advanced than the old model of mainframe in which the

central server computer used to perform all jobs for all the terminals in a network.

Components of the client-server model

The client-server model works with three components: servers, network devices and workstations. Workstations in a network are those computers which are subordinate to the servers. Workstation sends out various requests to the servers for accessing the shared files, programs, databases and files. It is governed by the server policies. The server in a network serves all the requests that come from the workstations and can also perform several other functions like management of the programs, files, databases along with the policies of management. Network devices in a network help in establishing communication between the servers and the workstations. In simple words, the network devices act as the connectors and also routes the data in and out from the network.

Workstations

Workstations, also known as client computers, are the ones which send out requests to the servers. They are differentiated by the OS which runs their systems. In a network of client-server, Windows XP, Windows 7, Windows 10, Linux etc. are the OS of the workstations. As these OS are cheaper than the OS of servers, the processes and functions of such OS are intended for the client computers or workstations only. Shared programs, policies of security and management and centralized databases are not part

of the OS. They come with a localized version of policies programs and databases. The workstations come with a lower level of technical specifications when compared with the servers in respect to processor speed, memory and space of hard drive as the client systems are not required to record any form of data or process any request like the server system.

Servers

Servers are differentiated from each other by their individual sets of OS such as Windows 2003, Windows 2008 or Windows 2000 server. When it comes to the servers, they come with faster speed of processing, higher hard drive space along with more memory. It is mainly because the servers stores up various forms of data and also services multiple workstation requests simultaneously. A server can perform any type of role within a client-server network. It can act as the mail server, file server, domain controller and database server at the same time. However, for a network which is well-setup always divides all these roles among all the available servers for optimizing the network performance. But, no matter what role a server performs, it acts as the centralized repository for databases, programs, network files and policies.

Servers are very easy to manage and also take backup as the servers in a network are not all dependent on the configuration of the individual user and it can be implemented seamlessly across the network.

Network devices

Network devices act as the intermediary between the server and the workstation and help in establishing a connection between the two. Network devices make sure that the requests going from and to the workstations are properly routed with the concerned server. There are various types of network devices available today and each performs different functions of connectivity. In a basic client-server network, the hub helps in connecting a server with the various workstations. It also functions as a repeater and passes on information and data from one device in the network to another. Network devices such as bridges help in separating the various segments of a network.


10/100/1000 PCI-E
eth0
eth1
eth2
USB 2.0

Chapter 4: Peer to Peer Connection

In the world of networking, there are various types of connection that can be found and created easily. Each of the connections comes with a particular purpose and structure of its own. A P2P or peer to peer network is created when two or more than two computers are connected with each other and share resources and data with each other without the presence of any separate server system. In this form of connection, all the computers within the network share an equal amount of responsibility for the purpose of data processing. Peer to peer network is completely different from client-server networking. In a client-server network, the server acts as the master system and processes data which is consumed or used by the other client systems within the network. However, this is not the case with peer to peer connection.

A peer to peer network can act like an ad hoc connection in which several computer systems are connected with each other via Universal Serial Bus for the purpose of transferring files and data. It can also perform as a permanent infrastructure which links up several computers within a small office network with the use of copper wires. A P2P connection can also be a larger network of much bigger scale which uses up special protocols along with applications for the purpose of setting up a direct relationship with all the users over the internet. In simple words, a peer to peer network can assume various at times and as required.

Peer to Peer connection and its characteristics

Peer to peer connection can be found on all forms of small-sized LAN or local area network. It is most commonly found in home networks. Both the wired and wireless form of home network can be set up as peer to peer network. All the computers which are involved in a peer to peer network run the same protocols of networking and software. The network devices of peer are most often located near another peer generally in small businesses, homes, schools and smaller organizations. There are also other types of peer to peer connection that utilizes the internet and are dispersed at long distances geographically all over the world.

The home networks which use routers of broadband are a hybrid form of peer to peer and client-server network. The broadband router provides a centralized sharing connection of internet but the printer, files and all other sharing of resources are directly managed between all the involved local computers.

Peer to peer along with Ad Hoc network

The Wi-Fi or wireless networks support ad hoc connection in between the devices. Ad Hoc networks are a form of pure peer to peer connection which can be compared with those networks that use wireless routers as the intermediary device. The devices that build up ad hoc networks require no form of infrastructure for the purpose of communication.

Benefits of Peer to Peer connection

Peer to peer network is robust in nature. In case one of the attached devices fails to perform, the network continues to function with the use of

other devices. You can easily configure the computers in a peer to peer network workgroups for allowing file sharing, printers along with other resources across all the connected devices. Peer to peer connection allows both way sharing of data, whether for the purpose of downloading to the computer or for uploading from the computer.

While on the internet, peer to peer networks can easily handle huge volumes of traffic of file sharing. It handles huge traffic by distributing all the load across all the computers in the network. As P2P connections are not dependent on any form of central server, this network is better in scalability and is also more functional when compared to client-server network at the time of any kind of emergency or heavy traffic.

You can easily expand a peer to peer network. As you keep on increasing the total number of devices in the network, the power of peer to peer network also keeps on increasing. This is because in peer to peer connection, all the devices are responsible for data processing and with the increase in the number of devices within the network, the processing power and speed of the network also increases.

Peer to Peer connection and the security concerns

In this world of today, none of the network systems is safe from external attacks. Just like client-server network, peer to peer connection is also a vulnerable network form to security attacks. In peer to peer connection, all the devices in the network participate in traffic routing across the network. So, it becomes easier for the attackers to launch attacks such as denial of service by the use of one such device on the network. The software for

peer to peer connection acts both as the client and the server. This makes P2P network much more prone to remote attacks when compared with a client-server network.

The corrupted data can still be shared on the peer to peer network simply by modifying the files which are on the network for the purpose of introducing malware or malicious codes.

Chapter 5: Basic Components of Computer Networking

Computer networking functions with various components. All the components work together and make data transfer possible from one system to another and help in establishing a smooth connection between the sender and the receiver. A computer network works with one or more than one servers, network interface cards or NIC, workstations, passive and active hub, gateways, bridges, modem, routers, hub, software like OS for networking and many more.

Server

It is regarded as the mother of a network. It is the most powerful system within a network. In the case of LAN, a powerful computer is generally used as the server. In computer networking, two types of servers are used: dedicated and non-dedicated. A dedicated server performs all the services and functions in a network. It helps in running the user applications and also helps in improving the overall cost of the system. However, in a dedicated server, the users cannot directly run their applications. A dedicated server provides the users with sharing of various hard disks, service regarding email along with sharing of several other data and resources. It comes with a very fast time of response. For all those networks where it is required to handle heavy loads, dedicated servers are employed usually.

In the case of the non-dedicated server, it also functions as a workstation besides functioning as the controller of network. It comes equipped with a prodigious form of memory. The network in which this server is used uses up only a portion of the memory of the server. The rest of the server memory is used up for applications of the users. It is useful for light traffic load condition.

Networking hardware

Network hardware is those devices which are used for interconnecting the various components of a network like the network cards, connection between the servers and the workstations and the cables that connect the peripherals to the network.

Resource sharing

These are the resources of both hardware and software devices. The most commonly found hardware devices are drives, printers, hard disks, CD drives etc. The software resources include programs, applications, files etc.

File Server

The main goal of computer networking is to share information and data among various users. The users also make their printers, modems, disk drives and other links of communication with other client stations as well. The client systems can raise a request to access the shared facility from the server. The file server runs on a special software and is generally

served by a powerful system of computer. It helps in sharing files and other resources to all the users within a network. File server also provides other facilities such as authentication of user, program and data security and many more. It generally operates via NOS. All the file server activities are controlled and monitored from the console. The prodigious memory of the file server is used for caching of files and directories.

Workstation

Workstation is regarded as a critical component of a network system. It is also known as the client system. It comes with the capability of connecting and communicating with all other machines in a network. However, for a workstation to function properly, it is required to comply with the software and hardware of the LAN. A workstation is capable of communicating with the server for getting data and other resources. The hardware which is required by the workstation depends completely on the size and application of the network.

NIC

Also known as network interface card, it serves as an add-on card for the computers in a network. It is also called network interface adapter or Ethernet adapter. NIC performs the function of moving the signals across the cables of the network into a parallel stream of data directly inside the systems of the computers. You can also use more than one NIC for splitting the load in the network.

Hub

It is a centralized point of distribution which is required for transmission of data in the network. The hub is generally used for receiving the data packets and then rebroadcast them to all the other computer systems which are connected with it. It is a passive device in nature. The destination of the received data packet is unknown to the hub. Hubs can be easily classified into three categories:

- **Stackable and non-stackable**: The stackable hubs are those hubs which can be interconnected for making a single hub. The non-stackable hubs cannot be connected.
- **Active and passive:** Active hubs are those which connect to the backbone of the network. The hubs which only connect with the active hubs are the passive hubs.
- **Intelligent and non-intelligent:** Intelligent hubs come with a special type of firmware which can also be accessed by the workstations which are remote in nature. The non-intelligent hubs come without any form of firmware.

Bridge

It is used for interconnecting two different networks by the use of the same technology like Ethernet. It reads the address of the destination of the received packet and also makes sure that the destination address is also on the similar network segment as the origin. In LAN, local bridges are being used for connecting two different segments.

Gateway

Two networks which are different in nature can be connected with the use of a gateway. It converts the data format which is sent in between the networks.

Modem

It helps in facilitating two-way communication in between a telephone network and a computer network.

Chapter 6: OSI Model

OSI model or Open System Interconnection model is a model which has been created for enabling diverse systems of communication for communicating with the use of various standard protocols. In simple words, OSI provides a network standard for the different systems of computer for communicating with each other. The OSI model is also regarded as the universal language for networking. It is based on a concept in which a communication system is split into seven different layers each of the layers are stacked upon one another. Each layer of the model performs a specific function and also communicates with the layers above it and below that layer.

Importance of the OSI model

The modern internet structure does not follow the structure of OSI model strictly but it is still useful for the purpose of network problems troubleshooting. Whether it is just one single person who is unable to connect his PC with the internet or a huge website which is down that serves thousands of users, OSI model helps in breaking down the main problem in layers and also isolates the trouble source.

Seven layers of the OSI model

The seven layers of the OSI model are stacked in inverted order which means that the 7^{th} layer at the top and the 1^{st} layer at the bottom.

Application Layer

This layer is the one which interacts directly with the user data. Various software applications like email clients and web browsers depend on this layer of the OSI model for initiation of communication. However, it needs to be cleared that the software applications of the clients are not a part of this layer. The application layer is liable for manipulation of data and protocols on which the software relies on for presenting data which is meaningful for the user. This layer includes both HTTP and SMTP.

Presentation Layer

The presentation layer is liable for data preparation which can be used by the application layer on top of it. In simple words, this layer transforms data in presentable form so that it can be consumed by the applications. This layer is liable for encryption, translation and also data compression. The 6th layer is responsible for the translation of incoming data into a simpler syntax so that it can be understood by the application layer on top of it. In case the devices are communicating with each other over a connection which is encrypted in nature, this layer applies encryption to the sender's end and also decodes the data on the end of the receiver so that the data can be presented to the application layer in a readable and unencrypted format. It also helps in data compression before delivering data to the 5th layer.

Session Layer

The session layer is responsible for the closing and opening of the system of communication between two devices in a network. Session is the time in between the opening and closing of the communication. This layer

makes sure that the communication stays in the open state till the time before the data exchange has been done.

Transport Layer

This layer is liable for communication between two devices as an end to end communication. This whole process involves data collection from the session layer and then breaking them into segments just before sending them out to the 3rd layer. This layer on the recipient device is liable for segment reassembling into complete data so that it can be consumed by the session layer. This layer also takes care of flow and error control. Flow control helps in determining a normal speed for transmission so that a sender who is having a fast connection does not deluge the receiver who is having a slow connection.

Network Layer

This layer is liable for allowing transfer of data in between two different forms of networks. In case both the devices in the communication are functioning on the similar network, this layer becomes unnecessary in such case. This layer breaks up the segments from the transport layer just above it into various smaller units known as packets on the device of the sender and the reassembles the packets on the device of the receiver.

Data Link Layer

This layer is very much similar to that of the network layer. The only difference is that this layer allows transfer of data between two devices

which are on the same network. This layer takes in packets from the network layer and then breaks them into frames.

Physical Layer

This layer involves all the physical form of equipments which are used in the transfer of data like switches and cables. This layer also converts data into bit stream in which the string is of 0s and 1s. The physical layer present in both the devices needs to agree on the convention of the signal so that it is possible to distinguish 1s from 0s in both the devices.

Chapter 7: Wired Network VS. Wireless Network

There are two types of networks systems that can be found in most of the organizations and homes: wired network and wireless network. Wired form of network in which Ethernet is used is the most common choice in most of the homes but Wi-Fi along with other forms of wireless networking are also gaining its momentum. Both forms of networking come with pros and cons over each other where both can be used for homes and for office purpose.

Wired LANs

In this form of network, Ethernet cables are used along with the network adapters. Two devices can be easily connected with each other by using Ethernet cables but sometimes intermediary components such as hubs, routers and switches are also used.

Installation

The Ethernet cables run from one computer to the other or directly to the server or central system. The installation process is time-consuming especially when the computers are at a distance from each other or at different rooms. However, CAT5 cables are also used today which helps in simplifying the process of cabling and also minimizes the cable runs which are unsightly. The configuration of cabling depends greatly on the mixture of devices which will be used on the network, the internet connection type and also on various factors such as whether internal or external modems will be used or not. The configuration of the network relies on the standard IP and on other options of network OS.

Costing

The whole setup of wired LAN is cheap. The cables, switches and hubs are inexpensive. The software required for connection sharing such as ICS comes free. In general, the wired LAN is really cheap in nature however, it might turn out to be costly when other features such as security devices and broadband routers are used in the network.

Reliability

The hubs, Ethernet cables and switches are reliable in nature as the developers of such items have been improving the technology with time. The only drawback of a wired network is loose cables. It might hamper the entire network if one of the cables is not connected properly. However, this form of network allows fast transfer of data across the computer systems with no lags in performance.

Performance

The wired LANs come with superior quality of performance. It can offer a bandwidth of 10 Mbps to 100 Mbps. It makes file sharing among the systems a very easy job and can transfer them within no time. It also allows high-speed access to the internet.

Security

Firewalls are the main consideration for security in wired LANs. The various components do not support firewall but it can be installed on the computer.

Wireless Network

This form of network uses Wi-Fi for setting up a connection with the other devices on the network. It does not involve any type of wired connection with the systems.

Installation

The wireless networks or Wi-Fi networks can be easily configured and it can be done in two different ways:

- Infrastructure mode which allows the devices to communicate to a prime node that can, in turn, communicate with the wired form of nodes on the LAN.
- Ad-hoc mode allows the devices to connect with each other using peer to peer mode.

Ad hoc mode allows only the basic form of file sharing between the devices. Both the configuration types need network adapters which are also known as WLAN cards.

Costing

Wireless networking is much more expensive when compared to wired LANs. The wireless adapters are costlier than the Ethernet adapters, switches, hubs etc.

Reliability

Wireless LANs also suffers from reliability problems just like wired LANs. The main problem that comes with wireless LAN is the concern

about signal strength. It is subject to various interferences such as microwave ovens, garage door openers and cordless phones. It requires to be installed carefully for minimizing the interference in signal strength.

Performance

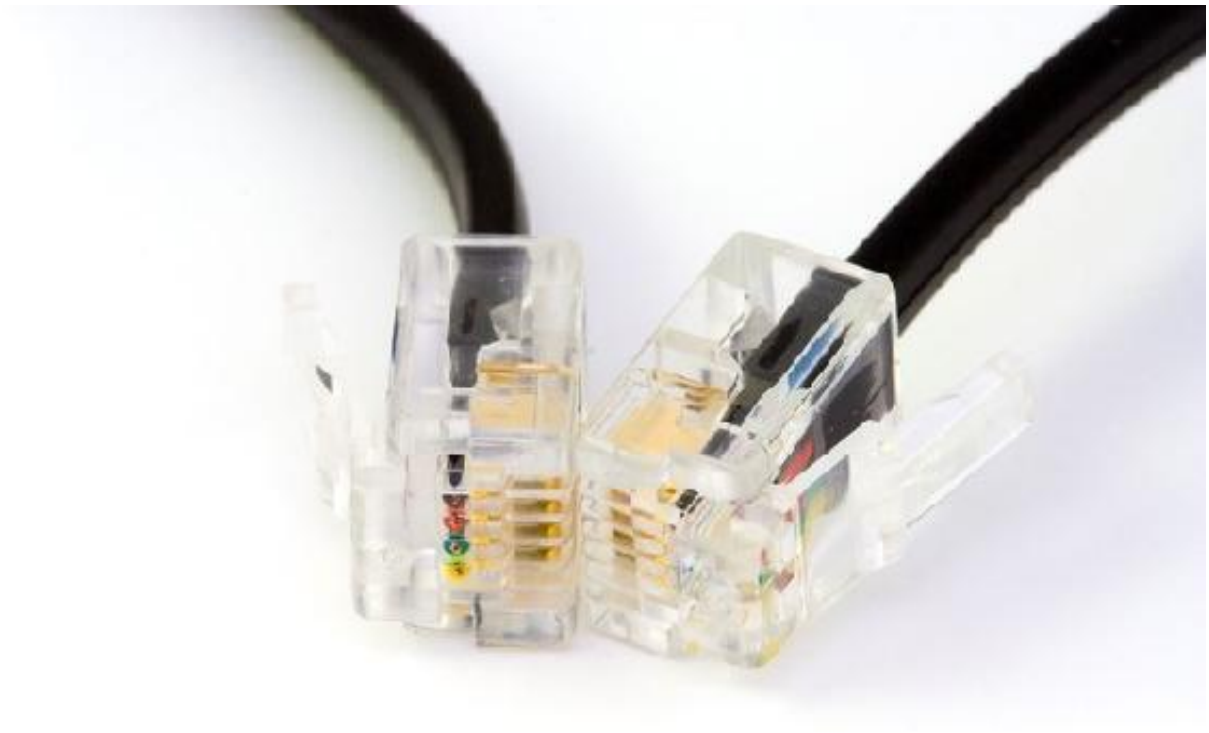
The wireless LANs which uses 802.11b can provide a maximum bandwidth of 11 Mbps. It can support a maximum of 54 Mbps which is half when compared with the bandwidth of wired LANs. The performance of Wi-Fi connection depends on the distance between the access point and the device. The larger the distance the slower the connection. However, it removes the use of long Ethernet cables for setting up a network and is thus mobile in nature.

Security

The wireless LANs are less secure in nature when compared with the wired LANs. This is mainly because of the fact that the signals of wireless communication travel through the air and it can be intercepted very easily. For making the connection more secure some measures need to be taken such as the internet firewall needs to be configured properly. Any inappropriate access to the network should also be avoided.

Bottom line

In case you are looking out for a networking system which is cost-effective, fast and you are not concerned about mobility, then wires LAN is the best option. If you are willing to speed up with the technology with the mobility of network, then wireless LAN is the option for you. Both come with pros and cons and you need to analyze them according to your need.



Chapter 8: Hardware Involved in Computer Networking

Computer networking is mostly about hardware. There are various types of hardware components used in setting up a network and for its functioning. You can set up a network with the minimal hardware requirements but as you keep on adding more elements one by one, the performance and reliability of the network also increase.

Networking cables and wires

In spite of so much advancement in wireless networking technologies, many of the computer systems in this 21st century still rely on wires and cables as the physical medium for transferring information data across the network. There are various standards of cables in the world of networking and each of them is designed for some particular purpose. The most common types of networking cables and wires that can be found today are Ethernet cables and fiber optic cable.

Ethernet Cable

Ethernet cable is the most common form of cable that is used for wired networking. It helps in connecting various devices such as computers, switches and routers within a network of local nature. However, Ethernet cables are very much limited when it comes to durability and length. If the cable is kept too long or is of not good quality, the cable won't be able to carry good signal. That is the reason why different types of Ethernet cables are used for different functions.

Types of Ethernet cable

The Ethernet cables which are used today support many of the industry standards that also includes category 5 and 6. The technicians who are experts in computer networking refer to these Ethernet cable standards as CAT5 and CAT6. Ethernet cables are developed in two forms:

- **Solid Ethernet cables:** This form of Ethernet cable offer a bit better performance along with improved security against all forms of electrical interference. Such cables are also being

used in the business networks, office wall wiring and under-floor wiring.

- **Stranded Ethernet cables:** This form of Ethernet cable is less vulnerable in nature are also less prone to breaks or cracks. This type of Ethernet cable is suitable for the home-based network.

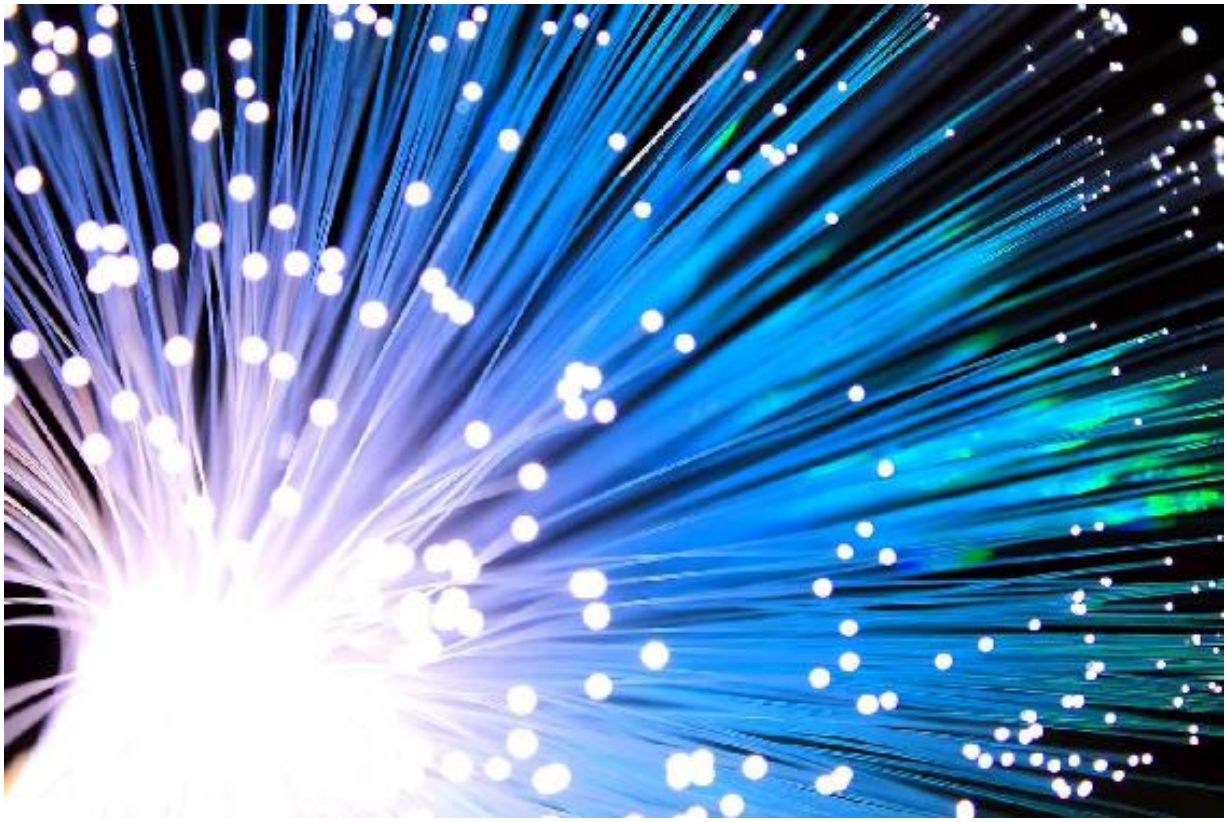
Ethernet cables and limitation

Ethernet cables come with distance limitation. It comes with a distance capacity where the cable comes with a maximum upper limit for how long it can run before there is any form of loss in network signal. This is also known as attenuation. This is mainly because long cables come with an electrical form of resistance that prohibits signal flow and thus affects the overall performance of the network. Both the ends of the Ethernet cable needs to be close enough for receiving signals fast and also at a distance from any form of external interference for avoiding interruptions in the connection. This practice does not interfere with the network size as various hardware components such as routers and hubs can be used joining various Ethernet cables on the same wired network. The distance between the two devices is known as network diameter.

The length of CAT5 cable just before attenuation takes place is 324 feet. However, CAT6 can extend up to a distance of 700 feet. If you want you can also keep the Ethernet cables longer than the standard lengths but the only problem that you will be facing is loss in signal, especially in cases when the cables need to pass across large appliances.

Alternative option for Ethernet cable

There are various alternatives that can be found today for Ethernet cables such as Bluetooth and Wi-Fi. It is mainly because the devices and systems of today are not having a network port and come with Wi-Fi only. But, still the security and performance which is provided by Ethernet cables are really outstanding and many of the big organizations and various home networks still use Ethernet cables for a wired network.



Fiber Optic Cable

Fiber optic cable is a form of network cable that comes with glass fiber strands inside the insulated casing of the cable. It has been designed for long-distance transmission of data, telecommunications and for high performance of the network. When compared with Ethernet cables, fiber optic provides larger bandwidth and it is capable of transmitting data to long distances without any loss in signal. It supports most of the world's cable television, internet and telephonic systems.

How does fiber optic cable function?

Fiber optic cable is composed of several strands of glass which are slightly thicker when compared with human hair. The center of each of the glass strand is known as the core which provides the travelling pathway for light. The core of the glass strands is surrounded by a glass layer which is known as cladding which helps in reflecting all the light inwards and thus helps in preventing signal loss. It also allows the light to travel through cable bends easily. Fiber optic cables are of two types: single-mode and multi-mode. The single-mode cable uses super thin strands of glass along with a laser for the purpose of generating light. The multi-mode cable uses LEDs for generating light.

The single-mode fiber optic cable uses a technique known as Wave Division Multiplexing for the purpose of increasing data amount traffic which can be carried by the glass strands. This technique allows light to travel at various wavelengths for combining and then separating later for transmitting various streams of communication via a single pulse of light.

Fiber optic cable and its advantages

Fiber optic cables offer various advantages for long distance transmission. Fiber optics can easily support higher capacity of transmission. The bandwidth of fiber optic cables is 10 Gbps, 40 Gbps and 100 Gbps as standards. Fiber optics do not need any form of signal booster this is because light travels for longer distances without any form of loss in its strength.

The cable of fiber optics is less vulnerable to any form of interference. The Ethernet cables require shielding for its protection from

electromagnetic interference. However, this shielding is not enough for the ultimate protection. However, the physical properties of fiber optics cable can easily avoid all these problems.

Fiber optics to the home

In most of the cases, fiber optic cables are being used for long distance communication in between the cities and countries. However, some of the local internet providers are also extending their network by installing fiber optics which can be accessed directly by the households. One of the prominent fiber to home service which is available in the market today is Google fiber. Such fiber optics services can easily provide gigabits of internet speeds to the households. There are various versions of fiber to the home network such as:

- **Fiber to the premises or FTTP:** In this, the fiber optic cables are laid to the buildings directly.
- **Fiber to the building or FTTB:** It is similar to that of FTTP.
- **Fiber to the curb of node or FTTC/N:** In this, fiber optic cables are laid till the node and then copper wires are used for completing the overall connection inside the household building.
- **Direct fiber:** In this, the fiber optic cable is taken from the central office and is connected to the system of the customer directly. This form of connection provides the best bandwidth but is expensive as well.
- **Shared fiber:** It is similar to direct fiber but as the fiber optic cable reaches the premises of the users, it is distributed into several fiber optic cables for the users.

Other Required Forms of Hardware

Wireless Hardware

For setting up a wireless network, you need certain components of hardware. When it comes to a wireless network, there are two types of network: ad hoc and infrastructure. The infrastructure mode of network is the kind of wireless network that can be found in offices and homes. It is somewhat similar to the wired network but it is done without wires.

The basic form of wireless network which is peer to peer network requires these hardware components.

- **Router:** Wireless router can be regarded as the heart of a wireless network. Just like a wired network, it is the central location with which all the computers connects to for accessing the network. The wireless routers are also called as access points. It helps in managing the connections in a wireless network and also helps in establishing a connection with the network.
- **NIC:** Every computer which wants to connect with the network requires a NIC or network information card. It allows the system to communicate with the router. Laptops come with in-built NIC but in the case of PCs, you are required to install NIC for getting a wireless connection in the system. It can be installed either internally or it can also be used as a plug-in

USB device. This is the standard which is used for infrastructure mode of wireless network.

In the ad hoc mode of wireless network, all the computers in the network are connected with one another. It functions without any form of router or central hub. Instead of sharing one common server, all the computers in the ad hoc mode can access directly the files and resources in the other computers.

Wireless network comes with various advantages when it comes to hardware components. You can easily mix up wired network components like switches to a wireless network in case you require more number of Ethernet ports. In spite of the wireless structure, you are still required to use an Ethernet cable for the purpose of connecting the router of a wireless network with the modem of broadband.


SECURITY

Chapter 9: Network Mode Security

The algorithms of network security have gone through various changes along with upgrades since the year 1990. It has turned out to be more effective and secure in nature. Today, various types of protocols have been developed for the protection of home wireless networks. The most common protocols are WPA, WEP and WPA2. All of these serve a similar purpose but each differs from one another in some aspects. Wireless protocols for security not only helps in preventing unwanted people from connecting to the network but it also helps in encrypting the data which is sent via the airwaves.

WEP

Also known as wired equivalent privacy, it was developed for the security of wireless networks and was accepted as a standard in the year 1999. WEP was expected to offer the same kind of security level just like wired networks but there are various issues in security in this protocol. It is very easy to break the security and is also very hard to configure the same. Despite all the upgrades which have been applied to WEP, it is still a very vulnerable form of security protocol.

WPA

It is also known as Wi-Fi protected access. It was adopted one year back just before WEP was abandoned. Most of the WPA applications of modern-day use a PSK or pre-shared key which is often referred to as WPA personal and TKIP or temporal key integrity protocol for the purpose of encryption. It uses a server for the purpose of authentication for the generation of certificate and for the keys.

Just like WEP, WPA was also found out to be vulnerable to external intrusions. The attacks which were posed as most dangerous for the protocol were not direct in nature but the ones which were set up on WPS or Wi-Fi protected setup developed for simplifying the linkage between the devices for the modern-day access points.

WPA2

WPA was improved and was made into WPA2. It is also known as Wi-Fi protected access version 2. The major upgrade that this protocol received was the usage of AES or access encryption standard. AES has been approved by the government in the U.S. for the purpose of encrypting data and information.

The main form of vulnerability to a system with WPA2 is when the attacker has complete access to the secured network of Wi-Fi and can also access some of the keys which are required for carrying out the attack on the devices in a network. In WPA2 systems, the security threats are mainly at enterprise levels and are not at all relevant to the home networks.

However, attacks via WPS are still there in the WPA2 systems just like WPA.

Which method of security to opt for?

When all the security methods are arranged in order of best to worst it goes on like:

WPA2+AES
WPA+TKIP/AES
WPA+AES
WPA+TKIP
WEP
Completely open network

The best method is to deactivate WPS and then set the wireless router for WPA2+AES. Both WPA2 and WPA are used for securing networks from any form of unauthorized access. In case you leave the system with no form of security, any third party can easily steal bandwidth of the network, perform various illegal jobs with the help of the network, monitor your activity on the web and can easily install malware on the system.

WPA2 is regarded as the best out of all. The only downside that comes with WPA2 is determining the power of processing that the protocol needs for protecting the network. So, it means that super-powerful hardware is required for avoiding lower performance of the network. You should

always opt for WPA2 or otherwise WPA in case you have no other option. Using WPA can help in handling heavy loads but when there is heavy load in WPA2 system, it might also affect the network speed.

When it comes to encryption, it will depend on the type of protocol that you are using. WPA2 comes with the fastest speed of encryption and WEP provides the slowest speed of encryption.

Protecting the Wi-Fi network

While it is evident that WPA2 provides more advanced protection than WPA and WEP, the router security depends completely on the password that the user sets. WPA2 and WPA allow a maximum password length of 63 characters. Try to use as many characters as you can for your Wi-Fi password. Hackers always lookout for easy targets. If they are unable to crack the password within minutes they will move on to the next target.

WPA3

WPA3 or Wi-Fi protected access version 3 is the next-gen security protocol for Wi-Fi. It helps in safeguarding the Wi-Fi networks completely and also saves the users from their own shortcomings in security. WPA3 protects the Wi-Fi network password from dictionary attacks by the implementation of a new key exchange protocol. WPA3 also supports the function of forwards secrecy in which any form of traffic that has crossed the system just before an attacker gained access to the network, remains encrypted which is not the case with WPA2. WPA3 also

provides extended security to the public networks that keep the users safe from any form of vulnerability that they cannot realize.

Chapter 10: Circuit and Packet Switching

Circuit Switching

In the process of circuit switching, the network bandwidth or resources are divided into small pieces and a little bit of delay is permanent at the time of establishing a connection. The circuit or path which is dedicated between the sender and the receiver gives out a proper data rate. All forms of data can be transported via the circuit without any form of delay once the dedicated circuit has been established. The system of a telephone network is the best example of circuit switching. Time division multiplexing or TDM and frequency division multiplexing or FDM are the two different methods which are used for multiplexing various signals into one single carrier.

- **FDM:** It divides the network bandwidth into various frames. It is mainly used when various data signals are connected for transmission through a shared medium of communication. It is used for dividing the bandwidth into a number of non-overlapping sub-bands frequencies. Each of the sub-band frequency carries various forms of signals. It is used in optical fiber along with radio spectrum for sharing various signals of independent nature.
- **TDM:** It divides the network bandwidth into frames. It is used for transmission and receiving of independent signals across a common path of signal with the help of switches in a synchronized manner at every end of the line of transmission.

It is used for communication for long-distance links and it can also bear huge data traffic load from the end-user.

Phases of circuit switching

In circuit switching, everything is done in various phases.

- **Establishment of the circuit:** During this phase, a circuit is established directly from the end of the source to the receiver across various intermediary centers of switching. The sender and the receiver both transmit signals of communication for requesting and acknowledging the establishment of the circuits.
- **Data transfer:** After the circuit has been created, voice and data are transferred from the sender to the receiver. The connection stays as long as both the parties want to communicate.
- **Disconnection of the circuit:** Once the transfer of data is finished, the connection is abandoned. The disconnection request rises from either of both the parties. The process of disconnection includes removal of all forms of intermediary links between the sender and the receiver.

Advantages of circuit switching

Circuit switching comes with a wide range of advantages:

- It is best suited for transmission of longer duration. It is possible because a continuous route of transmission is created which remains in place as long as the conversation goes on.

- The dedicated communication path makes sure that there is a steady communication rate.
- There are no forms of intermediary delays after the circuit has been established. So, it is a great option for real-time communication for both data and voice transmission.

Disadvantages of circuit switching

- In circuit switching, a connection is established between two parties. This connection cannot be utilized for transmission of any other form of data, no matter what is the load of data.
- The bandwidth is required to be very high even if the data volume is low.
- The total time which is required for establishing a connection is high.
- The system resources are underutilized. After the resources have been allocated for one particular connection, the resources cannot be utilized for any other connection.

Packet Switching

It is a method which is used for transferring the required data to the network in the form of packets. The data which is meant for transmission is broken down into smaller pieces called packets. This is done for ensuring that the file is transferred fast and in an efficient manner directly across the network and also for minimizing and latency in transmission. All the small data packets are reassembled after reaching the destination. A packet is composed of payloads along with several information of

control. For this, there is no need for reservation or pre-setup of the resources.

The whole process of packet switching uses the technique of store and forward at the time of packet switching. While the packets are forwarded, each of the packets is stored first and is then forwarded. This whole technique is very important as the data packets might get discarded at any of the hops due to any form of reason. There can be more than one single path in between the source and the destination. Each of the data packets comes with the addresses of both the source and the destination and thus the packets can travel independently across the network. In simple words, data packets of the same file might or might not travel along the same path. In case of any form of congestion at any of the paths, the packets can choose some different path over the existing network.

For overcoming the all over weaknesses of the circuit-switched network, packet-switched network was developed. This is mainly because the circuit-switched networks are at all effective for messages of smaller size.

Advantages of packet switching

Packet switching comes with various advantages over circuit switching.

- It is more efficient when it comes to the bandwidth of a network. It is because there is no concept of circuit reservation in packet switching.
- There is very less latency in transmission.
- It is of more reliable nature as the destination is capable of tracing out the missing packet.

- It is more tolerant of faults as the packets can choose any other path if there is any congestion in the path.
- It is very cost-effective and is also cheaper when implemented.

Disadvantages of packet switching

- The packets are not delivered in proper order but in circuit switching the packets are delivered in an orderly manner as all the data packets travel through the same circuit.
- As the packets travel unordered, each of the packets needs to be provided with a sequence number which is time-consuming.
- The complexity arises at the nodes as the packets can follow several paths.
- There is delay in transmission because of rerouting of the packages.
- It is not at all suitable for heavy load and is best for small messages.

Packet switching and its modes

- **Connection oriented:** Before the transmission starts, it helps in establishing a virtual connection or logical path with the use of signaling protocol. The path is established in between the sender and the receiver and all of the packets which are part of

this flow will follow this established path. Virtual circuit ID is given out by the routers or switches for unique identification of the virtual connection. All of the available data is divided into various smaller units and the units are affixed with a sequence number. In this, three phases work together: setting up, transferring of data and tear down phase. The information regarding address is transferred only during the phase of setup. After the destination route has been figured out, entry is added up to the table of switching for each of the intermediate nodes. At the time of data transfer, the local header or packet header might contain other information like timestamp, length, sequence number and many others. It is of great use in switched WAN.

- **Connectionless switching of packet:** In connectionless packet switching, each of the data packets contains all the relevant and important information like destination address, source address, port number etc. which is not the case with connection-oriented packet switching. In this form of packet switching, all the data packets are treated in independent form. All the packets which belong to one flow might also take up different paths as the decision of routing is completely dynamic in nature. So, the data packets after arrival might not be in proper order.

Types of delay in packet switching

- **Transmission delay:** It is the time which is taken for putting a data packet into the link. It completely depends on the packet length along with the network bandwidth.
- **Propagation delay:** It is the time which is required by the bits for reaching the destination from the origin. It depends on propagation speed and distance.
- **Queuing delay:** It is the time that one job waits in the queue for getting executed. It is dependent on network congestion. It is the difference in time when the destination received the packet and when the data packet was executed.
- **Processing delay:** It is the time which is taken by the routers for processing the packet headers. The packet processing helps in the detection of bit-level faults that takes place at the time of packet transmission to the destination.

Chapter 11: Connection Between the Network Devices

For the purpose of connecting to a network, the computer systems need to have certain components for a seamless connection. Without such components which include IP address, subnet mask, DHCP and many others, it will not be possible for the system to connect with a network. Each system comes with its unique set of components that helps in establishing a new connection.

IP Address

The IP address or Internet Protocol Address is the number of identification for the network hardware which is connected with the network. When your system has an IP address, it can communicate with all the other devices across a network based on IP address such as the internet. Most of the IP addresses look like 123.121.52.141.

What is the use of an IP address?

The IP address helps in providing a unique identity to the devices in a networked structure like the internet. It is somewhat similar in nature to your home or business addresses which helps in the delivery of supplies to a particular location that comes with an address which is identifiable. All the devices on a network can be differentiated from each other with the help of IP addresses. When you want to send a gift or package to one of your friends who live in a foreign country, you need to know the exact location of your friend. This same process is being sued for sending data across the internet. However, in place of using a physical form of mailing address, the computer systems use DNS servers for looking up at a hostname in order to find out the IP address.

For example, when you want to browse a website by entering the URL of the respective website such as www.google.com, your request for loading the page is sent over directly to the DNS servers which find out for the hostname for google.com for finding out the related IP address. Without the presence of a proper IP address, your computer will be having no clue that what are you up to.

IP address and its versions

IP address comes in two different versions: IPv4 or internet protocol version 4 and IPv6 or internet protocol version 6. IPv4 is the older version of IP address whereas IPv6 is the latest and the upgraded version.

- **IPv4:** IPv4 addresses are constructed in such a way so that it capable of providing about 4 billion IP addresses which are all unique in nature. Although it comes with a huge number of addresses, it is still not enough for the modern world of today with various types of devices being used on the web or internet.
- **IPv6:** IPv6 can support 340 trillion, trillion and trillion addresses which come out like 340 along with 12 zeros by its side. It means that each and every person on the Earth will be able to connect a billion numbers of devices with the internet.

One of the reasons why IPv4 is being replaced by IPv6 is that the latter one provides more number of IP addresses when compared to the former. When various devices are all connected on the similar network, it is very important for each of the devices on the network to have a unique address of its own. IPv6 also comes with a wide number of added benefits over IPv4:

- There is no collision of IP addresses which is caused by the private addresses
- It comes with auto-configuration feature.
- There is no need for NAT or network address translation.

- It comes with an efficient feature of routing.
- The administration of the IP addresses is very easy.
- It comes with in-built privacy for the IP addresses.

In IPv4, the IP address is displayed as a 32-bit number which is written in the format of decimal such as 210.251.165.40 or also 192.251.1.1. As in IPv6, there can be trillions of possible IP addresses, it is written in a hexadecimal format such as 3gge:1500:6565:4:100:f7ff:fe31:97cf.

IP addresses and its types

There are various types of IP addresses that can be found. While all forms of IP addresses are constructed of letters or numbers, not all of them are being used for the same function. The types of IP addresses are private IP address, public IP address, static IP address and dynamic IP address.

- **Private IP address:** This form of IP address is generally used inside one network such as any form of a home-based network which is used by Wi-Fi cameras, mobile devices, desktop PCs and wireless printers. This type of IP address allows the devices to communicate with the central router along with other devices which are based on the similar home network which is private in nature. This type of IP address can be configured manually or it can also be assigned automatically by the network router.
- **Public IP address:** This type of IP address is used for the outside area of a network and it is assigned by the internet service provider or ISP. It is the prime address which is used by the business or home networks for communicating with the

other networked devices all over the world. It helps by providing a path for the home-based devices to reach the ISP and therefore with the world outside as well. It allows the devices in a network to access various websites and also to communicate with the rest of the computers directly along with other servers all over the world.

Both these types of IP addresses are either static or dynamic in nature which means that they change either or not. The IP address which has been assigned by the DHCP server is known as a dynamic IP address. In case a device is not having DHCP server enabled or if it does not support DHCP, the IP address needs to be manually assigned and in such case, the IP address is called static IP address.

Dynamic IP Address

A dynamic IP address is the one which is assigned automatically to every node in the network like desktop PC, smartphone or tablet. This automatic assigning of the IP address is done by the DHCP server. An IP address which has been assigned by a DHCP server is known as dynamic as it will be changing in the future depending on the future connections with the network.

Where to find dynamic IP addresses?

The public IP address which is assigned for the router for most of the business and home network users by the internet service providers or ISPs is dynamic in nature. Bigger organizations and companies try not to connect with the internet with the use of IP addresses which are dynamic in nature and prefer using static IP addresses which are assigned specifically for them.

In any form of a local network like the one in your business place or home, where private IP addresses are used, most of the devices are pre-configured for DHCP. This means that all such devices use a dynamic IP address. In case the devices do not have DHCP enabled, each of the devices is required to manually set up the network information.

Dynamic IP address and its advantages

One of the prime advantages that come with assigning of IP addresses dynamically is that it is more flexible in nature. It is very easy to set up and the administration part is also easier when compared to static IP

addresses. For instance, when one of your devices connects with the network, it is assigned with one specific IP address. Once the device disconnects from the network, the same IP address becomes free and it can be used for another device that can connect afterwards, even if it is not the same device again.

Dynamic IP addresses come with little limitation to the total number of devices which can connect with the network as the devices which do not require to stay connected can easily disconnect from the network and thus freeing up the available pool of IP addresses for the other devices. There is an alternative in which the DHCP server can pre-configure some specific IP addresses for each of the devices in a network in case all of the devices want to get connected with the network at the same time. In such case, hundreds of networked devices, whether they were being used by the users or not can have their own specific IP address which can easily limit network access for all the new devices in a network.

The implementation process of dynamic IP addresses is easier when compared with the static IP addresses. There's no need to set up anything manually for the new devices which want to connect with the network. All that you need to do is to be sure that the DHCP has been enabled on the network router. As all the networked devices are by default configured to have a specific IP address for each from the huge pool of available IP addresses, each and every step turns out to be automatic in nature.

Dynamic IP address and its disadvantages

It is a very common thing which is acceptable technically as well for any form of a home network to use a dynamic IP address which has been assigned by the DHCP server for the router, problem comes up when the user tries to access the same home network from any other outside network.

Static IP Address

A static IP address is the one which has been manually configured for a networked device in place of the one which was assigned by DHCP server. The name static IP address means that the IP does not change and is static in nature. It can be regarded as the complete opposite of a dynamic IP address which changes. Phones, tablets, laptops, routers and other forms of network devices which uses IP address can be easily configured for having a static form of IP address. This can be done by the device which gives out the IP addresses such as a router or also manually by typing the device IP address into the device only.

Why does static IP address needs to be used?

You can think of static IP addresses just like your physical home address or your email address. Such addresses do not change and they are static in nature. It helps in contacting with people or finding someone. Similarly, IP addresses of static nature are very beneficial when you are hosting a website from your home, having a file server in the network, forwarding network ports to some particular device, using networked printers, using any form of remote access program or running a printing server. As static IP addresses never change, all the other devices in a network will know how to connect with a device which uses IP address of static nature.

For example, when IP address which is static in nature is set up for a PC within a home network, once the device gets a particular IP address for itself, the network router can be configured in a particular way for forwarding all the inbound requests to that device directly, like requests for FTP in case the device can share files over FTP.

If you are hosting a website and not using a static IP address for the same, it might turn out to be a hassle. This is mainly because when the computer gets some new IP addresses, you need to change the settings of the router every time for the purpose of forwarding the requests to the new IP addresses. When you neglect to do so, anyone can get inside your website as the router will be having no idea about which device within the network is serving solely for the website.
Another great example of an IP address of static nature at work is the DNS server. The DNS servers always use static IP addresses for making sure that the devices in the network know exactly how to connect with the servers. If they were regularly changed, you would also have to reconfigure the DNS servers regularly on the router for using the internet.

The static form of IP addresses is also very useful when the domain name of the device is not accessible. Those computers which connect with the file server within a workplace network could also be set up for instance with the server by using the static IP address of the server in place of the name of the host. Even if there is malfunctioning of the DNS server, the computers in the network can still access and connect with the file server as they communicate with the server by using the IP address. With applications which support remote access like the Windows Remote Desktop, using an IP address of static nature means that the user can access the computer always by using the same address. When you use an IP address which changes frequently, you need to know what it has changed to so that the new address can be used by you for establishing the remote connection.

Disadvantages of static IP address

One of the major disadvantages that come with static IP address when compared with a dynamic IP address is that all of the devices in a network are required to be manually configured. All forms of home-based web servers along with programs of remote access requires setting up the devices with a particular IP address and also configure the same properly with the router in order to communicate with a particular address. This comes with more amount of work than just plugging in the router and then allowing it to give the dynamic IP address via the DHCP servers.

In case a device has been assigned with an IP address like 192.168.1.10, and you are going to a completely new and different network which gives out the address as 10.x.x.x, you will not be able to connect with your static IP address. The device will require to be configured again for the purpose of using a DHCP server or for using an IP address of static nature that will work well with the new network.

Security can also be regarded as another downfall when a static IP address is being used for a device. When an IP address is used which is never changed, it will give the attackers much time for finding out various vulnerabilities within the network of the device. The only alternative would be to use an IP address of dynamic nature which changes and thus it will also make the attackers to change the way in which they communicate with that device.

Static IP address vs. Dynamic IP address

A dynamic IP address is exactly the opposite type of IP address than the IP address that never changes. Dynamic form of IP address is like any regular IP address just like static IP, but the dynamic IP is not tied with the device permanently. Instead of using one IP address for a lifetime, the dynamic IP addresses are used only for a particular time frame and then it returned to the pool of IP addresses so that the same can be used by the other devices in the network.

Dynamic IP addresses can outnumber in case of benefits when compared to static IP address. In case if an ISP kept on using static IP address from all its customers, there will be shortly a limited IP address supply for all the new customers. Dynamic IP addresses provide with the solution in which one IP address can be reused by some other device when it is not being used by any other device. Thus, providing access to the internet for more number of devices than it would have been possible with static IP address.

The static form of IP addresses come with limited downtime. While the dynamic form of addresses obtains a new IP, the user who is connected with the existing IP address is removed out of the connection and else has to wait for finding any new address. This will not be a recommended setup while you are going to a website, service of file sharing or online game, all of these will be requiring active connections constantly.

In case of any local network such as in place of business or in home, where you generally use an IP address of private nature, most of the devices in such network are configured for DHCP. Thus, all the devices use dynamic form of IP address. The public form of IP address which is assigned to the routers of the business or home-based network is dynamic in nature. Large-sized companies do not use the dynamic address for connecting with the internet. Instead of dynamic addresses, they use static IP address which is assigned to them.

How can you get a static IP address?

Some of the routers of today already reserves and IP address for the devices which are connected with the network. This process is generally done with the help of DHCP reservation and it performs by linking a specific IP address with the MAC address so that every time that device requests the router for IP address, the router can assign it the one which has been already chosen by the user with that particular MAC address. When you want to get a static IP address for your business or home network, you can do it by contacting your ISP but this option varies depending on the company that provides you with the internet. Having a static IP address for home-based and other local network is quite expensive when compared with getting a dynamic IP address.

Faking static IP address by using dynamic IP address

As getting a static IP address for your home or business network might turn out to be very expensive than a regular dynamic address, the best option is to opt for both forms of IP addresses by using dynamic DNS

service or DDNS. The service of DDNS associates a changing form of a dynamic IP address with the hostname that does not change as well. It is exactly like having your very own static form of IP address without even paying anything extra than a dynamic IP address.

No-IP is an example of a free DDNS service. You can use this for redirecting your required hostname for associating with the present IP address. In simple words, if you are having a dynamic IP address, you can access the network by using the exact same hostname. DDNS service is very helpful when you are required to access the home-based network remotely but you do not want to pay more for static IP. You can also host your personal website from your home and use up DDNS for ensuring that the visitors of your website can have access to the network any time they want.

DHCP Server

A DHCP server is nothing but a server of the network which provides and assigns the IP addresses automatically along with default gateway and various other parameters of a network for the devices of the clients. It is dependent on the standard protocol which is called DHCP or Dynamic Host Configuration Protocol for responding to the queries of the clients regarding broadcasting. The DHCP servers send out necessary parameters of the network automatically for the clients for establishing proper communication with the network. Without the presence of a DHCP server, the administrators of a network need to set up manually each and every client who joins with the network. This might turn out to be a cumbersome process, especially when large networks are involved. The DHCP servers assign each of the clients with one unique IP address of dynamic nature.

Benefits of DHCP server

A better option than using DHCP on the switch or router is to have a centralized server of DHCP. This is true in case of network environments which requires support from both DHCP for IPv4 and DHCO for IPv6, both at the same time. DHCPv6 comes with various benefits.

- When you have DHCPv6 server which is also integrated into the system of IPAM for IPv6, it will provide you with the visibility of all the client nodes of IPv6.

- The DHCP servers also provide management and logging of interfaces which aids in managing the scopes of the IP addresses by the administrators.
- DHCP servers also provide high availability along with redundancy. In case one of the DHCP servers fails to perform, the clients in the network will be preserving their present IP addresses and will not lead to any form interruption for the nodes at the end.

Why should you use a router as DHCP server?

Most of the switches and routers have the capability of providing the following server support for DHCP:

- DHCP client and obtaining an IPv4 address interface from an upstream service of DHCP.
- One relay of DHCP along with forward UDP DHCP messages from the clients directly on a local area network to and from a server of DHCP.
- Running DHCP server on switches and routers consumes all the resources which are available on the device network. Such packets of DHCP are handled by software.
- Does not need the support of dynamic DNS. The switch or router DHCP server will not be able to create an entry into the DNS on part of the client which is based on IPv4 address which was leased for the client.

- No form of redundancy or high availability of the bindings of DHCP. This might result in some serious form of problem if the present DHCP along with the default gateway fails together.

The organizations which have started the implementation of IPv6 need to migrate to the DHCP for IPv4. This change in DHCP will also point out that the organization also wants to have DHCP for operating both the protocols.


Sep 15:53 .
Sep 15:53 ..
Sep 2015 bin -> usr/bin
Sep 09:31 boot
Sep 15:50 dev
Sep 09:32 etc
Sep 15:52 home
30. Sep 2015 lib -> usr/lib
30. Sep 2015 lib64 -> usr/lib
23. Jul 10:01 lost+found
1. Aug 22:45 mnt
30. Sep 2015 opt
21. Sep 15:52 private -> /home/encrypted
21. Sep 08:15 proc
12. Aug 15:37 root
21. Sep 15:50 run
30. Sep 2015 sbin -> usr/bin
21. Sep 15:51 srv
21. Sep 15:45 sys
12. Aug 15:39 tmp
23. Jul 10:25 usr
var

Chapter 12: Background and History of TCP/IP

TCP/IP is a protocol set which enables the communication between various computers in a network. Protocols are nothing but the standards or rules which help in governing communications. When two devices in a network want to communicate with each other, both need to use the same protocol. This can also be compared to the communication of human beings. A person who speaks French will not be able to communicate with a person who speaks Chinese as both of them speak different languages. You have the option of selecting from a large pool of network protocols for using in the network. But, when it comes to TCP/IP, it is regarded as the industry standard. All forms of operating systems support TCP/IP. The whole internet works on TCP/IP. It is also called the language of the internet. In case you want a computer to communicate with the internet, you are required to use TCP/IP.

History of TCP/IP

Just before the internet of today, there was ARPAnet. It was created by ARPA or Advanced Research Projects Agency. It was launched at the time of the Cold War in 1969. ARPAnet was created as a response to the rising threat of nuclear attack from the Soviet Union. ARPA's main goal was to create a network which would be fault-tolerant and would enable the leaders of the U.S. military to stay in touch in case of a nuclear war. The protocol which was used for ARPAnet was known as the NCP or Network Control Protocol. As ARPAnet grew in size, another protocol was also required as NCP was unable to meet the growing needs of a large-sized network.

In the year 1974, a paper was published describing the features of TCP or Transmission Control Protocol. NCP was eventually replaced by TCP. After further development and testing of the new language, it led way to a brand new set of protocols which was called TCP/IP or Transmission Control Protocol/Internet Protocol. It was finally in the year 1982 when TCP/IP replaced NCP as the standard language for ARPAnet.

Features of TCP/IP

TCP/IP has been in the industry for more than 35 years. It a proved set of protocols that make it possible for the devices to connect with the internet. It comes with various features that make communication much more easier.

- **Support of multi-vendor:** TCP/IP is being implemented by several software and hardware vendors. It has been now a standard of the industry and is not at all limited to a particular vendor.
- **Interoperability:** Today, people can work in a network which is heterogeneous in nature only due to TCP/IP. While you are using a computer which runs on Windows OS, you can still download your required files from a machine that runs on Linux. This is possible only because both the systems support TCP/IP. It helps in eliminating the boundaries of cross-platform.
- **Logical addressing:** Each and every adapter of the network comes with a unique physical address which is permanent in

nature. This permanent address is known as MAC address, also known as the hardware address. This address is being burnt into the hardware card at the time of manufacturing. The protocols which are low-lying in nature and are hardware conscious on LAN delivers the packets of data with the use of the physical address of the adapter. The local adapter present in each computer tracks each and every transmission on the LAN for determining whether the message has been addressed to its very own physical address.

For a small-sized LAN, this whole thing works very well. But, when a computer is connected with a very large network just like the internet, it will need to listen to billions of transmissions every second. This might result in the failure of the network connection. For avoiding such cases, the administrators of the networks divide the big networks into various smaller networks with the use of devices like routers for reducing the network traffic. It makes sure that the unwanted traffic from any network will not create any kind of problem in some other network. The administrators can again subdivide a network into subnets for efficient travelling of the message directly from the sender to the receiver. TCP/IP comes with great capacity of subnetting which is achieved with the help of logical addressing. The address which is configured by the network software is called the logical address. TCP/IP uses a system of logical addressing which is known as the IP address.

- **Routability:** A router is a device of the network infrastructure which is capable of reading the information of logical addressing and then directs the data through the network right to the destination. TCP/IP is a routable kind of protocol. This

means that the data packets of TCP/IP can be easily moved from the segment of one network to another.

- **Flow and error control:** TCP/IP comes with various features that make sure that the data is delivered from the source to the destination reliably. Transmission Control Protocol or TCP also checks many of the error checking and flow control functions along with functions of acknowledgement.

Chapter 13: FTP – File Transfer Protocol

FTP which stands for file transfer protocol is a technique of sending files online. It acts as an application layer protocol which helps in moving the files between the local file system and remote file system. It functions on top of TCP such as HTTP. In order to share a file, two connections of TCP arranged parallel are used by the FTP: data connection and command connection.

FTP belongs to the oldest set of protocols which are still used today. It is a very convenient way of moving your files around. The server of FTP provides all-round access to any directory along with the sub-directories. The users can connect with all these servers with the help of FTP client. FTP client is a software which allows the users to download their required files right from the server and also upload files to the same server. If you are a normal internet user, you will not be requiring FTP. But, in case you are building a full website, it is a very important tool.

What is FTP used for?

FTP is useful for moving of information from the system on which you are working to the server where the website is being hosted. For example, if you want to install WordPress on a server, you need FTP for copying over the files. It is also used as a tool for sharing files. You can upload a document or file on the server of FTP and then share the file link with the person you want. However, this service is not much common today as people prefer cloud file transfer services rather than FTP file sharing.

There are various people who prefer to upload their files on the home server and they need to enable FTP for such service.

FTP uses two very basic types of channels: the command channel which carries all relevant information about the task and the data channel which transfers the files between the devices.

- **Command channel:** It is used for sharing all information of controls like the identification of the user, password, commands for changing remote directory, commands for retrieving and storing the files etc. The command channel is started on the port number 21.
- **Data channel:** For the purpose of sending the data file in actual, FTP uses a data channel. It is started at the port number 20.

FTP sends out the information of control out of band because it utilizes a completely separate command channel. Some of the protocols also send in request along with the header lines with the data in the same connection of TCP. That is why FTP sends out control information in the form of bands.

The FTP connection can also function in active and passive mode. Active mode is the most common of all and it allows an open form of communication in between the device and the server over both the channels. In this form of connection, the server assumes the active function for establishing a connection after approval of data requests. However, the active mode can be disrupted easily by the firewalls. So, in such cases, passive mode comes into play where the server attends the

connection but doesn’t maintain the connection actively and thus allowing all the devices in that network to perform all the tasks.

FTP session

When a session of FTP starts between the server and the client, the client starts a controlled TCP connection along with server side. The client uses this for sending out information on control. After the server receives this information on control, it starts a connection of data directed to the side of the client. It is to be noted that it is possible to send only one file over one single data connection. However, the connection of control stays active throughout the session of the user. HTTP is stateless in nature which means it does not require to keep detailed tracking of the state of the user. But, in the case of FTP, it is required to maintain the user state all throughout the session.

Data structure in FTP

In FTP, three types of structured data are allowed:

- **File structure:** In this, there is no form of internal structure. The file in this structure is regarded as the continuous sequence of the data bytes.
- **Record structure:** In this, the data files are composed of records in sequence.
- **Page structure:** In this, the data files are composed of indexed pages of independent nature.

Is FTP secured in nature?

No, FTP is not at all secured by its design. FTP is from that time when cyber security was only a study of hypothetical field. In simple words, the transfers made using FTP are not in encrypted format. So, anyone who is capable of sniffing data packets can easily intercept the files. That is the reason why people turn towards FTPS rather than FTP. FTPS works exactly in the same way just like FTP but it helps by encrypting every data files so that the prying eyes cannot read the files even if they intercept the files.


USERNAME:
PASSWORD:
LOGIN

Chapter 14: Remote Login

Remote login, also known as remote access, is the technique which is being used for accessing a system of computers like office network computer or home computer from a location which is remote in nature or is much away from the physical location of the system. This technique allows the office employees to keep up with their work offsite, like at their home or at any other place, while still accessing a network or computer at a distance, for example, office network. Remote login or access can be easily set up with the use of LAN or local area network, WAN or wide area network or even with the help of VPN or virtual private network so that all the systems and resources can be accessed from a remote distance.

Remote login can be created through a line which runs in between the computer of the user and an organization's or company's LAN. It is also possible to establish a connection between the LAN of a company and a remote LAN by the use of a dedicated line. This form of lines provides great speeds but also has the drawback of being very expensive. Another way of establishing remote login connection is by the VPN. VPN is a network which uses the internet for connecting with the remote sites and also the users together. This form of network uses encryption and also tunneling for the purpose of accessing the network of a company. This might turn out to be the best choice for those organizations which are small in size.

There are other means for establishing remote login that includes the using of wireless network, integrate services, cable modem, digital network or digital subscriber line. For the purpose of establishing a remote login

connection, both the remote computer or server and the local machine needs to have software of remote-access. There are various service providers that can be found today which provides remote access services via the internet.

Remote desktop software

One of the most sophisticated forms of remote login is remote desktop software. It allows the user of one computer to interact and see the actual desktop interface of another system. For setting up remote desktop access, both the computers, i.e. the computer of the client and the computer of the server need to be configured on the remote desktop software for establishing a connection. After being connected, the software opens up a window directly on the host computer which contains the view of the client's desktop.

The client computer can also maximize the window of the program for taking up the complete screen which will depend on how the software works on both the systems and what is the screen resolution of both the screens. The latest versions of Windows OS offer users with Remote Desktop Software which is only available for those computers which are running on either Enterprise, Professional or Ultimate version of the OS. When it comes to Mac, the Apple Remote Desktop Software is designed only for the business networks and the users are required to buy the same

separately. The ecosystem of Linux offers users with various types of solutions regarding remote desktop.

However, there are various types of remote access programs which are non-native in nature which the user can install on their system and then use the same in place of the desktop tools which comes built-in. Most of them function absolutely in the proper way in most of the OS of today. Many of the remote desktop solution today rely on the technique of virtual network computing. The packages of software which are based on virtual network computing works across various OS.

Remote accessing of files

The basic remote login software allows access of files on the system that can be read and also written on the system of the client. The technology of virtual private network offers remote login and functionality of file access across WAN. For a VPN to function properly, the client software is required to be present on both the systems. The client/server software which is based on SSH protocol can be used as an alternative to VPN for remote access of files. SSH offers an interface of command line to the system of the target. The task of sharing files within a local area network such as within home is not actually considered to be an environment of remote access even if it is actually remotely accessing the system of other device.

Is using remote desktop safe?

All the programs which are used for connecting remotely to your computer are most of the times safe. But, like all other software, there are some which go through some malicious process for the purpose of information stealing, installing malicious programs on another system, deleting important files and many others. In order to make sure the security of your system, try to disable those programs of remote desktop which you no longer use. You can also disable some of the functionalities of the program. You can easily disable remote desktop in Windows along with other OS.

Chapter 15: Networking In Detail

Computer networking functions with various components and systematic parts, all of which functions together for making the connection to a network a successful one. Let’s have a look at some of the primary components of networking.

Protocols

Network protocols help in defining the various conventions and rules for the purpose of communication between various devices in a network. The protocols of networking include various mechanisms for all the network devices for identifying and making connections with one another along with formatting the rules which help in specifying how the data is going to be packaged into received and send messages. Some of the network protocols also support compression of data and acknowledgement of the message which is designed for the high performing and reliable form of network communications. The network protocols incorporate all the constraints and requirement of processes for the initiation and accomplishment of communication between the routers, computers, servers and other devices which are network-enabled. The network protocols need to be confirmed as well as installed by both the sender and the receiver for ensuring data or network communication.

The modern network protocols use generally the techniques of packet switching for sending and also receiving messages in the form of data packets. Data packets are nothing but subdivided messages which are broken into pieces. The data packets are collected at the destination and then reassembled for getting the complete message. There are various types of network protocols which have been developed and designed for some specific functions in specific environments.

Internet Protocol

IP or the internet protocol family is composed of a set of related protocols of networking. Besides having internet protocol itself, there are also

various higher class protocols such as UDP, TCP, FTP and HTTP. All such protocols integrate with the internet protocol for the purpose of providing many more added capabilities. There are some lower-level internet protocols as well such ICMP and ARP which coexists within the family. The higher-level protocols which belong to the family of IP have much closer interaction with the applications such as web browsers. The lower-level protocols interact with the adapters of a network along with some other hardware of the computer.

Wireless Network Protocols

The wireless networking system now has turned out to be commonplace which is mainly because of Bluetooth, Wi-Fi and LTE. There are wireless network protocols that check the functioning of wireless networks. The network protocols which have been designed for the purpose of wireless networking needs to support roaming in mobile devices and also deal with various issues like network security and variable rates of data.

Network Routing Protocols

The network routing protocols are the specially designed protocols which have been designed to be used specifically for the network routers. A network routing protocol is capable of identifying several other routers on the network, manage the destination of the messages of a network, manage the message pathways which are called routes and also makes dynamic decisions on routing. Some of the most common protocols of routing include OSFP, EIGRP and BGP.

TCP or Transmission Control Protocol

The TCP or Transmission Control Protocol is regarded as the core protocol of the IP suite. It originates in the implementation of a network in which it has complemented the IP. So, the entire suite is also known as TCP/IP. TCP helps by providing a reliable system of delivery of octet streams over the network of IP. The main characteristics of TCP include checking of errors and ordering. All the major forms of internet-based applications like email and the World Wide Web along with file transfer relies on TCP.

How are networking protocols implemented?

Most of the modern operating system of today comes with in-built software services which help in implementing support for some of the network protocols. Various applications such as web browsers come with software library which supports high-level protocols when needed by the application for functioning. For some of the lower level protocols of routing and TCP/IP, the support is being implemented directly within the hardware for improving the overall performance.

Each of the data packets which are transmitted and received by the destination over the network consists of binary data, zeros and ones which helps in encoding the message contents. Most of the protocols of networking add up small header at the starting of every data packet for the purpose of storing information about the sender of the message along with the intended destination. Some of the protocols also add up footer at the very end of data packets. Each of the network protocols comes with the capability of identifying all the messages of its own form and then process

the header along with footer as parts of the moving data across the devices.

A large group of protocols related to networking which functions together at both the higher and lower levels is known as protocol family. Some of the most common protocols which are used are HTTP with default port 80, FTP with default port 20/21, SSH with default port 22, Telnet with default port 23 and DNS with default port 53.

Layers of the OSI Model and Its Functions

The OSI model or the Open System Interconnection model is an architecture of 7 layers in which every layer performs some specific function. All the layers work in close collaboration for the purpose of transmitting data from one system to the other all around the globe.

- **Physical Layer:** The layer at the bottom of the OSI model is the physical layer. It performs the duty of establishing an actual physical connection between the concerned devices in a network. All the information in the physical layer is stored in the form of bits. At the time of receiving the data, the physical layer receives the signal and then converts the same into 1s and 0s. It is then sent to the layer of data link which puts back the frame together. Functions of the physical layer are:
    1. **Bit synchronization:** This layer helps in bit synchronization by providing a clock. The clock provided by the physical layer is responsible for controlling both the sender and the receiver and thus provides synchronization at the level of bit.
    2. **Bit rate control:** This layer is also responsible for defining the rate of transmission which is the total number of bits sent out every second.
    3. **Physical topology:** This layer determines the way in which all the nodes and devices are going to be arranged in the network which are star, bus and mesh topology.

4. **Transmission mode:** This layer determines how the data is going to flow in between the connected devices. The possible modes of transmission are: simplex, full-duplex and half-duplex.

- **Data Link Layer:** This layer is the second layer right above the physical layer. It is responsible for message delivery from node to node. The primary function of the data link layer is to make sure that the transfer of data is absolutely free from errors while travelling from one node to the other, right over the 1st layer i.e. the physical layer. After a packet has arrived in a network, it is the duty of this layer to transmit the same to the host by using its MAC address. The data link layer is being divided into two layers: Logical Link Control and Media Access Control.

The packet which is received from the network layer is then divided into frames which depend on the size of the Network Interface Card or NIC. This layer also encapsulates the MAC address of the sender and the receiver in the data header. The functions of the data link layer are:

1. **Framing:** The main function of the data link layer is framing. It provides the sender with a way for transmitting a set of bits which are meaningful for the receiver. This is achieved by the attachment of special patterns of bits right at the beginning of the frame and at the end.
2. **Physical addressing:** After this layer is done with the job of framing, it adds physical addresses also known as MAC

addresses for the sender or of the receiver in the frame header of each.

3. **Error control:** This layer comes with the mechanism of controlling errors in which errors are detected and the lost or damaged frames are retransmitted.
4. **Flow control:** The rate of data needs to be constant on both the sides otherwise the data might result in getting corrupted. So, with the help of flow control, the data amount is coordinated which can be sent before receiving the acknowledgement.
5. **Access control:** When a single channel of communication is being shared by various devices, the sub-layer of MAC in the data link layer helps in determining which device has the control of the channel at some given time.

- **Network Layer:** This layer functions for transmitting data from one host to another which is located in some other network. The network layer also looks after packet routing which means it helps in selecting the path which is the shortest of all for the purpose of transmitting the packet, from the total number of routes which are available. The network layer also places the IP addresses of the sender and the receiver in the header. The functions of the network layer are:

  1. **Routing:** The protocol of the network layer determines that which route will be the best for the packet from the source to the destination. This function performed by the network layer is called routing.

2. **Logical addressing:** For the purpose of identifying each of the devices on the internetwork in a unique way, the network layer helps by defining a scheme of addressing. The IP address of the sender and the receiver are placed in the header which helps in distinguishing each and every device in a unique and universal way.

- **Transport layer:** The transport layer helps by providing all the required service to the application layer and also takes up services from the network layer. Segments are those data which are present in the transport layer. It helps in end to end message delivery. This layer is also responsible for providing the acknowledgement after successful transmission of data and also re-transmits any data if any form of error is found.

At the sender side: The transport layer receives the data which has been formatted from the layers above it and performs segmentation. After segmentation is done, it also implements error and flow control for ensuring that the data is transmitted properly. It also adds up port number of the sender and the receiver in the header and then forwards the data which has been segmented to the network layer. The sender of the data needs to have the port number which is associated with the application of the receiver. The destination port number is generally manually configured or is configured by default. For example, when any web application sends any request to the web server, it uses the port number 80 because it is the port number which has been assigned for the web applications by default. Many of the applications come with default assigned port number.

At the receiver side: The transport layer reads up the number of a port from the header and then forwards the packet of data which it has received for the respective application. This layer also performs reassembling and sequencing of the data which is segmented.

Functions of the transport layer:

1. **Segmentation:** The transport layer accepts the sent message from the session layer and then breaks it onto several smaller units. The segments which are produced after segmentation comes with a header associated with every segment. The segmented message is reassembled by the transport layer at the destination.
2. **Service point addressing:** For the purpose of delivering message to the proper process, the header of the transport layer also includes an address type which is called the port address or service point address. By determining this specific address, the transport layer makes sure that the intended message gets delivered to the right process.

Services provided by transport layer:

1. **Service oriented to connection:** This whole process is done in three phases:

-Connection establishment

-Transfer of data

-Disconnection or termination

In this form of transmission, the device on the receiver's side sends out an acknowledgement intended for the source right after a data packet or group of packet has been received by the destination. This form of transmission is very secure and reliable as well.

2. **Connection less service:** This process is one phase in nature and it includes transfer of data. In this form of transmission, the receipt of a packet is not at all acknowledged by the receiver. This form of transmission approach allows a faster mode of communication in between the devices. However, the connection oriented service is much more reliable than the connection less service.

- **Session layer:** The session layer serves the function of connection establishment, session maintenance, authentication and also security of the session. The functions of this layer are:

1. **Establishment of session, maintenance of session and termination:** This layer helps in the establishment of the two processes, uses and also terminates the connection.
2. **Synchronization:** The session layer helps in adding up checkpoints which are regarded as the points of synchronization by a process into the data. The points of synchronization help in identification of the errors in order to ensure that the data has been re-synchronized in the

proper way. It also ensures that the message ends are not prematurely cut for avoiding loss of data.

3. **Dialog controller:** This layer allows the two systems to begin the communication with one another in full-duplex or half-duplex.

- **Presentation layer:** The presentation layer is also known as the translation layer. The data which is received from the application layer is extracted in this layer and is also manipulated as per the requirements of the format for transmitting the same over the network. The functions of this layer are:

  1. **Translation:** It helps in the process of translation such as from ASCII to EBCDIC.
  2. **Encryption and decryption:** The encryption of data translates the whole data into some other form or code. The data which is encrypted is known as the cipher text. The data which is decrypted is known as the plain text. For the purpose of data encryption and data decryption, a key value is used by this layer.
  3. **Compression:** This layer helps in reducing the total number of bits which is to be transmitted into the network.

- **Application layer:** At the top of the stack of layers of the OSI model exists the application layer. It is a layer which is implemented by the applications in a network. The applications of the network produce the data which is to be transferred across the network. The application layer serves as

a window for the services of applications for accessing the network and also for the purpose of displaying the information which is received to the user. Some examples of network applications are web browsers, messengers etc. The functions of this layer are:

1. Mail services
2. Network virtual terminal
3. FTAM or file transfer access and management
4. Directory services

The OSI model as the reference model and is not at all implemented for the internet as it is considered as being outdated. TCP/IP model is used in place of the OSI reference model.

VLAN

VLAN or virtual LAN is a group composed of devices on one or more than one LANs which are configured for communicating in a way as if all of them are attached with the same wire whereas they are located at several different segments of a LAN. VLANs are extremely flexible in nature as it is based on a logical connection in place of a physical connection. VLANs help in defining the domains of broadcasting in a network of Layer 2 nature. A broadcast domain is nothing but a set of all the devices which will be receiving frames of broadcast originating from any of devices within that set. The broadcast domains are bounded typically by the routers as the routers will not be forwarding the frames of the broadcast.

The switches of Layer 2 create broadcast domains which are completely based on the switch configuration. Switches are the multiport bridges which allow in creating several broadcast domains. Each of the broadcast domains is similar to a distinct form of a virtual bridge which can be found within a switch. You can easily define one single or many bridges of virtual nature which are available within a switch. Each of the virtual bridge which a user creates within the switch helps in defining a new VLAN or broadcasting domain. It is not possible for traffic to directly pass to some other VLAN between two switches or within that switch.

VLAN acts just like a sub-network. VLAN eases up the job for the network administrators to divide one single switched network for matching the security and functional requirements of the systems without the need of running new cables or without making any major changes in the present infrastructure of the network. VLANs are generally set up by the large-

sized businesses for the purpose of re-partitioning the devices for the better management of traffic.

VLANs also help in improving the all-round performance of the network simply by grouping all the devices together which communicates the most. VLANs also provide proper security for the large-sized networks by providing a greater degree of control across which the devices have access to each other. One or more than one network switch can support several independent VLANs by creating Layer 2 subnet implementation.

VLANs and its types

There are various types of VLANs present. Let's have a look at them.

- **Protocol VLAN:** This type of VLAN comes with traffic handled base on the protocol. The switch on the network will either forward or segregate the traffic based on the protocol of the traffic.
- **Static VLAN:** It is also known as port-based VLAN. It requires the administrator of a network for assigning the ports on the network switch to a network of virtual nature.
- **Dynamic VLAN:** It allows the network administrator to define the membership of the network which is based on the characteristics of the device which is in opposition to the switch port location.

How does VLAN work?

Ports or interfaces on the switches can be assigned to one single or more than one VLANs which enable the systems to get divided into various logical groups which are based completely on the departments with which they are associated with. It also establishes the rules about the systems about how the systems in the separate groups are going to communicate with one another. These separate groups can range from practical and simple to legal and complex. Each of the VLAN provides access of data link to all the hosts which are connected to the switch ports configured with the similar VLAN ID. The VLAN tag is a field of 12-bit in the header of the Ethernet which provides support for 4,096 VLANs per domain switching. The tagging of VLAN is standardized in the IEEE 802.1Q and is also called Dot1Q.

When a frame is received of untagged nature from a host which is unattached, the VLAN ID which is configured on the interface is added up in the header of the data link frame by using the format 802.1Q. The frame of 802.1Q is forwarded towards the proper destination. Each of the switches uses the tags for keeping each traffic of the VLAN separate from the traffic of the other VLANs, forwarding the same only to the place where VLAN is configured.

The trunk lines in between the switches can handle several VLANs by using the tags for keeping them all segregated. A trunk line is a line of communication which has been designed for carrying several signals for the purpose of providing network access in between two different points. When the frame reaches the ultimate switch port of the destination, the tag of VLAN is removed just before the frame is transmitted to the device of destination.

It is possible to configure multiple VLANs on one single port with the use of trunk configuration in which each of the frames sent through the port is being tagged with the VLAN ID. The interface of the neighboring device which might be on some other switch or host which supports 802.1Q tagging will require to support the configuration of trunk mode for transmitting and receiving the frames which have been tagged. Any of the Ethernet frames which are untagged are assigned to a VLAN of default nature which can also be designated in the configuration of a switch.

When a switch which is VLAN-enabled receives an Ethernet frame of untagged nature from an attached host, it adds up the VLAN tag which is assigned to the interface. The frame is then sent forward to the host port along with the MAC address of the destination. Broadcast multicast and unknown unicast is then forwarded to all the ports in the VLAN. When any previously unrecognized or unknown host replies to an unknown frame of unicast, the switches get to know about the host location and do not flood the host with the subsequent frames which were addressed for that host.

The STP or Spanning Tree Protocol is being used for creating a topology of loop-free nature among all the switches in every Layer 2 domain. As per the regulations of VLAN, an instance of STP can be used which in turn enables the various topologies of Layer 2 or a MISTP or multi-instance STP can be used for reducing the overhead of STP in case the topology is also the same among the multiple VLANs. STP blocks away the forwarding on the links which might produce some forwarding loops and thus creating a spanning tree from the selected switch of root. The concept of blocking means that some of the links will not at all be used for the purpose of forwarding unless and until there is a failure in some other part of the network which causes the STP to turn the link a part of any forwarding path of active nature.

Advantages and disadvantages of virtual LAN

VLAN comes with some basic advantages such as reduced traffic of broadcast, proper security of network, confinement of broadcast domain and easy administration of network.

When it comes to the disadvantages of VLAN, it comes with the limitation of 4,096 VLANs only for per switching domain which creates lots of problems for the large-sized providers of hosting, which also often comes with the need to allocate hundreds of VLANs for the customers. For addressing this limitation, several other protocols such as NVGRE, VXLAN and Geneve supports larger sized tags and also comes with the ability of tunneling frames of Layer 2 within the packets of Layer 3.

Routing

Routing is the process by which path is selected along which the requested data is to be transferred from the source of origin right to the receiver or destination. Routing is done by a special network device which is known as a router. The router functions at the networking layer in the OSI reference model and in the internet layer in the model of TCP/IP. A router is a device which is used in networking which helps in forwarding the data packets based completely on the available information within the header of the packet along with the forwarding table. For the purpose of routing the data packets, various routing algorithms are used. The routing algorithm is a software which helps in deciding the path which will be the optimal one for the data packet to be transmitted to the destination.

The protocols regarding routing use metric for determining the perfect and fastest path for the delivery of the packet. Metric is nothing but the standard which is used for measurement such as bandwidth, hop count, current path load, delay etc. which is being used by the algorithm of routing for determining the optimal delivery path. The algorithm of routing maintains and also initializes the table of routing which is required for the process regarding the determination of path.

Metrics of routing

Routing metrics along with costs are used by the router for determining the most suited route up to the destination. The factors which are used by the routing protocols for determining the fastest path are known as metrics. For some of the routing protocols, they use static form of metrics

whose value cannot be changed and some of the protocols use the dynamic version of metrics whose value can be changed and then assigned by the administrator of the system. The most common values of metrics are:

- **Hop count:** It is the metric which helps in specifying the total number of passes across the devices of internetworking like the router. A data packet needs to move in a route for travelling right from the source to the destination. If the protocol of routing takes the hop as a primary value of the metric, the path which comes with the least hop count is going to be considered as the fastest and the best path for moving the data packet from the source to the destination.
- **Delay:** It is the time which is taken by the network router for processing, queuing and transmitting one datagram to the interface. The protocols of routing use this form of metric for determining the values of delay for each and every link which are in the path from end-to-end. The path which will be having the lowest value of delay will be taken as the best path for the data packet.
- **Bandwidth:** The capacity that a link has is called the bandwidth of that link. The link bandwidth is measured as bits per second. The link which has the highest rate of transfer such as gigabit will be preferred over any other link which comes with a link capacity of like 52 kb. The protocol of routing will be determining the capacity of bandwidth for each and every link along the path and the link which comes with overall higher bandwidth will be taken as the perfect route for moving the packet from source to destination.

- **Load:** Load is the measurement with which it is measured that the resource of a network like network link or router is busy to which extent. The load can be measured in various ways such as packets processed every second, utilization of CPU etc. In case the traffic increases, the value of load will also increase. In simple words, the load value will change in relation to the change in the network traffic.
- **Reliability:** It is a factor of metrics which might be composed of only one fixed value. It depends on the links of the network along with its value which is dynamically measured. There are some forms of networks which go down more often when compared to others. After a network fails, there are some links of the network which gets repaired more easily when compared with the other links of the network. Any factors of reliability can be considered reliability rating assignment which is in numeric values in general and is assigned by the administrator of the system.

Routing and its types

Routing is of various types and it can be easily classified into three broad categories:

- **Static routing:** It is also known as the nonadaptive form of routing. With this routing technique, the administrator of a network manually adds the preferred routes within the table of routing. A router sends the data packets towards the destination by following the route which is defined by the

administrator. In this routing technique, the decisions of routing are not at all made based on the topology or conditions of a network.

Advantages:

1. **No overhead:** It has no form of overhead on the usage of the CPU of the network router. Therefore, a cheaper variant of the router can easily be used for obtaining static routing.
2. **Bandwidth:** It has no usage of bandwidth between the network routers.
3. **Security:** It provides proper security as the administrator of the system is allowed control only over the process of routing to a specific network.

Disadvantages:

1. For a large-sized network, it turns out to be a very difficult task for manually adding each of the routes to the table of routing.
2. The administrator of the system is required to have proper knowledge of the network topology as he needs to manually add each of the routes.

- **Default routing:** It is a technique in which the network router is configured for sending all the data packets to the exact same hop device and it is not necessary that whether it belongs to

that specific network or not. A data packet is being transported to the device for which it has been configured in the default form of routing. Default routing is being used when the networks only deal with one single point of exit. It is very helpful in situations when the transmission network bulks need to transmit the packet of data to a similar hop device. When any particular route has been mentioned in the table of routing, the network router will be selecting the route which has been specified rather than using the default route. The default path or route is selected by the router only when any specific route has not been mentioned in the table of routing.

- **Dynamic routing:** It is also called adaptive routing. In this technique of routing, the network router adds up a new route in the table of routing for every single data packet in response to all the changes which has been made in the topology or condition of the network. The dynamic protocols are being used for the purpose of discovering the brand new routes for reaching the destination. In this form of routing, OSPF and RIP are the only protocols which are used for the purpose of discovering new routes. In case any of the routes go down, the automatic adjustment will be done for reaching the destination.

Advantages:

1. It is very easy to configure.

2. It is the most effective of all for selecting the perfect and best route in response to all the changes in the topology or condition of the network.

Disadvantages:

1. It is very expensive with respect to the bandwidth and CPU usage.
2. It is not much secure when compared with static and default routing.

The dynamic protocol needs to have these features:

- All the network routers need to have the similar protocol of dynamic protocol for the purpose of exchanging the routes.
- In case the network router discovers any form of change in the topology or condition of the network, the router needs to broadcast this information among all the other routers.

Network Services

DHCP

Also known as Dynamic Host Configuration Protocol, is a protocol for network management which is used dynamically for the purpose of assigning IP address for the devices or for any node on any network so that is possible to establish communication by using the IP. DHCP manages centrally and also automates all of these configurations instead of having the administrators of a network to manually assign the IP addresses for all the networking devices. It is possible to implement DHCP on small-sized local networks and also on large-sized enterprise networks. DHCP helps in assigning new IP addresses for every location when the networking devices are moved from one place to another. This means the administrators of the networks are not required to manually configure the devices with new IP addresses when it is moved to a completely new location within the network.

How does DHCP work?

DHCP functions at the application layer of TCP/IP model for dynamic assigning of the IP addresses to the DHCP clients and for allocating TCP/IP configuration to the clients of DHCP. This is composed of subnet mask, IP addresses, default gateway and DNS address. DHCP serves as a client-server protocol. In this, the servers manage a unique pool of IP addresses along with various information regarding the configuration parameters of the clients and also assign address from those pools of address only. The clients which are DHCP enabled send out requests to the server of DHCP whenever they connect with the network.

The clients which are configured with DHCP broadcast requests to the server of DHCP and requests information regarding network configuration for that local network with which they are connected or attached. The clients generally broadcast their query for information as soon as they boot up. The server of DHCP responds to the requests of the clients by providing information regarding IP configuration which was specified previously by the administrator of a network. This also includes one particular IP address as well for that time period which also called a lease and the allocation is valid for this one. At the time of refreshing any assignment, a client of DHCP requests out for the same parameters but the server of DHCP might also assign a new IP address completely based on the policies which are set by the administrators of the network.

The server of DHCP also manages a proper record of all those IP addresses which it allocates to the nodes of a network. In case any node is relocated within the network, the server of DHCP identifies it quickly by using MAC address which helps in preventing the accidental configuration of several devices by using the same IP address.

DHCP is not at all a routable form of protocol nor is it secure. DHCP is limited within a LAN which means one server of DHCP every LAN is enough for usage in case of any failover. The larger form of networks might also have WAN which contains several individual locations. Depending completely on the connections in between the points and the total number of clients in every location, several servers of DHCP can be set up for the purpose of handling address distribution.

In case the administrators of a network want a server of DHCP to provide IP addresses for multiple subnets on any given network, they are required to configure the relay services of DHCP which located on the interconnecting routers across which the requests of DHCP needs to cross. These agents help in relaying the messages between the clients of DHCP and servers which are located on various subnets. DHCP lacks the feature of built-in mechanism which would have allowed the clients and the servers to authenticate one another. Both the clients and the servers are susceptible to deception and to attacks as well.

Static DHCP leases VS. Dynamic DHCP leases

By having a dynamic DHCP, the client does not own an IP address which has been assigned but instead of that leases the address for a period. Every time when a device with a dynamic form of IP address gets powered up, it needs to communicate with the server of DHCP for leasing another IP address. The wireless types of devices are the examples of those clients which are assigned with dynamic IP addresses whenever they connect with the network. The devices which are assigned with a static form of IP address have permanent IP addresses. They are used for various devices such as switches or web servers.

Under a setup of dynamic DHCP, the clients need to perform certain tasks that result in termination of its address and then reconnect with the network with the use of other IP address. The lease times of DHCP varies depending on the period of time for which a user needs the internet connection at one specific location. The devices with a dynamic IP

address, release the IP addresses when the lease of their DHCP expires and then the devices request for renewal of IP addresses from the server of DHCP in case they want to stay online for a longer time. The server of DHCP might assign a completely new IP address instead of just renewing the old IP address.

NAT

For accessing the internet, a user needs one IP address which is public in nature. Private IP addresses can be used in those networks which are private in nature. The primary goal of NAT is to permit several devices to get access to the internet by using one public address only. For the purpose of achieving this, it is required to translate the IP address to a public IP address. NAT or Network Address Translation is the process by which one or more than one local form of IP address is readily translated into one or more than one Global form of IP address and vice versa for the purpose of providing internet access to all the local hosts.
Also, NAT translates the port numbers which means it helps in masking the port number of the host with some other port number within the data packet which will be moved to the destination. NAT then makes the required entries of port numbers and IP addresses in the table of NAT. It operates on the firewall or router generally.

Types of NAT

There are three ways in which NAT can be configured.

- **Static NAT:** In this form of configuration, one private IP address is mapped with one public IP address which means one-to-one mapping between the local and the global address. This form of configuration is generally used for the purpose of web hosting. This form of configuration is not at all used in the organizations as there will be various devices which will need access to the internet at the same time.
- **Dynamic NAT:** In this form of NAT configuration, one private IP address is being translated into one public IP address from a huge pool of IP addresses of public nature. In case any IP address from a pool is not free, the packet will be dropped off as only a specific number of IP addresses can be translated from private to public.
- **Port address translation or PAT:** This configuration is also called NAT overload. In this form of configuration, various private IP addresses are translated into one single public IP address. For the purpose of distinguishing the traffic, port numbers are used.

Advantages of NAT

- NAT helps in conserving public IP addresses.
- It helps in maintaining proper privacy as the IP address of the device which will be receiving and sending traffic will be in hidden form.
- It helps in the renumbering of address when any network evolves.

Disadvantages of NAT

- The translation of IP addresses might result in delay in path switching.
- There are various applications which will not be functioning when NAT is enabled.
- It complicates various protocols of tunneling like IPsec.

Switching

VLAN Trunking Protocol

VTP or VLAN trunking protocol is used for maintaining proper continuity and consistency throughout a network. VTP allows the users to add up, remove or rename VLANs which is propagated to some other switches within the domain of VTP. However, there are certain requirements for the VTP to communicate about VLAN information between the switches. The version of VTP needs to be on similar on all the switches which the user needs to or wants to configure. Also, the domain name of VTP needs to be same on all the switches. For VTP communication, one of the switches needs to act like the server or be the server.

Modes of VTP

There are three different modes of VTP:

- **Server:** All the switches are set for this mode by default. This mode allows the users to add, delete or create VLANs. Any kind of change that the user wants to make needs to be done in this mode. Each and every change which is made in this mode will be propagated to every switch which belongs to the same domain of VTP.
- **Client:** In this mode of VTP, the switches receive all the updates and are also capable of forwarding all those updates to the other switches.

- **Transparent:** This mode of VTP forwards only the summary of VTP advertisements via the trunk line. The switches of this mode can create their own database of local nature which can keep secrets from all the other switches.

Spanning Tree Protocol

STP or spanning tree protocol is being used for creating a loop-free network by the process of network monitoring for tracking all of the links and then shutting down those which are less redundant in nature.

STP and its types

- **802.1D:** This type of STP is also called CST or common spanning tree. This is a standard of STP which has been developed by the IEEE which selects one single root bridge only for every topology. All of the traffic in the network flows in the same path but this might not be good always as there might be issues in which the path which has been optimized for reaching the VLAN is completely different from the path which has been obtained after electing root bridge. It is also very slow in nature as it takes minimum 32 seconds of time for converging.

Advantages:

It requires very less CPU and memory.

Disadvantages:

It comes with a lesser percentage of optimization as the path which is calculated as the perfect one to root bridge might turn out to be not the best path for reaching the network. It also offers no form of load balancing.

- **802.1w or RSTP:** RSTP or rapid spanning tree protocol is the standard which has been developed by the IEEE for providing a faster rate of convergences that CST. However, it also holds a similar idea of finding a single root bridge within the topology.
- **RPVST:** Also known as rapid per VLAN spanning tree, is a standard which has been developed by Cisco for providing faster rates of convergence than RSTP and also finds out separate instances for 802.1w for every VLAN. However, it needs more memory along with CPU when compared with the other standards of STP.

Routing Configuration

OSPF

Also known as Open Shortest Path First protocol, is a form of link-state routing protocol which helps in finding the best path between the destination and the source router by using up its own shortest path first. OSPF protocol has been developed by IETF as an IGP or interior gateway protocol which is the protocol for moving the packets within a very large system of autonomous nature or domain of routing. It acts in the network layer and works on the protocol number 89.

Terms of OSPF

- **Router ID:** It represents that IP address on the router which is the most active of all. The highest address of loopback is considered at the first place and in case no form of loopback has been configured, the IP address which is the highest active within the interface is considered.
- **Router priority:** It is a value which is assigned to the router which is operating OSPF. It is 8 bit in nature and helps in electing BDR and DR within a broadcast network.
- **DR or designated router:** It is elected for minimizing the total number of adjacency which has formed.
- **BDR or Backup designated router:** BDR acts as the backup of DR within a broadcast network. Whenever DR performance goes down, BDR assumes the role of DR and starts to perform the functions of DR.

BDR and DR election

The election of BDR and DR takes place within a broadcast network or within a multi-access network. The criteria for election are:

- The router which has the highest priority of router will be elected as the DR.
- In case there is any form of a tie in choosing the router priority, the router ID which is the highest will be considered.

EIGRP

EIGRP or enhanced interior gateway routing protocol is a form of dynamic routing protocol which is being used finding the best route between two devices of layer 3 for delivering the data packet. It functions at the network layer of the OSI reference model. It uses up protocol number 88 for functioning. EIGRP uses the method of metric for finding out the perfect path between the two devices which operates EIGRP.

Characteristics of EIGRP

EIGRP functions with the following characteristics:

- It works with an advanced form of operational efficiency.
- It acts as a classless protocol of routing.
- It comes with the capability of both distance vector and link state.
- It comes with some unique features like RTP or reliable transport protocol, DUAL or diffusing update algorithm and all forms of updated information about the neighbors.
- It offers a faster rate of convergence as it precalculates all the routes and also does not broadcast timer packets prior to convergence.

It uses delay, load, bandwidth and reliability for calculating the metrics for the table of routing.

Chapter 16: Troubleshooting of Network

A complete setup of network uses up various components, hardware, configurations of network, setups and operating systems which works together for making a network successful. However, it might happen that some of the components stop functioning due to some glitch or error. Such a situation might result in the complete shutdown of a network which can also call up huge losses for the large-sized networks. So, all that is needed in such a situation is troubleshooting of the network for making the network functional again.

Adapter resources

Try to make sure that the adapter of the network has been installed properly and has also been detected by the computer without any hassle. If you are using Windows OS, open up the device manager and then verify that there is no form of error. In case there is any form of discrepancy in the adapter of the network or if it has been detected by the computer as other device, you need to check that whether the adapter has been installed properly or not.

Verifying the connections

In case you are using a wired form of network, make sure that the network cable has been connected properly and the LED indicator right next to the network jack is blinking. A solid green LED or light means that the cable has been attached properly and it is receiving signals from the network. In

case there is no light in the indicator, it might indicate that the card is not good or it has not been connected in the proper way or there is any form of error in the network signal. If you are on a small-sized local network, check all the hubs and routers and make sure that the cables are connected properly in all.

In case you are using a wireless network like a laptop, make sure that the Wi-Fi option in your laptop has been turned on. If you are still facing any issue, make sure that you have selected the proper Wi-Fi network. Also, check the connection of the Wi-Fi router for ensuring that the router is receiving signal from the internet.

Functionality of adapter

You need to verify that the card of the network is able to ping itself by the use of ping command. If the local host is properly functioning you will receive replies from the host. In case you receive any error such as time out, check that the network card has been properly installed and the drivers are updated as well.

Chapter 17: Networking on PC and MAC

PC and MAC are completely two different forms of system which uses two different operating systems. A PC generally runs of Windows or Linux whereas MAC uses its own OS for functioning. There is a very common question that is it possible to establish a network between PC and MAC and the answer to this question is yes. It is not at all a strenuous job and can be done within a few minutes.

Steps to follow

- Right before you start with the process, make sure that you have set up the IP in both the PC and MAC systems. Note down both the IP addresses as it will be used in setting up the connection.
- Set up a password for your PC sharing system which can be found in the network and sharing option.
- Put the PC running on Windows or Linux and the MAC system in the same workgroup.
- In the MAC system, open up system preferences and then select the adaptor of the network. Select the advanced option which is available on the right pane and select wins tab and type in the same name of the workgroup as you are using in the system of PC.

- Create a folder named as shared in the PC system.
- Create a folder named as shared in the MAC system.
- The next step is to open system preferences in the MAC system and select the option sharing under the option of internet & network. Check out the option of file sharing.
- Under the file sharing option, check share folder and file by using SMB.
- Now you will be able to connect both the systems and transfer files and folder between your PC running on Windows or Linux and the MAC system.

Make sure that nothing is in the encrypted format while sharing as with encryption turned on, the system of PC will not be able to log in the MAC system and share files and folders.

Conclusion

As you have completed reading the whole eBook, you have developed a clear perception about the basics of networking along with various protocols of the same. By now, you must have learnt the basic requirements for setting up a network and how can you speed up the functioning of your network. The protocols and the types of system that you choose will ultimately determine how your network is going to function. You are the one who can make a network function to its fullest.

With the help of various tools of networking along with its components, you can create your own network, whether you need one for your home or you need a large network for your business place. You have also learnt about various components of a network and how each of them functions in different forms of environment.

As you have leant about the basics of networking in this eBook, you can try out the other eBook on *Hacking With Kali Linux* from which you can learn about the various concepts of network hacking along with the security of your network. Kali Linux can help in testing the vulnerabilities in your network system which you can ultimately use for securing up your network. As the number of prying eyes is increasing day by day, it is very important for the network administrators to use the best components of networking and also perform regular security checks for the ultimate security infrastructure.

If you find this book helpful for your business in any way, kindly leave a review on Amazon.

Hacking with Kali Linux:

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

JOHN MEDICINE

Introduction

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

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

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

Chapter 1: Analyzing and Managing Networks

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

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

Most of the IT administrators of today just ask their staffs to opt for the powerful automated technology for network assessment. It is more or less like a temptation of the new technological innovations. Most of the people are of the notion that the available tools for network analysis are very effective, useful and instructive as well. However, if you really want to analyze your network in the proper way, opting for the automated tools might not be the right option.

Overlooking the sirens

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

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

Assessments and the various methods

You, as the owner of a business or organization, can ask your staffs to perform certain measures for the ultimate monitoring of your network.

- **Verifying the forwarding configuration policy of firewall:** You can use traffic-generating tools like ping for verifying that the rules of firewall blocks or allows the traffic between the trusted or shared networks and external networks. It needs to function according to the policy of security which you want to enforce in the network.
- **Verifying the configuration policy of egress traffic:** For this, you need to place a testing system just outside your network firewall. On the system of testing which has been placed outside the firewall, try to run applications like Port Listener. You need to use port scanner like nmap and then try to connect to the system of testing at each and every port of listening that you have configured. It needs to be done for confirming that the firewall is allowing access to all those services that you generally want to make accessible to the web and restricts all those services that all the users tried to connect with your trusted networks. The restricted services will only be allowed depending on the AUP or Acceptable User Policy.
- **Find out who is trying to probe into your networks and also from where:** Open up the log of your firewall. Select the source of traffic that is attempting or trying to probe into your network. Use a program of route analysis such as tracert or

traceroute for properly identifying the forwarded attack traffic path along with the IP addresses on that path, the service providers which are along the same path and the network from which the traffic of attack has originated. You can use several other utilities like whois, dig and nslookup for performing lookups of reverse DNS along with the whois queries. In the real situations, your website is generally the target of DDOS or distributed denial of service attack.

- **Try to take stock of the network:** An analysis program along with LAN traffic capture program like Ethereal helps in providing the most important information about the networks. By simply observing the application types which are in use, you can very easily identify the hosts which are providing the various unauthorized services. You can even determine if your employees within the organization are adhering to AUPs, whether any other harmful code and rootkits are trying to establish any type of back connections to the computer of the attacker and if your network is hosting any kind of spam bot.

Strategy for improvisation of the assessment skills

You can nurture the various skills of assessment with your staffs with the help of several exercises. You can start by introducing to your staffs the various techniques of information-gathering which are used by the attackers. Ask your staffs to perform scans of ping and then port the ping scans with the use of nmap. As they advance, introduce other complex

techniques like service fingerprinting. Let them assess whether the present measures of security are enough or not.

Chapter 2: Hacking Process

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

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

- **Reconnaissance:** This is the first step in the process of hacking. In this phase, the hacker tries all possible means for collecting information about his target. The means might include identification of target, finding the range of the target IP address, DNS records, network and many others. In short, the hacker collects all the contacts of a server or website. The hacker can do this by using various search engines such as maltego, research about the target, for example, a website or by using other tools like HTTPTrack for downloading an entire website for the purpose of later enumeration. By doing all these, a hacker can easily determine the names of the staffs, their designated positions in the organization and their email addresses as well.
- **Scanning:** After the hacker is done with collecting relevant information about the target, he starts with scanning. In this

phase, the hackers use various tools such as port scanner, dialers, sweepers, vulnerability scanners and network mappers for scanning the server or website data. In this step, the hackers seek for the information which can probably help them in executing an attack like the user accounts, IP addresses and the names of computers. After the hackers are done with collection of basic information, they move to the next step and start to test the target network for any other attack avenues. The hacker chooses to use various methods for helping them in mapping the network like Kali Linux. The hackers look out for automated system of email or simply based on the gathered information, they try to email the company staffs about various queries, for example, mailing an HR with a detailed enquiry about job vacancy.

- **Gaining of access:** Gaining access is the most important phase when it comes to the process of hacking. In this step, the hacker tries to design the target network blueprint with relevant information which is collected during the first and second phase. After the hackers are done with enumerating and then scanning, they might decide to gain access to the network based on the information.

Suppose, the hacker decides to use Phishing Attack. The hacker might try to play safe and so might use a very simple phishing attack for gaining access. The hacker might decide to penetrate from the department of IT. The hacker might find out that some recent hiring has been done and they are not to speed the procedures. The hacker sends a phishing email using the actual email address of the CTO by using a specialized program and will

send it out to all the techs. The email will have a phishing website that will gather the login ids and passwords. The hacker might use a number of choices such as website mail, phone app or something else for sending an email to the user and asking them to login into a brand-new portal of Google by using their relevant credentials. When the hackers use this process, they already have a special program running which is known as the Social Engineering Toolkit and uses it for sending an email along with the server address directly to the users by masking the same with tinyurl or bitly.

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

- **Maintaining server access:** Once a hacker gains access to a server, they try to keep the access safe for exploitation and attacks in the future. As a hacker owns an overall system, they can easily use it as their base for launching several other additional attacks. When a hacker gains access and owns the system, such system is known as zombie system. As the hacker gathers multiple email accounts, he can now start to test all the accounts right on the domain. At this point, a hacker tries to create a new account as an administrator and tries to blend in the system. As a precautionary measure, the hacker starts to search and identify all those accounts which have not been used for a very long time. The hacker changes the passwords of such accounts and then elevates all the privileges to the administrator just like a secondary account

for maintaining safe access to the target network. The hacker might also start sending out emails to all the other users with a type of exploited file like a PDF with reverse shell for extending their overall access. The hackers wait for any kind of detection in the system and when they get sure that there no one has detected any kind of disturbance in the system, the hacker starts to make copies of all the user data such as emails, contacts, messages, files and many other for later usage.

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

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


dev
etc
home
lib
lib64
lost+found
mnt
opt
private
root
run
srv
sys

Chapter 3: BASH and Python Scripting for Hackers

BASH Scripting

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

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

Shell types

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

Basics of BASH

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

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

Setting the permissions for execution

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

Running the script

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

Use of variables

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

Python Scripting

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

Adding the modules of Python

The standard library of Python along with the modules provide the hackers with a wide range of capacity that also includes exception handling, file handling, built-in data types, internet data handling, numeric and math modules, cryptographic services along with interaction with the IPs. Despite all the available pre-existing modules and standard libraries, you

might also need some third-party modules in addition to the existing ones. All the third-party modules which are available for scripting in Python are comprehensive in nature and that is the prime reason why a majority of the hackers try to opt for Python when it comes to scripting.

Formatting

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

Running files on Python

The process of running the files in Python is somewhat similar like BASH. You need to start with #! Followed by /usr/bin/python. This will indicate the system that you want to use the interpreter of Python. Following this,

you can enter your required command just like BASH. For running the script, you are required to change the permission first by using the chmod command.

Comments on Python

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

Variables

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

Functions

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

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

Chapter 4: Installation of Hacker ’ s OS Kali Linux

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

Kali Linux in detail

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

Why use Kali Linux?

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

- It comes with approx 600 tools for penetration testing.
- Kali Linux comes with multilingual support.

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

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

How can you install the OS Kali Linux?

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

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

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

Requirements for installation of the OS

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

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

Getting started with the process of installation

- **Start by installing VMware**

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

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

For download the OS, you can directly visit the official website of Kali Linux and select the version that you need. On the page of download, you will come across various hexadecimal style numbers. Those

numbers are for security tasks and you are required to check the image integrity right before downloading the OS.

- **Launching an advanced virtual machine**

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

Procedure of installation

- Once the machine powers up, you need to select the preferable mode of installation right in GRUB menu. Choose graphical installation and then select continue.
- The next few screens will be asking you for selecting the locale information like your preferable language, location of origin and also layout for the keyboard.
- Once you are done with all the additional local information, the installer will be automatically installing various additional components. It will then configure the settings related to your network. The installer will immediately prompt for your hostname along with the domain for completing the process of

installation. You need to provide all the appropriate and required information and then continue with the process.

- Now you are required to set up a password for the Kali Linux machine. You need to remember this password as long as you are going to use the machine.
- After you have set your password for the Kali Linux machine, the OS installer will prompt for setting up the time zone. It will then pause for partitioning of disk. The installer of OS will provide you with four different disk partition choices. The easiest option out of all is the Guided-Use Entire Disk option. If you are an experienced user, you can opt for the manual disk partitioning for having granular options of configuration.
- You need to select the disk partitioning and then click on continue.
- Make sure that you confirm all the changes that you have made on the host machine to the disk. In case you continue with the process, it will be erasing all the data on the disk.
- Once you have confirmed the changes in the partition, the OS installer will start the process of file installation. The system will be installing the files automatically. The whole process might take up some time.
- After completion of file installation, the system will be asking you for setting up the network mirror for obtaining future updates. Make sure that you select this function is you are going to use Kali Linux in the future.

- The installer will be configuring the package manager for all the related files.
- Then you will be asked for installing boot loader of GRUB. Click on yes and select the device for writing up the required information of boot loader directly to the hard disk which is necessary for booting Kali Linux.
- Select continue for finishing the process of installation.
- After this the installer will be installing some files in the final stage.

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

Chapter 5: Insights on Kali Linux Concepts

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

You are required to be more attentive

Though an operating system might automate all your tasks, it is your task to be anxious always. You are required to keep a close eye on the settings of our application and various other details. When you have a well-configured system of Kali Linux, it might turn out to be the most difficult thing to crack. However, most of the users of Kali Linux do not have profound knowledge about what is required for keeping their whole systems locked up. In case you start using a brand-new application, try to pay very close attention to the details of its configuration. Running the application with the same example settings and then using it is not the ideal option. It is not at all recommended. Some of the developers in the past also put decoy settings in the applications for making sure that the applications are prevented from running. This was a great way for

ensuring that all the users have checked out the file of configuration of the application.

Handling all the permissions in the right way

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

Kali Linux does have viruses

Linux comes with a widespread reputation of being virus-free. It is really a surprising thing for all the newcomers. However, in actual, the picture is completely different. Linux is less popular as an operating system as compared to Windows or Mac. So, it is not much targeted by the hackers

and so the development of viruses for Linux is not much. But, Kali Linux malwares do exist. The malwares of Linux are even more destructive than the counterparts of Windows. This might turn out to be more dangerous for all those Kali Linux users who avoid to pay attention to the application permissions and various other core concepts of Linux security.

The security tools are available

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

Being open source is not secure always

Kali Linux is an open source software which has made this OS the most favorite for all the ethical hackers and IT personnel. Many people think being open source is the ultimate key for being more secure. The same goes with Kali Linux. However, in reality, it is not like that. You might think that being an open source software which is exposed in front of the

entire world, any kind of issue will be taken care of immediately. That's absolutely not the case. There have been various recorded cases of security breaking and backdoors in the system of Kali Linux. In many of the cases, the security holes were put there in the system purposely. So, it can be concluded that being open source is not the ultimate sign of security. Having a closed system and reviewing the same by experts in case of any issue has its own benefits. You should never underestimate the tools of security in Windows just because of its nature being close-source.

Kali Linux is indeed a fantastic operating system for all the ethical hackers and for those practicing penetration testing. Kali Linux is obviously secured than the other distributions. However, its full effectiveness can only be pictured after computing it for a long term. Without proper insights into the application settings and its permissions, you might expose the entire system to some serious risks of security without you even realizing the same. Starting off as a beginner and having a Kali Linux distribution which has been configured poorly might turn out to be a disaster as a whole. So, make sure to check each setting and if you want, you can customize them according to your need.

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

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

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

Functions of C.I.A.

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

- Counterterrorism as the main priority
- Nonproliferation of weapons regarding mass destruction

- Informing the state about various important events overseas
- Counterintelligence
- Cybersecurity and intelligence


CYBER SECURITY

Chapter 7: Cybersecurity

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

Cybersecurity in details

Cybersecurity is nothing but protection of your networks, systems and various programs from the attacks digitally. The cyber attacks are generally targeted at changing, accessing and destroying of very sensitive data, money extortion from the users and also interruption in the processing of businesses. Cybersecurity is also known as electronic information or information technology security. Now, you might be thinking that what is cyber attack then? It is a deliberate and malicious form of attempt by a hacker in general or also maybe by an organization for the purpose of breaching organizational data.

The term cybersecurity in various contexts

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

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

where it is stored all come under the umbrella of operational security.

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

Why is cybersecurity so important?

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

Breaching of data can result in a devastating condition for an organization, especially at a time when all the organizations use networks for data transmission that includes government, corporate, medical, financial and

military organizations. It might turn out to be a threat for national security as well when confidential data is leaked from the government networks. A large portion of such data might turn out to be ultra-sensitive in nature, whether the data is financial data, intellectual data, information of individuals or any other form of data. Cybersecurity helps in describing the form of discipline which is required for the protection of data and data systems which are being used for processing and storing of data.

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

Various types of threats related to cybersecurity

- **Ransomware:** It is a kind of dangerous malicious software which has been designed for the purpose of money extortion by blocking away file access or networking system until and unless the amount of ransom is paid. However, there have

been various cases where the access to the files or the systems was still blocked after payment of the ransom.

- **Malware:** Malware is nothing but malicious software. It includes various types of software such as ransomware, spyware, worms and viruses as well. The functioning of malware is very simple so that the user cannot even detect any kind of breaching in the network. It is done by taking advantage of the vulnerability of a network when any user clicks on any dangerous email attachment or link that readily installs the risky software in the system. Once the malware has been installed in the system, it can do anything it wants such as:

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

- **Phishing:** It is the practice of cyber attack where fraudulent communication is sent and appears as a genuine form of communication from any kind of reputable source. It is most commonly done via email. The primary goal of this type of attack is to steal confidential personal data such as credit card details, information regarding login and many more. This form of cyber threat is increasing day by day.

- **MitM:** It is also known as man in the middle attack or eavesdropping attack. It takes place when the attackers place themselves in between a two-party communication. Once the attackers are successful in interrupting the traffic, they can easily filter out and steal relevant data. There are two very common points of entry for the MitM attackers:

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

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

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

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

Challenges regarding cybersecurity

For an all-round system of cybersecurity, a company or organization is required to coordinate all its available efforts within the overall system of business operation. The hardest form of challenge that comes in cybersecurity is the everyday growing structure of the risks in security within itself. In the past years, the government bodies along with the business organizations used to focus only on their very own resources of cybersecurity for the sole purpose of security of their perimeter for protecting only those components of their system which are crucial in nature. They used to defend only against the known threats. But, in today's

world of cybersecurity, this form of approach is not at all sufficient. This is mainly because of the fact that the threats have evolved in size and are advancing day by day. The threats of today are on the verge of changing themselves much before the organizations can learn to cope up with the older versions of the threats. This, in turn, results in the promotion of the advisory organizations for more adaptive along with proactive form of approach towards cybersecurity. The NIST or National Institute of Standards and Technology also issued various guidelines in the framework of assessment of risk that strongly recommends a steep shift in the way of regular monitoring along with on-time assessments, which will be focusing on an approach which will be focused on data for security directly in opposite to the traditional model which was based on perimeter.

Management of cybersecurity

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

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

Cybersecurity and the C.I.A. triad

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

Confidentiality

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

How can confidentiality be maintained properly?

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

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

Integrity

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

How can integrity be ensured?

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

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

Availability

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

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

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

Authorization, Authentication and Accountability

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

Authorization

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

Authentication

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

- **Knowledge:** It is based on something the user knows or based on the knowledge of the user
- **Characteristics:** It is based on the characteristics of the user

- **Ownership:** It is based on something you are having or based on the ownership of the user

Accountability

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

Access control

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

with access. It comes with a variety of controls that prohibits the access to all the resources of the system completely based on the group identity, membership, logical & physical location along with clearance. The access can take the form of permission for entering, consuming, restricting, controlling and protecting the system resources for guaranteeing the A.A.A framework in the system.

Non-repudiation

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

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

Non-repudiation levels

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

- **Of origin:** This can be very easily ensured by sending the data with certificates and digital signatures.

- **At delivery:** This can be ensured with the acknowledgement of the recipient.
- **For submission:** This can be ensured simply by sending the delivery recipient directly to the sender.

Evolution of cybersecurity

The traditional form of cybersecurity is constricted only around the usage of defensive measures within a specific boundary. Several initiatives of enablement just like BYOD or bring your own device and remote workers policy have helped in completely dissolving the boundary and have also expanded the surface of attack. Today, the incidents of data breaching are developing rapidly despite of the huge amounts of spending on security. Most of the global organizations are turning towards a new kind of approach towards cybersecurity which is completely human-centric. This new approach focuses on the rapid changes in the behavior of the users in place of just tracking the growing number of threats. This form of cybersecurity helps in providing deep insights into the interaction of end-user with the data and also extends the controls of security of all systems.


WARNING
CYBER

Chapter 8: The Threat of Malware and Cyber Attacks

Malware

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

Malware, also known as malicious software is the term which is used for describing any type of malicious or harmful code or program which is dangerous for the health of a system or network. The malware is intrusive in nature, invades the systems and damages the system of computer, network and even mobile devices. Some malware is so dangerous in nature that they can even take over the functioning of a system. Malware cannot damage the hardware of the systems; however, it can steal, delete or encrypt confidential data without the permission of the user.

Most common ways of getting malware in the system

When it comes to malware, it can enter the system via various pathways. However, two of the most common pathways via which malware access

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

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

Common types of Malware

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

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

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

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

- **Ransomware:** It is a form of malware that locks out the users from the systems or encrypts essential data. The attackers of such malware force the victims to pay out a ransom amount for getting the access of their systems back. The existence of such malware is increasing day by day and has been the most threatening form of malware.
- **Rootkit:** This form of malware provides the attackers with all forms of administrative privileges on an infected system. It has been designed for staying hidden from other forms of software on the system, from the users and from the operating system of the infected system as well.
- **Keylogger:** This malware is regarded as the trickiest of all. It records the keystrokes of the user which he makes right on the keyboard. This malware stores all the gathered data and then sends it directly to the attacker who is looking out for details of credit cards, usernames, passwords and various other sensitive forms of data.
- **Cryptomining:** Also known as cryptojacking, it is a form of prevalent malware which is being installed by Trojan. It allows someone else to operate the system of an organization for mining out cryptocurrency such as Monero or Bitcoin.
- **Exploits:** It is a type of malware that takes full advantage of the bugs along with the prevalent vulnerabilities within a system for allowing the attackers to take overall control. Among all the other form of threats, exploits can be linked with malvertising that is well known for attacking via a legit website that pulls harmful content from any bad site

unknowingly. The harmful content tries to get installed in the system and take over it completely.

Who are the prime targets of malware?

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

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

How to protect the devices and networks from malware?

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

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

Cyber Attacks

With the advancement in technology, the attacks of third parties on organizational networks and servers are increasing day by day. Gone are those days when people used to store all their confidential data and information in files as physical items in the lockers. With new technological innovations, this storage of data has been shifted to online networks and servers. The online storage of data on clouds and servers allows the users to store as much data as they want and also access the

same whenever they are in need of them. But, every form of advancement comes with certain side effects that adversely affect the whole functioning of a system. The same goes in the case of organizational and personal data stored in online servers and networks. The attackers are always ready to find a victim and steal everything that they get.

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

Examples of cyber attacks

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

- **WannaCry:** This was a ransomware attack that broke in the year 2017. Like every other ransomware, it also took over the systems of computers and encrypted all the information on the storage. In turn, the attackers demanded for Bitcoin for decrypting those data. The game of malware is nothing new but WannaCry left its mark as it oppressed the susceptibility in

Windows by the use of a code that was developed by the US National Security Agency.

- **GitHub:** GitHub is famous for the service attack with about 1.30 TB per second of traffic that hit many popular sites.

Types of cyber attack

Phishing

Phishing is a very common form of cyber attack. The attackers use this technique for fooling the victims. The attackers craft emails in such a way that the victims assume the emails to be legit and fall prey to the harmful actions. The victim might get fooled in downloading dangerous malware that might be disguised in the form of any important document or any website link. It is most commonly done using website links where the victim is asked to enter their bank or credit card details and passwords. Such websites are generally fake and are made for such purpose only. Most of the emails of phishing are coarse in nature and are sent to thousands of victims at a time. But, there are also specific phishing emails that are sent only to a particular target to get the information that the attacker wants. Phishing can be done via email, website, advertisements and even game demos that can be found online.

SQL injection

It is means used by the attackers for exploiting susceptibility in order to take complete control over the database of the victim. There are many databases which have been designed for obeying all the commands which

are written in SQL or Structured Query Language. There are also various websites that take up information from the users and then sends the gathered data to the databases of SQL. In the case of SQL injection, the attackers try to write some commands of SQL in the web form that will ask for address along with information of name. In case the website along with the database is not properly programmed, the attackers will gain control over the database with the database trying to execute all the commands of the attackers.

MITM

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

DoS & DDoS

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

Maps of cyber attack

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

MAC Spoofing

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

According to the tech world, as the users cannot change the MAC addresses which are built in the NIC it does not mean at all that the users cannot make the other devices to think that their MAC addresses are completely different. Each and every data that will be leaving your device will be in your control. The data packet headers come with the device address, IP address along with the MAC address. So, it is possible to instruct the NIC to completely discard the MAC address that is built-in and instead of that use something which is customized by the user. It can be anything, in the way the user wants. This changing of MAC address is known as MAC spoofing.

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

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

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

Other uses of MAC spoofing

Anonymization

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

Theft of identity

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

ARP Spoofing

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

Attacks of ARP spoofing

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

Detection and protection from ARP spoofing

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

- **Packet filtering:** The packet filters help in inspecting the data packets as they are transferred across any network. Packet

filters can help in preventing ARP spoofing as it is capable of easily filtering and blocking those packets which comes with any form of suspicious information of source address.

- **Using ARP spoofing detecting software:** Most of the organizations today are using detection software for ARP spoofing. Such software functions by properly inspecting and then certifying the data before the transmission takes place. It also helps in blocking those data that seems like being spoofed.
- **Using protocols for cryptographic network:** SSH or secure shell, TLS or transport layer security and HTTPS or HTTP secure are some of the protocols that can help in preventing the attacks of ARP spoofing by encrypting all the data just before the process of transmission and then also authenticates the data when received.

Rogue DHCP Server

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

More about DHCP and DHCP server

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

How does DHCP work?

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

DHCP attack

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

Details about Rogue DHCP server

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

DHCPig

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

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

Chapter 9: Server and Network Scanning

Network and server scanning is nothing but using of computer networks for gathering information related to the system of computers. This form of scanning is mainly done for assessment of security, maintenance of system and also for attacking the systems by hackers. The purposes of scanning are:

- Recognizing all the available TCP and UDP networks which are running of the hosts which are targeted
- Recognizing systems of filtering in between the host which is targeted and between the user
- Determining the OS which is in use after assessing the responses of the IP address
- Evaluating the TCP sequence number of the target host for the purpose of prediction sequence attack and for spoofing of TCP

Network scanning

When it comes to network scanning, it includes scanning of network port along with scanning for vulnerability. The scanning of network port is the method by which the data packets are sent through the network to the system of a computer with specified numbers of service ports. This is used for identifying all the network services which are available on a specific system. This method is very useful for troubleshooting of system related issues and also for gearing up the security of a system.

Vulnerability scanning is used for detecting the vulnerabilities which are present within a system of computer available right on the network. It helps in the detection of particular weak spots in the OS or software which might be used against the system for crashing down the system or for any other form of undesired attack. Both scanning of network port and scanning for vulnerability are techniques of information gathering. But, when such actions are performed by any other third party, it might turn out to be the introduction of an undesired attack.

The processes of network scanning such as ping sweeps and port scans return valuable details about the map of IP addresses which hosts live along with the services it provides. Another form of network scanning is also used which is called inverse mapping. This process gathers all the details about the IP addresses that are not capable of mapping to the live hosts and this, in turn, helps the attackers in focusing on the various advantageous addresses.

Network scanning is one of those methods which are used by the attackers for gathering relevant information about a network or the target system. At the stage of footprint, the hacker creates a designated profile of the target system or network. This includes all forms of relevant information about an organization such as the DNS of the organization, the range of the IP addresses and also the servers of email. At the stage of scanning, the attacker tries to find out all the details about a particular IP address which is accessible online, the architecture of the system, the operating systems which are used along with the services which are running on the computers of the organization. At the stage of enumeration, the attacker tries to collect all relevant data that also includes the tables of routing, network

group and user names, SNMP or simple network management protocol data and many others.

Why are server and network scanning required?

Server and network scanning are very much required in this world of today where all the systems are vulnerable to the attacks of cyber criminals. With the shifting of storage from the physical database to the online version, the rate of cyber attack is also increasing day by day. The organizations are required to perform server and network scanning for preventing the following scenarios:

- Loss in the trust of the customers
- Complete disturbance of the online form of collection or generation of revenue
- Website crashing, loss of time and expenditures for the purpose of damage recovery
- The cost of securing the application on the web from further cyber attacks
- Loss of confidential data that might result in the downfall of an organization

Natures of server scanning

Server scanning can be performed in a variety of ways. Let’s have a look at them.

- **Active scanning:** This is the process which is used for identifying the services of a network simply by transmitting probe packets directly towards the hosts of the network and the devices and then monitoring the same for the responses. This form of scanning is used by the attackers who try to find out the vulnerabilities of a network. This process allows the operator of the network to discover the various open services which are available within the network in a direct attempt to check all those for some of the known vulnerabilities. The probe packets which are sent to the network host can either be in generic form which will be targeting only a particular protocol in place of an application or can also be targeted which will be focused on some accurate application by the host.
- **Passive scanning:** This method is used for identifying the services of a network by simply observing the generated traffic by the clients and the servers as it keeps on passing a point of observation. For the purpose of establishing passive monitoring, specialized form of hardware or software can also be inserted at the point of monitoring and can also be installed at the point. Many of the routers can replicate the ports in which the copies of the probe packets will be sent out of some other interface to the host of monitoring. Various hardware taps like the optical splitters will be adding no extra hardship on the router. However, it requires some detailed interruption for installation. The detection of both UDP and TCP with the use of passive scanning is pretty simple and straightforward.

For the detection of TCP, host of monitoring requires only to capture the TCP setup message of connection. After the completion of three-way handshake, it will clearly indicate that the service is accessible. The services of UDP can also be identified with traffic observation. But, because UDP is a type of protocol which is connectionless, the overall concept behind client and server is not clear without the information of application protocol.

Chapter 10: Inspection of Wireless Networks

In this era of unique technological innovations, it is of utter importance to opt for wireless networks or WLAN testing and inspection. It needs to be done for ensuring that the involved system meets all the requirements of performance along with security. There are lots of factors that come into play while inspecting WLAN. Therefore, all that you need is proper planning along with documentation of the test.

Considerations along with planning for WLAN inspection
While you plan for WLAN inspection, it is a crucial part to consider the available varieties of the areas of testing. It includes:

- **Testing of signal coverage:** It makes sure that the levels of signal are enough for supporting the performance levels that the users require throughout the coverage areas of WLAN.
- **Testing of performance:** This certifies the capabilities of the WLAN for meeting the needs of the users while using some particular applications over the network.
- **In-motion testing:** This helps in determining that whether the network of WLAN allows all the users for successfully using the applications at the time of moving across various areas of coverage.
- **Testing of security vulnerability:** This helps in certifying the network security by authenticating the application of the mechanism of security which is required along with the proper protection degrees from the access which are unauthorized.

- **Testing of verification or acceptance:** It offers a type of insurance to the organizations which hires various contractors for the implementation of WLAN after ensuring that the overall system has the required coverage of signal, capacity, performance along with security. It is a process which is kind of formalized that also takes into account the various practices of installation, documentation of system along with the various procedures of maintenance.
- **Simulation testing:** This helps in providing a proper visualization along with the representation of the behavior related to WLAN right before it is being deployed. It offers deep insights into the network design's effectiveness in relation to the activity of traffic, software and hardware. It also takes into account any form of potential issue in the performance.
- **Testing of prototype:** It has been designed for specifically assessing the parts of the product or the system of WLAN which are not familiar in nature in the environment of a lab right before the deployment of the same.
- **Pilot testing:** This involves the installation of WLAN in its real version with some specific facilities just before implementation of the system in the whole organization. This testing can provide with various outcomes which can offer detailed insights into the potential issues of performance and realistic usage.

Testing of signal coverage

This method uses up a signal coverage tester which is also known as signal meter for properly measuring the signals of WLAN across the overall area of coverage. The main purpose of this type of testing is to make sure that the level of signal is up to the mark for supporting high level performance which is required by the user while using various web applications on WLAN.

- **Wireless survey of site coverage:** The testing of coverage of signal often involves survey of wireless site. It is generally performed right before the installation of WLAN. It is carried on by proper positioning of access test point across different locations. The locations are situated throughout the area of WLAN coverage. It uses the signal meter for the purpose of measuring the values of signals within the area of the access point of testing. The result of such survey helps in deciding the location of the final installation of the points of access.

Testing of performance

This form of WLAN starts with the testing of association. This test ensures that the device types of the clients associate properly with one single or more than one points of access which act as parts of the system which is installed. This is regarded as a beginner's test for ensuring whether the devices of the clients are capable of establishing wireless connections. You need to confirm enough association prior to moving

forward with the other tests. This testing is of utter importance as sometimes the devices of the clients turn out to be non-compatible with the WLAN points of access.

Test of network connection

For proper communication between the devices of the clients and the web application, the systems of wireless network use either UDP or TCP. In both the cases, it is ensured that the device of the client has connected successfully with the WLAN and also possesses an IP address which is valid in nature. This is typically done by observing the table of association which can be found easily in the points of access. It is a great mode of testing that will ensure that the device of the client is capable of reacting to a generated ping from the subnet which is of similar nature in which the application dwells. The result of the ping needs to indicate that the device of the client properly reacts to the generated ping sufficient delays along with no timing out. In case the test of network connection shows a problem, make sure that the device of the client comes with a valid IP address and the firmware of the client's device is upgraded along with the points of access.

Test of application connection

It is to be ensured that each type of device of the client connects in a proper way with the application. With the help of wireless implementation of IP phone, it can be made sure that the phone registers in the proper way with the software of call manager and also receives the phone number

which is applicable. In case the phone fails proper registration, try to check again that the device is actually having a convenient IP address, primary gateway, subnet mask and also settings of DNS. You need to keep in mind that the phone might connect to any point of access without being able to attain a proper IP address. The device IP address needs to correspond along with the plan of address for the particular location where the device is establishing a connection with the network.


Security

Chapter 11: Testing of Wireless Network Security

Wireless communication is an invisible form of communication which is invisible in nature and is also omnipresent. It allows seamless flow of data in and out from homes and from business organizations through various devices and infrastructure of wireless connection. Most of the modern form of business organizations has set up some form of wireless networking, mainly Wi-Fi within their organization. However, proper implementation of such services is not able to see the type of attention that it actually requires. Various segments of networking such as VLAN routing, segmentation of network and SSID controls are required to be defined in clear form and also set up. It will allow the users to easily connect with the network and use the related services along with keeping away the intruders and the third parties, much away from the network.

Regardless of the fact that a lot of or very less consideration has been entitled for the setting up of the wireless network, the organizations are required to hunt out any form of weakness within the wall of security of the network for the purpose of avoiding any form of unethical and unauthorized access to the resources of the network and prevention of data leakage.

Wireless network penetration testing

Penetration testing or pentesting of wireless network is nothing but scanning a network for any form of discrepancy within the security wall. In case when an organization fails to adapt proper pentesting for the

wireless networks, it results in data theft as well as unauthorized access to all the resources of the network. Proper security measures can help in preventing all forms of data leakage along with ensuring the data security of a business.

Steps to be taken at the time of wireless network pentest

The steps that need to be taken will depend completely on the standards which are being followed for the penetration testing along with the methods agreed to by the company and the areas of testing. In general terms, the process of pentesting begins with the gathering of information and intelligence. It will be creating a map of heating for the area which is tested. It will track the footprint along with the size of the signal which is being broadcasted by the wireless network. Various other forms of information such as total number of SSIDs which are being broadcasted, configuration of the network, installed hardware and many others are also required to be collected. You can also start by creating a proper site map of the network.

The second step is to find out the form of threats which a company can be vulnerable to. It will be based on the hardware which is installed on the site, the network equipment visibility right behind the infrastructure of Wi-Fi and the distance to which the signal of Wi-Fi can be detected outside the property of business. Questions such as are there any open file

shares which can is accessible over the network of Wi-Fi and many others are the basic questions that a pentester needs to begin with.

The analysis of vulnerability test is carried out using specialized tools which are used by the pentester that will easily inform the tester about the form of exploitation to which the organization is susceptible to. In case, any form of susceptibility is identified, it needs to be exploited right away and then use the same to a point that will breach the security. The pentester can easily show the client about the susceptibility extent with this step. With proper pentesting, it can also be identified that what type of tool was used for attacking the wireless network.

Once the threats have proved to work, the pentester continues scanning the overall network and then establish the extent to which the threat will be able to exploit the permissions of the users along with data breach. After all, these have been done, a report is presented to the client with the details of the threats and the security holes within the system. The client is supposed to modify the security measures according to the report. The pentester tests the network again with the same form of exploits to check whether the modified security forms are able to defend the attacks or not.

In general, the wireless penetration testing is carried on in two phases: active and passive. In the passive phase, all sort of information is collected and in the active phase, the threats are tested for the network. This whole thing can also be done by an attacker who is trying to target an organization for data breaching.

Tools used for wireless network scanning

There are various tools which are being used today for the scanning of wireless network against all forms of vulnerabilities. Some of the most commonly used tools are:

- **Kali Linux:** Kali Linux can be used for testing the breach within a network. It is a hacking tool that also provides various security tools for the systems such as penetration testing. It is regarded as a very helpful tool.
- **Wireless card:** If you want to use Kali Linux as your Virtual Machine, wireless card of the PC can be directly used within the VM. It helps in detecting any form of threat within a network and also returns significant results of security testing.

Benefits of penetration testing

The biggest benefit of pentesting is the benefit of knowledge. In case your organization is susceptible to any form of threat via the wireless network, it is always better to detect the same as early as possible rather than repenting later. With the help of pentesting, the assessing of the current Wi-Fi state can be easily determined and the required changes in the wireless network configuration can be applied. In case the report of penetration testing is detailed enough, it can help the organizations to determine what strategies of wireless security they are required to adopt for improvement of the wireless network. The whole concept of pentesting ultimately helps in building up and improving various security measures that can help in preventing data leakage. It is also beneficial for finding

out whether the present security measures are enough for the wireless networks or not.


Sep 15:53 .
Sep 15:53 ..
Sep 2015 bin -> usr/bin
Sep 09:31 boot
Sep 15:50 dev
Sep 09:32 etc
Sep 15:52 home
30. Sep 2015 lib -> usr/lib
30. Sep 2015 lib64 -> usr/lib
23. Jul 10:01 lost+found
1. Aug 22:45 mnt
30. Sep 2015 opt
21. Sep 15:52 private -> /home/encrypted
21. Sep 08:15 proc
12. Aug 15:37 root
21. Sep 15:50 run
30. Sep 2015 sbin -> usr/bin
21. Sep 15:51 srv
21. Sep 15:45 sys
12. Aug 15:39 tmp
23. Jul 10:25 usr
var

Chapter 12: Management of Linux Kernel and Loadable Kernel Modules

All the operating systems that can be found today are composed of the two most important components. The first component and the most important one out of all is the kernel. The kernel functions as a prime constituent of any form of OS. It is situated right at the center of your OS. It comes with the power of controlling each and every functioning of the operating system that also includes the function of CPU control, memory management along with control of the content that a user can see on the screen. The second most important element within an operating system is the user land and it constitutes of everything else.

The kernel of an operating system has been designed in a way to perform as a privileged or protected area which is possible to access by any other form of account which is privileged as well or by root. This whole protection thing is only for the good. This is because, with unlimited access to the kernel can result in providing all forms of unauthorized access to the functioning of an operating system. So, in the real world, majority of the operating systems which are available in the market provide all the users along with the access to the services only at the access land. In the access land, the users can easily have access to everything they want without the need of taking the operating system under control.

Kernel access by the users provides them with the ability of changing the looks of the operating system, the method of working of the operating system and also the way in which the operating system feels to use. The

users who get access to the kernel can also crash a whole operating system and thus making the whole system dead or unworkable. In spite of such risks involved with the kernel of an operating system, the administrators of the systems sometimes are required to access the operating system kernel for the purpose of security as well as operational reasons.

After knowing the actual power of kernel, you can easily figure out that in case a hacker gets access to the kernel of an operating system, he can actually control the entire system and that might turn out to be dangerous as well. Also, for some advanced form of attack such as MITM or main in the middle attack, the attacker might also need to alter the functioning of the kernel also.

What is kernel module?

Just like human beings perform all their functions with the help of the CNS or central nervous system, the kernel can be regarded as the central nervous system of the operating system. It controls every functioning of the operating system and also includes the management of interaction in between the components of hardware and the starting of required services. Kernel functions in between the applications of the users that you can actually see and between the components of hardware that performs everything such as hard disk and memory along with CPU.

Linux is an imposing type of kernel that allows the adding up of the kernel modules. In general, the modules can be removed or added right from the kernel according to the user need. Occasionally, the kernel of an operating system might also require some updates which require the installation of

some new form of device drivers such as Bluetooth devices, video cards and USB devices and drivers of the file system. While updating the kernel, it might also require installation of some system extensions. For being functional in its full form, the drivers are required to be embedded within the kernel.

There are some operating systems, in which, for the purpose of adding one driver for the update, the user needs to completely rebuild, assemble and reboot the whole kernel of the operating system. However, in Linux, it comes with the capability of adding up kernel modules to the system kernel without performing this whole process. Such modules are known as LKMs or loadable kernel modules. LKMs are powered with the access of kernel to the lowest levels and that too by necessity. This makes the LKMs a very easy target for all the attackers. There is a very particular form of malware which is known as rootkit. This malware inserts itself into the operating system's kernel and mostly through the LKMs. In case a malware like rootkit ingrains itself into the kernel, the attacker will be able to have complete control over the functioning of the OS.

In case an attacker gets access to the admin of Linux for the purpose of loading up new modules into the operating system kernel, the attacker will not only gain access to the controlling of the target system but will also control each and everything that the system which has been targeted reports in relation to the ports, space of hard drive, processes, services etc., in short everything that a kernel handles. This is mainly because the attackers will be functioning at the level of kernel of the OS. SO, it can be said that when an attacker is able to induce an admin of the Linux into the installation of drivers such as video driver that comes with rootkit

ingrained in it, the attacker will be able to take the complete control of the kernel along with the OS.

Management of kernel modules

Linux comes with two varied ways in which kernel modules can be managed. The first one is by using a command group which is built in the suite of insmod which stands for insert module. It has been made up for dealing with module management. And then comes the modprobe command which is the second method. This command is used for management of the LKMs. For adding a kernel module using modprobe, you need to use the command with -a switch. For removing a kernel module, you need to use-r along with the command. The command of modprobe comes with an added benefit when compared to insmod. The command of modprobe can understand all the options and procedures of removal or addition just before making any change in the kernel.

Chapter 13: Security and Hacking of the Web

Web Hacking

With the pace of time, the attacks of the web hackers are also increasing day by day. There is not a single day when someone hasn't been the victim of a hacking attack. This becomes more terrifying you act as the owner of a website. It might happen that all the work that you have done on your website gets wiped out the next day or it has been altered completely. This happens only when your website gets attacked by a web hacker. The news of data breaching and hacks are all over the new in today's world. You might also think that why would the hackers attack a small website of business? Well, nothing depends on the size of a website. It has also been found that 43% of data breaching is done from small business websites. So, it is clear that the attackers can victimize anyone they like.

The hackers are turning out to be more sophisticated in their operation within a community of close-knitted web hacking. The hackers try to target the new intrusions of web application. This is because when a new intrusion is found, it takes some time for the developers to apply the counter measures. The hackers take advantage of such situations and attack the business websites. The intrusions which are discovered newly are posted on various hacking forums which inform the hackers about the intrusions and the sites. The most common form of attack is infecting the website with some sort of malicious code. Ultimately, the websites which are infected turn out to be the attack launching sites for the hackers and installs the malware on those systems of computers those who visit that site.

Hacking of websites can be regarded as the result of adoption of technologies which are web-based for carrying out e-business. The applications on the web allow the organizations to seamlessly connect with the customers and with the suppliers. However, the vulnerability of such applications on the web has also opened up new doors for the attackers. The hackers opt for the vulnerable websites for various reasons such as data breaching, stealing of confidential information and many more.

Web hacking for stealing sensitive data

When someone conducts online business, the website is bound to function with a wide collection of applications such as submission forms, shopping carts, dynamic content, login pages and many others. The web applications are constructed in such a way that allows the customers to submit and also retrieve various forms of dynamic content that includes different levels of sensitive as well as personal data. Such sensitive data is stored in the databases of the websites. As such websites need to be accessible 24*7 from any location in the world, the web applications which are insecure in nature opens up the doors for the web attacks on the corporate databases. In case the attacker gains access to the credit card and bank details of the customers, the business might turn out to be in great danger.

Web hacking for implementing phishing sites

It might happen that the database of a business is not online or is secured already. However, in spite of such facts, it does not make the web site less

susceptible to the attacks. Hackers trace out weak and small sites for the purpose of injecting malware into the sites. They also look out for vulnerable applications for tricking the users and then redirecting them to the phishing sites. Phishing sites are used for retrieving the bank details of the users. Such attacks which are mainly targeted against the services of online payment can turn out to be the result of either SQL injection or any other type of hacking that can also be performed when the database and the servers contain no susceptibilities.

Securing websites from hackers

There are various ways in which the websites can be protected from the hacking attacks. You can start by installing plug-ins of security on your website. The website security plug-ins helps in improving the security of a website and also prevents any form of attempt of hacking. There are various forms of security plug-ins which are meant for websites of different formats such as Sucuri for WordPress, Amasty for Magento and RSFirewall for Joomla. Make sure that the website that you are constructing comes with HTTPS as SSL certificate is essential for protecting the details of the users such as personal data and credit card information.

Google Hacking

Also known as Google Dorking, is a technique which is used by hackers for information gathering by taking into consideration some of the prime searching techniques of Google. The search queries of Google hacking can be treated by the attackers for identifying the various vulnerabilities of security in the web applications, discovering messages of errors for disclosure of various confidential data and for discovering various files with credentials. The only way to prevent this is by checking out for regular website application vulnerabilities.

XSS Attack

XSS or cross-site scripting attack is a technique which is used by the attackers for injecting malicious form of scripts into mild and trustable websites. It occurs when a hacker takes help of a web application for sending out harmful codes in the form of side script in the browser to the end-user. The end-user will have no idea that the code is malicious in nature and will run the script without even knowing anything.

SQL Attack

It is a form of injection attack that allows the attackers to execute various harmful SQL statements. The SQL statements perform the function of controlling the servers of the database behind the web applications. The hackers can use this measure for bypassing the security measures of a web application. The attackers can also use this technique for adding, modifying and deleting various records from the database. SQL vulnerability can affect any application on the web or websites that use up database of SQL like MySQL, SQL Server, Oracle and others. The cyber attackers use this technique for gathering sensitive data such as personal data, intellectual property, customer information, secrets of trade and many more.

Chapter 14: Exploitation of Computer Systems

With the increase in the use of computer systems day by day, the percentage of attacks by third parties on the systems is also increasing gradually. There were days when people used to store all their data and confidential information in the form of physical copies. But, today most of the people prefer their confidential information in the computer systems and that is what gave birth to the attacks on computer systems.
Exploitation is nothing but a programmed script or software which allows hackers to gain control over the entire system and then exploit the same for the benefit of the hackers.
The exploitation attacks try to take advantage of any form of weakness in an OS of the user, in the application or in any other form of software code that also includes plug-ins of the applications or of the libraries of software. The owners of such codes issue a patch or fix in response. The system users or the users of the applications are completely responsible behind obtaining the patch. It can be downloaded from the developer of software which is readily available on the web or it can also be downloaded by the OS automatically or by the application that needs the same. In case the user fails to install the required patch for a specific problem, it will expose the user to the exploitation of the computer system and might also lead to breaching of security.

Computer exploits and its types

Computer exploits can be categorized into two different types:

- **Remote exploits:** Remote exploits are those exploits types where it is not possible to access a network or remote system. Such exploits are generally used for gaining access to the systems which are remote in nature.
- **Local exploits:** Local exploits are used for those systems which are having local system access. The attackers use this for over-passing the rights of the users of the local systems.

The security exploits can come in all forms of size and shape. However, there are certain techniques among the lot which are more often used than the others. The most common vulnerabilities which are web-based are XSS or cross-site scripting, SQL injection along with cross-site request forgery. It also includes abuse of authentication codes which are broken in nature or other misconfigurations of system security.

Zero-day exploit

The exploits of computer systems can be differentiated in various ways that will depend on the process of working of the exploits along with the attack type that it can accomplish. The most common form of exploit is zero-day exploit. This form of exploit takes ultimate advantage of the zero-day susceptibility. Zero-day susceptibility takes place when a software that might also be an application or an OS, consists of some critical form of vulnerability in the security measures that the vendor is also unaware of. The system vulnerability can only be detected when any hacker is detected with exploiting the susceptibility of the system. That is why it is known as zero-day exploit. After such an exploit takes place, the system which is running the software is also left vulnerable to all forms of

attacks until and unless the software vendor releases the required patch for the correction of the system vulnerability.

The computer exploits can also be characterized according to the expected form of an attack like the execution of remote code, delivery of malware, escalation of privilege, denial of service and various other harmful goals. The exploits can be characterized according to the vulnerability type which is being exploited that also includes code injection, exploits of buffer overflow and various other attacks of side channel and vulnerabilities of input validation.

How does exploit take place?

It is a fact that exploits can take place in various ways. However, one of the most common methods of all is exploits being launched from the websites which are malicious in nature. The victim of such exploits generally visits the malicious websites by mistake. The victim might also be tricked into surfing or clicking on a malicious site link that can come attached with a phishing mail or in the form of advertisement of malicious nature.

The malicious websites which are being used for the computer exploits come equipped with various toolkits of software and exploit packs which can be used easily for unleashing the attacks against the various vulnerabilities of the browser right from a harmful website. It might also be from a hacked website. Such form of attack generally attacks the software which is coded in JAVA, browser plug-ins and the browsers which

are unpatched. It is used for planting malware into the computer system of the targeted victim.

The automated form of exploits which are generally launched by various malicious websites are designed with two components: exploit code and shell code. Exploit code is a software which tries to exploit a known form of vulnerability. The payload of the exploiting software is the shell code which has been designed for running one single time when the breaching of the system is complete. The name of shell code comes from the very fact that many of the payloads open up command shell which is used for running the commands in opposition to the system of the target. However, all shell codes are not capable of opening a command shell.

Shell code

Shell code acts as a tiny piece of code which is used as the payload in the process of software exploitation. The shell codes are written in the form of machine codes. Download and execute is a form of shell code that performs by downloading and then executing some malware from directly on the targeted system. This form of shell code do not generate shell but instructs the target machine for downloading a form of an executable file which will be off the network, then save the same into the disk and execute the file. This form of shell code is most often used in drive download form of attack in which the victim clicks on a malicious website link and the

shell code downloads the malware and installs the same on the system of the targeted victim.

Chapter 15: Firewall Security

As the rate of cybercrime is increasing every day and is also threatening all form of business all over the world, it is a known fact that each and every organization of today are in need of firewall security. The term ‘firewall’ originates from the word wall which can be constructed for preventing the spread of fire. That is why it came to be known as firewall. However, the fire in the world of computer and networking is referred to as the sudden third-party attacks on the systems. Firewall security helps in blocking some specific form of network traffic and forms a barrier in between trusted and untrusted networks. It can be compared to a physical wall in the way that it tries to prevent spreading of malicious computer attacks.

Types of firewall

There are various types of firewall that can be found today.

Packet filtering firewall

This firewall type comes with a list of rules for firewall security and is capable of blocking internet traffic completely based upon IP address, IP protocol and port number. This firewall management program allows all types of web traffic along with the ones that can bring about web attacks. In such a situation, the user needs prevention of intrusion along with firewall security. In this way, it can easily differentiate among good and bad web traffic. However, a packet filtering firewall cannot tell the proper difference between various forms of web traffic. It also comes with an additional drawback in which the firewall cannot differentiate between a

return packet which is legitimate in nature and a return packet which acts like being a part of an established form of connection. So, this form of firewall will allow both types of return packets into your network.

Stateful firewall

This type of firewall is somewhat similar to that of the packet filtering firewall but it is more intelligent in nature. It can easily keep a track of all the connections which are active so that the user can customize the rules of firewall management as such by allowing only those return packets which are actually the part of an established connection. However, just like the packet filtering firewall, the stateful firewall cannot also differentiate between good and bad traffic and this needs prevention of intrusion for detecting and then blocking the malicious web attacks.

Firewall with deep packet inspection

This form of firewall examines the data packets in actual and thus can also look after the attacks of the application layer. This form of firewall is similar in nature to the technology of intrusion prevention. So, it is capable of performing some of the functions of intrusion prevention. It comes with three admonitions. Firstly, the explanation of “deep” inspection for some of the vendors extends to a specific depth within the packets and therefore, do not examine the packet entirely. This can ultimately result in missing out some of the major forms of attacks. Secondly, as it depends on the capacity of hardware, it might not have the processing power which is required for handling the deep inspection of the packets. As a user, you need to make sure about the bandwidth capacity

that the firewall can easily handle at the time of inspection. Thirdly, the technology of embedded management of firewall might not have the required flexibility for handling all forms of attacks.

Application-aware firewall

This form of firewall is similar in function with the deep packet inspection firewall. However, this type of firewall can understand various protocols and can also define them so that the rules or signatories can address specific sections in the protocol. Application-aware firewall provides flexible firewall protection to the computer systems and also allows the rules for being both comprehensive and particular. This firewall management system does not come with any form of drawback as in general, it will improve the functioning of deep packet inspection. However, some of the attacks might get unnoticed by the firewall as the defining of routines by the firewall is not potent enough for handling the variations in actual world traffic.

Application proxy firewall

Application proxy performs as the mediator for some applications like web, traffic or HTTP that intercepts all the requests and also validates all of them before allowing them. Application proxy firewall also comes with certain features of intrusion prevention. However, the application of complete application proxy is actually difficult and each proxy is capable of handling a single protocol only like incoming email or web. For getting

the ultimate firewall protection from an application proxy firewall, it needs to completely accept the protocols and for enforcing blocking of the protocol violations.

Importance of firewall security

Firewall security is of utmost importance for the computer systems of today's world. The attackers are always looking out for the vulnerable form of devices which are connected with the internet. The attackers can easily gain access to the system by implementing malware or any other form of malicious script into the system through the internet. It can lead to data breaching and also loss of sensitive data. Firewalls can provide ultimate security to the systems and are important because:

- It can protect the computer of the user from unauthorized access.
- It can easily identify and then block unwanted and harmful contents.
- It can help in preventing viruses, worms and malware from entering the system.
- It can create a secure environment of network for multi-person usage of the system.
- It can help in securing all sorts of sensitive and confidential information.

Firewalls come with the capability of blocking some particular online locations. This feature might turn out to be very beneficial for the purpose of security and also for blocking various sites that might contain content

which is not suitable. Filtering of content is useful for the parents, schools and corporations. Firewall can easily block the access to malware, however, it cannot detect any malware in the system and get rid of the same. So, it is always recommended to install an anti-virus software along with the system firewall protection right in place. Anti-virus software is capable of detecting any form of malware in the system and can also help in blocking the same.


Security

Chapter 16: Cryptography and Network Security

With a rapid increase in the rate of cyber attacks, it is of utter importance to protect all forms of confidential data as much as possible. Data leakage can lead to serious loss for various businesses and can also turn out to be a threat for an individual person where the credit card, as well as bank details, are breached. The term cryptography is linked with the technique used for converting plain and ordinary text into unintelligible form. With this method, transmission and storage of sensitive data become a lot easier. Only those to whom the message is intended can process the text and read it. It is not only helpful in protecting data from breaching or theft but it is also useful for data authentication.

In the world of computer science, cryptography is associated with securing all forms of information along with the techniques of communication which are derived from the concepts of mathematics. It uses a definite set of ruled calculations which are known as algorithms. The algorithms are used for transforming the messages in such a way that it becomes very hard to decipher the same. Such algorithms of deterministic character are used in the generation of cryptographic keys along with digital signing for protecting the privacy of data, browsing various websites on the internet and for sensitive communications like email and credit card or bank transaction details.

Techniques of cryptography

The technique of cryptography is often linked with the characteristics of cryptanalysis and cryptology. The technique of cryptography includes the

usage of various techniques like merging of words with various images, microdots and several other techniques which are used for hiding that information which is in transit or in storage. However, in the world of computer today, the technique of cryptography is often linked with the process of scrambling ordinary text or cleartext. Such form of ordinary text is known as plaintext. The plaintext is converted into ciphertext with the process of encryption and then back to the original form with the help of decryption. The people who specialize in the field of cryptography are called cryptographers.

Objectives of cryptography

The modern-day objectives of cryptography are as follows:

- **Confidentiality:** Confidentiality is the act of keeping all forms of personal and sensitive data protected for the concerned people. The information which is being transmitted or stored cannot be analyzed or understood by any third party for whom it was not at all intended.
- **Integrity:** The data or information which is being transmitted or stored cannot be changed or altered between the sender and the receiver who is intended to receive the data. In case any form of alteration is made, the sender and receiver will both be notified.
- **Non-repudiation:** The sender, as well as the creator of the data or information, will not be allowed to deny his/her intentions at a later stage during the creation or transportation of the data or information.

- **Authentication:** Both the parties in communication who are the sender and the receiver will have the capability of confirming the identity of each other along with the origin and final destination of the data.

The protocols and the procedures that meet all of the mentioned objectives and criteria are called cryptosystems. The cryptosystems are often taken as only referring to the procedure of mathematics and programs of computer only. However, in actual, they also comprise of human behavior regulation like logging off from the systems which are not used, choosing strong and difficult to guess passwords while logging in and not discussing any form of sensitive data and procedure with the outside world.

Algorithms of cryptography

The cryptosystems work along with a bunch of procedures called ciphers or cryptographic algorithms. It is being used for the purpose of encrypting as well as for decrypting the messages for securing up the communications among smartphones, applications and other computer systems. A suite of cipher uses up one single algorithm for the purpose of encryption, one more algorithm for authentication of messages and another algorithm for exchange of keys. This whole process is embedded within the protocols and is written within the programming of software which runs on the OS along with the computer systems which are based on the network. It also involves generation of public as well as private key for the process of encryption as well as decryption of data, verification for the purpose of message authentication, digital signing along with the exchange of keys.

Cryptography and its types

There are various types of cryptography which are being used today.

- **Encryption using single key or symmetric key:** The algorithms of this form of cryptography create block cipher which are actually particular length of bits. The block cipher comes along with one secret key that the sender uses for encrypting the data. The same key can be used by the receiver for deciphering the information. AES or Advanced Encryption Standard is a type of symmetric key encryption which was launched by the NIST as Federal Information Processing Standard or FIPS 197 in the year 2001. It is being used for the protection of confidential and sensitive data. In the year 2003, the U.S. government approved of AES for the purpose of classified information. AES is a form of specification which is free from royalty and is used in all forms of hardware and software in the whole world. AES succeeded DES and DES3. AES uses up longer lengths of keys for preventing attacks.
- **Encryption using public key or asymmetric key:** The algorithms for this form of cryptography uses two keys at a time in pair. One public key which is associated along with the sender and the receiver for the purpose of encrypting the information. Another private key is used for the purpose of decryption of the message. The private key is only known to the originator. There are various forms of cryptography using public key like RSA which is used all over the internet, ECDSA which is being used by Bitcoin and DSA which has been adopted as FIPS for all forms of digital signatures by the NIST.

- **Hash functions:** For the purpose of maintaining the integrity of data, hash functions are used that returns an accepted value from the value which is used as input. It is being used for mapping the data into a fixed size of data. SHA-1, SHA-2 and SHA-3 are the types of hash functions.


VPN

Chapter 17: Protection and VPN

VPN, also known as Virtual Private Network, is a technique of creating a highly secure connection with another network directly over the internet. In this world of today, VPNs are widely used now for accessing various websites which are restricted in several regions, for protecting the user's activity of browsing from the attacking eyes while using public Wi-Fi and many more. VPNs are very popular today but it is not being used for the purpose for which it was created originally. It was made for connecting to the networks of business in a secure way over the internet. It was also made with the purpose of allowing the user to access the network of business right from their home. VPNs help in forwarding all the traffic in the network which provides users with various benefits such as accessing the resources of local network remotely and bypassing of censorship on the internet. Many of the OS comes with integrated support of VPN.

How does VPN help?

The concept of a VPN is very simple. It connects the smartphone, PC or tablet of the user with another server or computer directly on the internet and also allows the users to browse the content on the internet by using the internet connection of that computer. So, in case the computer with which the user is connecting to for surfing the internet is from a different country, it will show that the user is also from the same country as the server computer. So, the users of VPN can easily access everything that they couldn't do normally.

A VPN can be used for various purposes such as:

- Bypassing the restrictions on websites based on geography or for streaming of video and audio.
- Watching online media streaming like Hulu and Netflix.
- Protecting the user from connecting to any form of malicious hotspots of Wi-Fi.
- Gaining a little bit of privacy online by hiding the original location of the user.
- Protecting the user from being scanned while using torrent.

Most of the people today use VPN for the purpose of bypassing their geographic restrictions for watching restricted content by using the network of any other country or for torrenting. VPNs are really useful while accessing public Wi-Fi such as at coffee shops.

How to get a VPN?

You can get a VPN depending completely on your requirements. You can either create a server of VPN all by yourself or host one VPN server out of the house. You can also create a VPN from your workplace as well. But, in real-world, most of the people are looking out for a VPN server for surfing restricted content which is banned in some areas or countries, like torrent. Just for the purpose of surfing restricted online content, you can download from the various options available online and use it according to your need.

Working of a VPN

When the user connects a computer or other device like a tablet or smartphone to the VPN, the system will start acting like it is from a similar local network as of the VPN. All the network traffic will be sent across a secure connection to the VPN. As the system behaves like it is also from the same network, it allows the users to access the resources of local network securely even when the user is at some different corner of the world. The user can also use the internet as if he/she was present right at the location of the VPN that also comes with some added benefits in case the user is using Wi-Fi of public nature or wants to access some sort of geo-restricted website.

When you are browsing the internet while being connected with the VPN, the computer will contact the website via the VPN connection which is encrypted in nature. The VPN will help in forwarding the user request and then brings back the website response through the same secure connection only. For example, if you are using a VPN based on the USA accessing content on Netflix, Netflix will be seeing your connection coming out from the USA only.

Uses of VPN

The usage of VPN is really simple and it can help the users do perform a variety of things such as

- **Accessing network of business at the time of travelling:** The most common use of VPN is by the business travelers who use it to access the network of their business along with all the resources of the local network while travelling only. The resources of the local network are not required to be directly exposed to the internet and thus it helps in improving the overall security.

- **Accessing home network at the time of travelling:** You can easily set up a VPN of your own for the purpose of accessing your network at the time of travelling. This will let you access a form of Windows remote access desktop directly over the internet. You can use it for local area file sharing, playing games on the web by acting as if you are also on the same local area network.
- **Hiding the browsing activity from the local network along with ISP:** In case you are using a Wi-Fi which is of public nature, all your activities of browsing on the websites which are non-HTTPS are visible to everyone on the same network nearby in case they know how to trace those activities. If you want to hide your browsing activity for gaining more privacy, you can use a VPN. The network of the local area will only be seeing one single VPN connection. All forms of other traffic will be traveling from over the connection of the VPN. This can also be used for bypassing monitoring of connection by the ISP.
- **Bypassing censorship on the internet:** There are various Chinese people who use VPN for accessing the Firewall of China for the purpose of accessing the complete internet.
- **Accessing the websites which are geo-blocked:** the use of VPN increased in recent years only because of one reason which is accessing websites which are blocked according to various locations. You can use a VPN for accessing such websites and also for watching online streaming media while you are out of your country such as Netflix and many others.

Chapter 18: Ethical Hacking and Penetration Testing

There is a misconception among most people which is that they think ethical hacking and penetration testing is both the same thing. However, in reality, it is not so in actual. Not only normal human beings who are not acquainted with the world of cyber security but the cyber security experts also get confused at times between the two. Although both of them fall under the same section of offensive security, there is a thin line that differentiates both. Offensive security is composed of various objects such as penetration testing, reverse engineering of software, social engineering, ethical hacking and many more.
In the world of cyber security, both the items ethical hacking and penetration testing are of utter importance. Let's have a look at some of the aspects of both the components.

Penetration Testing

Penetration testing, as the name goes by, can be understood that it is a process of testing whether penetration is possible or not. It looks out for all sorts of vulnerabilities, risks, malicious content and flaws within a system. By system, it can either be a computer system or an online server or network. This process is done for the purpose of strengthening the system of security in an organization for the sole purpose of defending the infrastructure of IT. It is a procedure which is official in nature and can be

regarded as very helpful and not at all a harmful attempt if used wisely. Penetration testing is an essential part of ethical hacking where it is focused on the attempt of penetrating a system of information.

As it is very helpful in readily improving the overall strategies of cyber security, the process of penetration testing needs to be performed at regular intervals. Several forms of malicious content are built up for finding out the weak points within an application, program or system. The malware is spread throughout the network for testing the vulnerabilities. Pentest might not be able to sort out all forms of concerns regarding security, but it can actually minimize the chances of any attack. Penetration testing helps in determining whether an organization or company is vulnerable to any form of cyber attack or not, whether the measures of defense are on point and which of the security measures needs to be changed for decreasing system vulnerability.

Penetration testing can easily show the strengths and weaknesses of the structure of an IT system at one point of time. The pentesting process is not at all a casual process. It comes with lots of planning, granting of permission for pentesting from the management and then starting the process without preventing the normal flow of work in an organization.

Ethical Hacking

The role of an ethical hacker is somewhat similar to that of a penetration tester. But, the process of ethical hacking comes with various forms of diversified duties. Ethical hacking encompasses all the methodologies of hacking along with all forms of methods related to cyber attack. The process of ethical hacking is targeted to the identification of vulnerabilities and also fixes all of them just before any attacker can exploit the information for the purpose of executing cyber attack. Ethical hacking is being called as ethical as all the required functions are performed only after the granting of required permissions from the authority for intruding the system of security. The ethical hackers perform their role on the ground of ethics whereas the attackers hack without any prior alarm.

The role of a professional ethical hacker is very critical as well as complex as the person who is intruding the system of security needs to perform everything without even affecting the overall functioning of the system and then locate the available vulnerabilities as well. The ethical hacker traces out the possible vulnerabilities and reports the authority about the required measures. An ethical hacker not only works with the methodologies of security but also suggests the implementation of the same. The safety of an IT infrastructure is in the hands of an ethical hacker.

Penetration testing Vs. Ethical hacking

Although the functioning of both penetration testing and ethical hacking might seem similar but both differ from each other in various aspects. The main goal of penetration testing is to look out for vulnerabilities within a

specific environment. In the case of ethical hacking, it uses various types of attacks for finding out the flaws in security. Penetration testing deals with the security of a particular area whereas ethical hacking itself is a comprehensive term and pentesting is a function of the ethical hacker. For being a good pentester, past experience is required in the field of ethical hacking. Ethical hacking is one step towards pentesting. Unless and until someone knows the methodologies properly, they will not be able to carry on with a penetration testing.

Penetration testing does not require very detailed writing of reports. However, in the case of an ethical hacker, an ethical hacker needs to be an expert report writer. Paper work is comparatively less in penetration testing when compared to ethical hacking. In the case of ethical hacking, detailed paper work with legal agreements is required. Penetration testing consumes very less time which is not the case with ethical hacking. It requires a lot more time and effort. For penetration testing, accessibility of the overall system is not required. In the case of ethical hacking, a hacker requires complete accessibility of the target system.

Bottom line

As penetration testing techniques are being used for protecting the systems from all forms of threats, the attackers are also coping up with the same and are coming up with new vulnerability points in the target applications. So, it can be said that some sort of penetration testing is not at all sufficient for protecting the system of security. This is not the case with ethical hacking as it effectively finds out the loopholes and reports about the same for further improvement. There are many cases where it has been found that when a new vulnerability has been found in a system, the attackers hacked the system immediately after the testing. However, it does not imply that penetration testing is not useful at all. It cannot prevent an attack from taking place but can help in the improvement of a system.

Chapter 19: FAQ

How often should penetration testing be done?

The organizations perform according to their own set of regulations and mandates. The standard that they follow will determine whether they need penetration testing or not. The standards of the organizations come with their own methodologies that help in describing what will be the best practice for protecting the security system. The standard will also determine that whether documentation of the tests needs to be done for compliance and purpose of auditing afterwards.

What is the rogue wireless network?

Rogue wireless network acts simply as a point of access just like a router or Wi-Fi station. It is plugged into the network of the organization; however, it does not even adhere to with the organization's standards for the wireless infrastructure which is in existence.

How a rogue wireless network can be installed?

This form of security threat occurs when any device has been adapted in an organization and is connected with the network, either knowingly or unknowingly. There are various types of equipment that come with activated Wi-Fi by default which is not configured at all. This means, that when the device gets turned on for the first time, it will start broadcasting signal for connection.

Can the employees of a business expose the organization to cyber threats?

Yes, they can. Any person who carries a device that has a connection with the Wi-Fi of the company might turn out to be a potential threat for the business. Malware can get into a system unknowingly via a network through laptop, tablet or smartphones. It happens when the segments of Wi-Fi are not properly locked. If the business servers are not separated on a completely different VLAN and all wireless network traffic can access the same, there is a high chance of security breaching and data theft.

Is it required to have wireless networks for businesses in spite of the associated potential risks?

Modern businesses cannot function without wireless technologies. However, the standards of technology and configuration which are applied for the wireless equipment will determine the usefulness of the wireless technologies and also the potential risks of security breach. There are various forms of businesses where the employees are required to work with tablets and scanners, especially in the manufacturing and warehousing sector. It will not be possible for such businesses to operate without the presence of a wireless network within the organization.

What are the most common types of Wi-Fi attacks?

When it comes to Wi-Fi attacks, the list is never-ending. There are several vulnerabilities, exploits and shortfall of security when it is related to

wireless attacks. But, the attackers employ certain common methods for the purpose of accessing the wireless networks.

Is MITM a serious security threat?

Also known as man in the middle, it is one of the most commonly found forms of attack and is the most used tactic as well by the attackers. The attacker tricks the victim and transmits data so that the sufferer believes that the communication is coming from a legitimate form of contact only. Using MITM, the attackers can easily target the system of the victim and control it remotely, gain access to several sensitive data such as bank details along with exploits.

What are packet analyzers?

The attackers are capable of analyzing and sniffing the data packets which are being transported through a wireless network. The attackers can also intercept various unencrypted data which is inside the packets of TCP as well. When data is gathered using this method, the attackers can easily gain insight into the internal working system of an organization which is being targeted and can also fish out valuable information that might turn out to be a huge loss for the business.

What is malware?

Malware is a form of cyber attack and is the most common form of attacks. It possesses a serious kind of threat to the networks and servers. It also comes with the power of self-propagating over various networks. It

becomes very difficult to detect and stop it once it has gained access to a network segment. It can infect the system when two devices are being connected with the same network which makes the spread of infection very fast.

Can poorly configured Wi-Fi lead to cyber attack?

Yes, it is possible when the Wi-Fi is configured poorly. It is the main reason behind the infiltration of a wireless network. This becomes more serious when there are no available management tools for the IT staffs to gain a perspective of the wireless environment.

Is it okay to share the result of penetration test outside the organization?

No, you should never disclose the test report outside the organization. You can only share it with the company officials and authorities. Sharing test results with the outside world will open up vulnerabilities for the organization and might lead to a serious cyber attack.

Conclusion

After you have completed the whole eBook, you can easily develop a clear perception of the process of hacking with the help of Kali Linux. By now, you have must have understood all the requirements for setting up a secure server and network for your business. Everything depends on you. You are the one who can secure the system of security from all forms of attacks.

With the help of various tools from Kali Linux, you can have overall control over the security interface of your organization. This book is not only about Kali Linux. You have also learnt about various components of a network and the measures required for securing them up. The key benefit of using Kali Linux is that you can perform various security tests that can help in removing all forms of vulnerabilities from your IT infrastructure.

The security of your organization and network completely depends on you. Make sure to employ the various steps that you have learnt from this eBook about securing your infrastructure.

If you find this book helpful for your business in any way, kindly leave a review on Amazon.