Cyber security Introduction

In our modern world, most people are using cyberspace for many things like shopping, social media, playing games, watching movies, even paying today's bills, which has many potential traps. In this tutorial, we are going to learn about the internet and the security measures for using the internet safely and the need for the security of the internet.

What is Cyber Security?

Security means protecting something from unauthorized or malicious attacks. Here also in the same definition, the term cyber security means protecting the systems such as computers, mobile, or any other devices or the data that is connected to the internet or inside the internet from malicious attacks.
Simply the term "cyber security" is formed by joining two words, which is "cyber" that means the internet that includes all the devices like computers, phones, routers, switches, and the data related to the internet and "security" means protecting them from the hackers or criminals who attack in cyberspace.
Therefore, as a definition, we can say "cyber security refers to a collection of principles or procedures which help to protect our information and the devices from all types of threats on the internet".

What is the need for cyber security?

Now we think about why I should be concerned about such types of threats and security, which is related to the internet? It is only for someone who is a software professional or someone who is working in cyberspace.

The answer is no. Every one of us is using the internet and the services that use the internet in all our day-to-day activities like social media, online transactions, online shopping, online bill payments, and more that we can't explain. Most of our phones are always connected to the internet and we all are a part of cyberspace so we all need to know how to use this internet without having any threats.

The internet is becoming a dangerous place for all including organizations and persons. There are a lot of people and machines accessing the internet and all the systems connected to the internet are mutually connected, so we need to protect our valuable data from vulnerable attacks.

Why is the internet becoming a dangerous place for all?

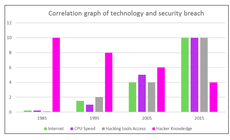
There are many reasons for that like

- Many criminal-minded people are now computer masters and can operate from anywhere.
- A large number of hacking tools are readily available on the internet and dark web
- Technology and the processing speed and bandwidth is increasing tremendously
- Many hacking books and tips and tricks are available

With all these methods, anyone who is able to use a system can learn these tricks and attack anyone who is illiterate about the internet.

What we can do to avoid such problems on the internet is to increase our knowledge about the internet or cyberspace. Making all the parts of the internet is not possible so we have to protect our networks and operating systems so that we can protect ourselves up to an extent. Now, cyber-attacks and hacking is one of the most important economic problems with international concern.

You can understand the current scenario from a simple graph given below.



What are the types of cyber security threats?

In cyberspace, there is a wide range of threats or attacks that involve the loss of confidential data, corrupting the data, financial loss, loss of control of a network, loss of accounts, and much more.
In general, cyber threats can be defined as malicious activity that is done by an individual or a group that results in loss or disrupts another person's life or property.

1. Malware:

It is the most common threat or cyber-attack tool in cyberspace. It is a malicious program that is able to be installed in our system or the browser and cause damage to our system. We all have encountered malware attacks but were blocked by antivirus or some defender. Some of the common type of malware attacks are

1. Virus
2. Worms
3. Trojans
4. Spywares
5. Adware
6. Botnets
7. Ransomware

2. Phishing:

It is a type of cybercrime we all have encountered in our daily life in the form of emails, messages, or even phone calls. In this method, the sender seems to be from an authorized company like some financial institutions, call centers, PayPal, or other shopping sites, etc. Here they will send us some E-mails or messages with some links or pictures. If we click these links or pictures, that will direct us to their fraud websites, which are programmed to take our sensitive and secret data or even install some malware in our device. Once the hackers got our data or the malware installed they even can remote login to our device and can control it.

3. Distributed Denial of Services (DDOS)

This is a kind of cyber-attack, which is not targeting the end-users. This cyber-attack will disrupt the working of a server and its functions. We know how the internet works like when a user requests some data from a server, the server sends the response with the data.

In a DDOS attack, the hackers are sending junk requests in large quantities to a server and making the server bandwidth filled, and making the server down temporarily. Finally, the server cannot able to handle a genuine request and we get a response as the server is down.

4. Man in the middle (MITM) attack

It is a type of cybercrime in which the hacker or a cybercriminal does an eavesdropping attack as the hacker intercepts the messages between the two persons and starts to involve in the conversations pretending to be a genuine user. Once they reach the middle of the conversations, they can get access to sensitive business data.

5. Brute Force Attack

This a also called a trial and error method which is a cryptographic method mostly to extract the password or pin or other sensitive information. In this method, the hacker will try all the possible combinations for a password until the real one is obtained.

6. Domain Name System (DNS) Attack

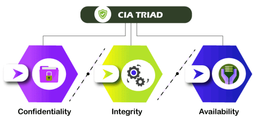
DNS is related to the website and its address; we are typing the address of a website to reach that website all the part of DNS. In this attack method, the hacker identifies some websites, which have some errors in their DNS and uses that website to divert the users to another malicious website to extract the information from the users.
There are much more attacks that will be detailed in the coming tutorials.

What are the goals of Cyber Security?

The main objective of cyber security is to provide security to the confidential and sensitive data and the devices, which are accessing cyberspace. In general, we can rely on three principles, which are needed to assure the security of the internet.

These three principles are called the CIA triad. This model is helpful to provide an organization with some rules or guidelines to protect their data and the resources in the internet. Let us discuss each of these principles in detail

1. Confidentiality
2. Integrity
3. Availability



Confidentiality

Confidentiality refers to the level of privacy for data. Confidential data means highly important data that needs to have high privacy which means we have to secure the data from unauthorized access. We need to block unauthorized access to the data. Data encryption is one of the methods used to make sure confidentiality.

Integrity

Integrity means protecting the data and the sensitive content from unauthorized modifications. It is important to keep the data secure without giving a chance to modify the data purposefully or accidentally. We also have to keep some measures to revert the original data if some modification occurs to keep the data genuine.

Availability

We said the data must be secure and genuine but the important thing is to make the data available for authorized or genuine users. That is done in availability that keeps the authorized users are not being blocked by malfunction or accidental.

Types of Cyber security

Cyber security is a vast area and each company or an organization has different areas and data and different combinations of data and systems to protect from the cyber criminals. Therefore, we have different types of cyber security as below

1. Network security
2. Application security
3. Information security
4. Identity management
5. Operational security
6. Mobile security
7. Cloud security

Etc and we detail each of them in coming tutorials

Advantages of Cyber security

1. Protects the data and devices from cyber-attacks and data breach
2. Helps in protecting data and network
3. All types of unauthorized access will be blocked
4. Help to recover fast if data breach happens
5. End to end protection for user devices and data
6. Safely continuing the operations
7. Helps to increase the company or organization's trust
8. Encrypt the data which cannot get to wrong hands
9. Helps servers from DDOS attacks
10. Block each and every cyber-attacks

Fundamentals of Computer network

What is a computer network?

A computer network can be defined as two or more computers are connected together (called **Hosts**) for the purpose of exchanging communication, or sharing resources either by wired connection like a LAN cable or by wireless like Wifi.
A network not only includes the host but also many other devices to transmit data and information are called Network devices like switches, routers, or hubs.
A network can be only for a specific geographic location like an organization or an office which are connected through physical cable is called LAN (Local Area Network) connection. We cannot able to access this network from outside the LAN network.
Opposite to the LAN network, we can connect the computer over the world with and without the help of a cable, which we call as internet or WAN (Wide Area Network) network. There are a lot of protocols and rules for transmitting data through the network.

What is Internet?

Internet is called a network of networks around the world. It is a global network that contains trillions of computers and network devices that connect together to form a massive network. Internet is connected together using a lot of wired connections like optic fiber and wireless connections. Internet uses different protocols for the safe and secure transmission to data through networks and TCP/IP is the most popular protocol that the internet uses at present.
Now each host on the internet has its own unique identification number that we call an IP address. It helps to know a unique host in that ocean of hosts or systems in the internet.

What is WWW or the World Wide Web?

In general, we are accessing all websites using the www and we call it as the internet. In fact, the www or World Wide Web and internet are not the same. World Wide Web or www is a network of different hosts and network devices and servers to form a giant network that can be connected through the internet.
Internet will act as a skeleton or a medium that the www uses to transmit data from the server to the user in response to the user's request. Web browsers for example chrome, firefox, safari, etc. help the users to access the www and its servers using the infrastructure called the internet.

How does the internetwork?

Before going to discuss the internet working, we need to understand some terms and details about the internet so that it will be easy for learning the working of internet.

Client and Server: The Internet is based on a client and server relationship, where the system we are using to browse different websites are the clients and the websites that we access are located in the servers. Servers also have an IP address and the collection of servers are stored is called a data center.

Once the client sent a request to access a webpage through a browser, the server process that request and sent the webpage to the client through the browser.

IP Address: Clients are not directly connected to the internet. The internet service providers commonly called ISP connect clients to the internet and they give each client a unique id to identify the client, which is called an IP address.

DNS Domain Name Service: As we said the server and websites are also having an IP address. For a user, remembering the IP address of different websites is not an easy task, so the internet provides a domain name for each IP address of different websites like learnetutorials.com, facebook.com, google.com, etc.
Please keep in mind that the internet cant able know the domain names as they just know the IP address of the websites and once we enter the domain name, internet search and find the IP address of that domain name and forward our request to that IP address. It is the same as we same names for phone numbers on our mobile.

Working of Internet

When we type a domain name in our browser address bar, the request for that corresponding IP address will be sent from our system to the DNS server. Once the IP address is received from the DNS server, the request for the specific information is sent to that IP address.

The request once reaches the server, the server process that requests and sends the webpage that the client requested.

This transfer of data from the server to the client and vice versa is happening through a series of network devices like modem, switch, router, hub, and optic cables.
Data is sent from a client to server and server to client through specific rules and regulations to overcome the errors and attackers, which are commonly known as protocols. The most common protocols are TCP/IP and UDP.

Data transfer across the internet in the form of packets, which have a header part for address and data part for storing data and trailer part for flow and error correction.

What are different computer networks?

There are different network types in computer networking that are used for some specific function. Some of them are,

1. **LAN** (Local Area Network): It is a geographical connection that is mainly used inside an organization or a building where the systems are connected through cables. LAN is normally short which is for data transfer and sharing of common resources, they are private networks which doesn't have access to the internet.
2. **WLAN** (Wireless LAN): It is a local area network as we discussed above the difference is the connection in WLAN is wireless.
3. **WAN** (Wide Area Network): WAN is the way of connecting the computer over a wide area. Internet is an example of WAN which connects a huge number of systems over the world.
4. **MAN** (Metropolitan Area Network): It is a network in between the LAN and WAN which will be coordinated by government or local authorities for connecting a city or an area.
5. **SAN**(Storage Area Network): SAN is a storage access network that will be helpful to get the users to access to the cloud or block storage or shared network storage.
6. **VPN** (Virtual Private Network): VPN is a secure channel between end-to-end nodes that are communicating. It makes a private encrypted channel for secure and private communication without disclosing the IP address. VPN has a very important role in cyber security to escape from hackers and attackers.

More Terms and components in Network

Switches: A switch is a network device that helps us to connect a device to a network. The switch helps us to share the resource and communicate in a network thereby reducing the cost.

Routers: Routers are special devices in the network that helps the data packets to move around the network by selecting the best path. Router helps you to analyze the data, which is sent across the network and helps to connect different devices to a single internet connection.

Transfer Media: This is the physical medium through which the data is sent across the network like the optic fiber, coaxial cable, etc. it is also called a channel or link.

Access Points: Access points are the points where a device can connect to a network wirelessly. A mobile hotspot is an access point.

Shared Data: Data that is shared to a network can be a LAN or a WAN network. It can be accessed by any user on that network.

Network Interface Card (NIC): Each computer is connected to a network using a NIC, it controls, sends, and accepts the data between a network and a computer.

Network Operating System: Network Operating system is an operating system that runs on the server, which allows the computers to connect to the network.

Protocols: Data is transferred through the network using a different set of rules that are commonly called protocols. Example, TCP, IP, UDP, FTP etc

Hub: Hub is a place where the distribution occurs in a network. Hub splits the connection to different systems. If a system needs any data it sends the request to the Hub and Hub distributes that request to the network.

OSI Model: It is a reference model to make the network functions easy and simple to understand.

Hostname: the system which is connected to a network that may be the client of the network is Host.

DNS server: we already discussed the DNS server, which converts a specific domain name to its IP address.

Port: We are using a system, which has different applications running like FTP client, Telnet, and browsers like that. So each application transfer and communicate with the network using different ports. It is a logical channel that helps to connect an application to a network.

Socket: A socket is a mix of IP address and port number that is used by applications running on a system.

ARP: ARP is Address Resolution Protocol, which converts the IP address of a system in a network to its physical address.

RARP: It is Reverse Address Resolution Protocol, which is the reverse process of ARP. It converts the physical address of a system to the IP address.

How to become a Cyber-Security professional

In this modern world, an uncompromised word is a Security. It is an essential factor in various fields. We are investing a huge amount of money in our security as for physical we use locks and doors, for health we go for the help of a doctor, and to protect the valuable things we add insurance on them.

Likewise, a huge number of organizations from small scale to large-scale use cyberspace for their work and business. These organizations need highly skilled security engineers to make the protection from cybercriminals and cyber-attacks. A cyber security engineer is one of the best career paths to select if you are a computer and network enthusiast.

Without any doubt, Cyber security is a good career path but it is not easy to enter that path easily but once you learned and have skills you will get a good career. A cyber security expert job is one of the highly responsible and stressful jobs, at the same time it rewards you the best.

Responsibilities of Cyber security engineer

The responsibilities of each cyber security specialist will be different according to the organization and the experience you have in the area. Some of the common responsibilities are

1. Analyze the Security vulnerabilities that may result in a security breach
2. Keep the security mechanisms updated.
3. Always monitor the network for malicious activity.
4. Protect the computer and network devices from illegal access.
5. Check and verify the firewall is intact and antivirus is updated and running.
6. Prepare the security reports in specific intervals.
7. Train the cyber security engineers.

Why learning cyber security is important

In this modern world, most of the activities are using cyberspace. Huge organizations are keeping all their sensitive information in cyberspace and the cloud. Even the common peoples use the internet for social media and even for payments.

In this surge of cyber activities, there is a huge increase in cyber-attacks of different forms and methods. It is very important to know about cyber security to protect ourselves and it is important for organizations to hire cyber security experts for preventing cyber-attacks on them.

Learning about cyber security will not only be benefitting you to hide your sensitive data from illegal cybercriminals but also open a new and good career option to follow.

Skills needed for a cyber-security expert

1. Good skill in mathematics
2. Always have the presence of mind
3. Ability to withstand unexpected situations
4. High skill to work under pressure
5. High skill in communication over a network
6. Good knowledge about networks and threats
7. Good knowledge about the hack methods and their tools
8. Must have knowledge about systems, OS, network, and network protocols
9. High problem-solving skills
10. Knowledge in some programming languages
11. Self-motivated critical thinker

Salary expectations for a cyber-security professional

The salary of a cyber-security expert depends on a lot of factors like the organization, the amount of information to protect, the experience you have, skills you have, the knowledge you have, and much more that is beyond our scope, but some general expectations about salary are in the range of $100000 per annum.

If you are interested to know more about cyber security, you are at the right place. We offer the best and simple tutorials for a beginner and intermediate to start with. Refer to our tutorials to get good knowledge about cyber security threats, tools, attacks, and cyber attackers, protocols, network topology, and its countermeasures. Happy learning!

Difference Between Ethical Hacking and Cyber Security

Cyber security and Ethical hacking are two names that make much confusion for a beginner. Both of them are aiming for a common goal that is to protect the systems and networks of an organization from cyber-attacks and cybercriminals. Both cyber security and ethical hacking are working for increasing the security of the organization, there is some difference between them.

Cyber security is a huge area that has different subsets or sub-areas to specialize and ethical hacking is one of those subsets or sub-area of cyber security. Let us check in detail how they are different even they have a common purpose.

What is cyber security?

Cyber security can be defined as a stream of technology that deals with methods and tools that are for maintaining the security of systems, network devices, and networks from illegal access, stealing or modification of sensitive data and even destruction of the system or a device or network that caused by the cybercriminals.

Cyber security teaches the methods and tools for keeping the network, systems, devices, and data safe and untouched from cyber-attacks.
As technology is increasing day by day, the internet and cyberspace are reaching millions of new users every year and the need for protection from cyber-attacks is increasing rapidly. The cause of such an increase in cyber-attacks is the revenue and the huge number of tools readily available in the internet for doing malicious activities.

Depending on where we use the security, we can divide cyber security into different categories such as

1. Network security
2. Data security
3. Application security
4. Information security
5. Mobile security
6. Cloud security
7. Endpoint security

A cyber security professional is a person who is responsible for doing all the security measures in an organization to protect that organization's assets and data from cybercriminals. A cyber security professional must have high skills, be self-motivated, and knowledgeable in various network aspects, and be able to deal with almost all kinds of threats from the internet like Malware, Scareware, Spyware, Ransomware, Viruses, Worms, and many more.

Definition of the Ethical hacking

Ethical jacking is a subset of the domain cyber security which is mainly doing penetration testing for understanding the vulnerabilities and risk areas that an external attacker can find in the system or network.

We can define Ethical hacking as a process of searching and finding all the vulnerabilities and risks in a network and preventing such loopholes that an attacker uses to penetrate into the organization's network or system.

Hacking is considered a criminal activity in almost all regions of the globe, but Ethical hacking is legal and even government seeks the help of highly skilled ethical hackers in some situations. Ethical hackers are doing almost the same as the hackers but they do not use their skills for any illegal activities or they never harm anyone with their skills. Ethical hackers are also known as White hat hackers, whereas the other hackers are called black hat hackers.
Let us detail the role of an ethical hacker with an example, suppose a client has a website that uses some sensitive information from the users. In such situations, clients will seek the help of an ethical hacker to check their website and they will identify the weak spots that a real hacker can use to penetrate and it's called penetration testing. It will help the website owner to close such weak spots.

Difference between Cyber security and ethical hacking

Cyber Security	Ethical hacking
It is a wide area that is concentrated on the continuous protection of data and devices that connected to the network from all threats and vulnerabilities	It is a subset of cyber security, which deals with identifying the security vulnerabilities using penetration testing.
The main aim is to protect the system and data	The main aim is to attack a system by penetrating tests to find vulnerabilities.
Cyber security is a continuous process of defense activity	Ethical hacking is a one-time process that is offensive
Cyber security experts will not break into a system or network devices; they never do penetration testing. Their aim is only to protect the system from attackers.	Ethical hackers penetrate into systems for finding the loopholes in the security and help the organizations to close them.
Career options in cyber security include security expert, security analyst, SOC engineer, CISO, etc	In ethical hacking, there is only two major career options as a penetration tester and security manager
Cybersecurity includes the maintenance of the security of the organization to make sure it is perfect.	Ethical hacking includes regular testing of the security of an organization to know any vulnerability in the system.
Cybersecurity is behind in providing access control by making access privileges in the organization	Ethical hacking is behind in creating reports on how hacking was done and how many chances are there for hacking

Roles of a Cyber security expert

We understand the difference between cyber security and ethical hacking. Now we are going to check the responsibilities of a cyber-security expert and ethical hacker. The exact roles of both will differ according to the organization, but we can say some general responsibilities of both security experts and ethical hackers.

As we said, cyber-security is responsible for maintaining the security of the organization. It is a defense game that provides monitoring of the network and makes strategies according to the attacks. Let us see some of the roles of cyber-security experts below

1. The main role of a cyber security expert is to maintain security and check any errors in the security systems
2. The help to make the security system updated and efficient
3. A security expert should check for every security system update available and must install them without delay
4. He should keep all the systems and network devices on monitoring for any malicious activity that is from inside or outside
5. He must be the responsible person of the organization to provide access rights to each person in the organization
6. He should make reports on the security measures and must be responsible if any malicious activity occurs
7. He must provide improvement reports with his suggestions to update the security if needed

Roles of an Ethical Hacker

Ethical hacking is a subset of cyber-security that specializes in penetration testing for finding vulnerabilities that a hacker can use to enter into organization security. Role of an ethical hacker are

1. The ethical hacker should do a penetration test and check the security performance.
2. He is responsible for searching and finding the weak parts in the security that may lead to a security breach
3. He is responsible for checking all the security breaches and giving reports for improving the security of the organization
4. He is responsible for doing pen tests on the networks devices and systems to check is there any chance to violate the security
5. He has to provide complete reports about the risks and possible points that lead to security breaches and what he did to resolve them.
6. He has to communicate with a security expert about the possible attacks, how that attack impacts the organization.
7. He has to use all the hack tools and methods on the security system to give solutions for the impact of hacking.

Roadmap to cyber security career for beginners

Cyber-security is the study related to the security of network devices and systems and their sensitive data from the attackers. Here we are going to discuss the path or road to reach a cyber-security professional path for beginners. Now, most of you are standing at a point of completing graduation or working in some jobs, but deeply like to become a cyber security engineer.

A cyber security profession is a highly paid job and has a huge number of diversities to divert inside the cyber-security. The job data says the need for cyber security engineers are increasing rapidly and many organizations are offering huge payment for cyber security experts.

Don't select the cyber security profession if you are not much interested in networks and devices and the packets and all. Also, a security engineer profession has to face different challenges every day that too in critical situations, so select the cyber security career if you are really interested in it.
Let us begin the journey, of how to become a cyber security professional.

What is cyber security?

It is a basic question as it provides the security for the network devices and systems that are working in cyberspace from the attacks which are done by cybercriminals. The definition is simple and lets us see how it becomes while going in-depth.

According to data and graphs, the cyber attacks are increasing every day as almost all type of users and organizations are entering to cyberspace for their daily routine and the need for cyber security experts are at peak as around 3.5 million jobs are available around the globe and it is the perfect time to start your career in it.

Cyber security career options

We already discussed that cyber security is a vast area with a lot of diversification inside it and let us see many job types are coming under cyber security. According to the employment data around 400000 professional shortages is there in the US only for a cyber security job. Let us see the job types in cyber security

1. Security analyst
2. Network security professional
3. Cloud security professional
4. Application security professional
5. Identity and Access Management (IAM) professional
6. Security architecture engineer
7. Penetration tester
8. Malware/forensics analyzer
9. Incident response analyst
10. Cryptography professional
11. Security train professional
12. Security auditor
13. Governance, Risk and Compliance engineer

Please understand these are not the full list as it is beyond our scope. These are some of them in the list and there are a lot of more career options in cyber security

Getting started in a cyber security career

1. Qualification

To start with you need a basic qualification as graduation in information technology or computer science-related course or any equivalent graduation as a basic building block. Please keep in mind there is no need to be engineering graduation it can be any graduation that is related to Computer science.

2. Skills

Next, you need to check the skills that a cyber security professional has which is really important to handle the security threats that are really happening suddenly and should be resolved in real-time as soon as possible. The skills needed for a cyber security professional are

1. Have knowledge in programming languages like java, python, c, and know the operating system Linux.
2. Have the ability to work under pressure
3. Problem-solving skill
4. Good communication skill
5. Basics of network and internet

3. Learn basics

Once you reach this milestone then your track to becoming a cyber security professional is half done. Now you have to learn the cyber security basics, OSI model of networking, terminologies of the network, Working of the internet, Hacking tools, Security policies, Type of threats, etc for getting the next building block of your path. We prefer to refer to any online free course to get this knowledge. If you are interested you can refer to our tutorials as it is refined and simple to learn about these all.

4. Read as many as you can

In this stage, you have to increase your knowledge as much as you can. Read a maximum number of online courses and tutorials available. If you are ok you can take paid courses at this stage and update your knowledge about the latest security measures hacking methods viruses and threats the world is facing. You can check tech magazines for such knowledge.

5. Prepare yourself

This is an important milestone as you are going to start practicing. Make your lab in your computer and don't forget to use only Linux for preparing the lab. Go and check simple hacking and security tools at first. Keep in mind to get maximum knowledge before practicing a tool. Also, be careful about the threats while checking for the tools. Work with firewalls and security measures to get more knowledge.

6. Select your path

In this milestone, there will be a lot of roads you can see. As we discussed above there are a lot of cyber security jobs and career options. Never take an option to look only at rewards, select one which you are interested in and confident to go further. Once you select the path, refine your search and practice according to that path.

7. Look for certifications

Now you are like a pro in your knowledge and practice but that is not enough for an organization to select you. You have to take any certification depending on the path you selected for impressing the organization. Never jump to this step without reaching the previous milestones as it will make your journey fail.
Let us see the important certifications in cyber-security

CompTIA Certifications

- A+
- Network+
- Security+
- Linux+
- CASP + : CompTIA Advanced Security Practitioner
- CySa+ : CompTIA Cybersecurity Analyst

EC Council Certifications

- CEH: Certified Ethical Hacker
- CHFI: Computer Hacking Forensics Investigator
- ECSA: EC-Council Certified Security Analyst
- LPT: Licensed Penetration Tester

ISACA Certifications

- CISM: Certified Information Systems Manager
- CISA: Certified Information Systems Auditor Cisco Certifications
- CCNA Routing & Switching: Cisco Certified Network Associate
- CCNA Security: Cisco Certified Network Associate

ISC2 Certifications

- CISSP: Certified Information Systems Security Professional
- SSCP: Systems Security Certified Practitioner
- CCSP: Certified Cloud Security Professional
- CAP: Certified Authorization Professional

8. Attend conferences and meetings

Try to get more and more knowledge about the network trends and their threats by attending important conferences and meetings that will help you to become smarter and smarter and be professional. Attending the meetings and conferences is worth not only for building knowledge but also for getting more and more relations which will be good in your career.

9. Practice Practice practice!!!

This is a never-ending milestone in your career as you have to gain knowledge and practice more and more all-time to become more worthy in the industry, do more certifications, and make more and more achievements in the career
GOOD LUCK!!!

History of Cyber security

From the previous cyber security tutorial, we understand what is the need for cyber security and what are the threats we have to face when using cyberspace or the internet. Before going to know in-depth about cyber security, it's very important to know where it all started and how we got here.

In this tutorial, we are going to know the history of cyber security that including how it all started and how it become such important, and what all changes have come to cyber security and cyberspace. The cyber security concept started in 1969 from a research project because of the invention of deadly viruses that are able to destroy servers or can steal user data.

Where does Cyber security begin?

The concept of cyber security was started in 1969. A professor of UCLA called "Leonard Kleinrock" and one of his students, Charley Kline' able to send an electronic message from his computer which was the first electronic message ever sent in the world to one of the programmers called 'Bill Duvail' at Stanford.

After that incident, a year after that, in 1970 one of the researchers of BBN technologies named "Robert Thomas" created a computer virus [which is supposed to be the first virus] and he understand the fact that a computer program can able to travel from one computer to another, and able to make some changes to the computer it travels.

He was thrilled and made it to travel through the Tenex terminals making a display message of "I am the creeper and catch me if you can" he also named that computer virus as Creeper. The creeper started traveling and it made many Tenex terminals to display the message and that triggered the need for a program to stop such creepers.

It was "Ray Tomlinson" the inventor of the email system which we use today to see this creeper program and like it. He thinks about that and understands the hidden danger behind such programs and starts work to stop this creeper program.

He made another computer program and named it "Reaper" it is the first known antivirus that aims to find the creeper and delete the copies of the creeper.

How much Cyber Security has reached now?

Now you understand the story behind the trigger the formation of cyber security. That Creeper and Reaper programs were made just for fun as it doesn't cause any problems to anyone. But as computers and networks made an immense development, criminals start to think to use the loopholes for stealing user data and even destroying a network or a computer.
When the internet and cyberspace become more and more popular then came the hackers who hack many systems and user data which is very dangerous. A German citizen hacked even many military computers and was able to access its data, even from the pentagon systems.

In 1987: the antivirus started to be used for commercial activities and available to the common man who was able to buy an antivirus for his computer.

1. Andreas Luning and Kai Figge were behind the first antivirus which is called UVK mean Ultimate Virus Killer. After that NOD antivirus was created
2. John McAfee from the United States found the McAfee
3. In the same year, the Bernd fix caught a wild virus which is named as Vienna virus. Which is supposed to be the first malware.

You heard about Morris worm or Internet worm. It was a man named Robert Morris who invented a computer worm with a crooked intention to know how many computers there are on the internet. He wrote a program to know that. Morris worms can infect a system multiple times and start running in the system making it slow and destroying the system eventually.
There are millions of stories like Morris and different hackers who made different computer viruses and malware. IN the present situation even some countries are making malware and worms which are able to get the information from other countries' systems.
In the **1990s**: there were drastic changes in the internet and cyberspace which make the world go online and some important issues also come with online changes.

1. First Polymorphic Viruses detected: Polymorphic viruses are next-gen viruses that change a file and spread but keep the original program intact so no antivirus till that date can find it.
2. Another virus named Disk Killer was detected by a British magazine which infects and destroys millions of computers.
3. It made the establishment of EICAR that is the European Institute for Computer Antivirus Research.

Now we have a different range of anti-viruses and anti-malware to protect from the known viruses and worms. But we can hear the news of new viruses and worms which make us understand the need for cyber security.

Types of Cyber Attacks

We know we are living in a digital world where almost all our daily activities depend on the internet and electronic devices such as e-shopping, mobile devices, social media, online banking, and many more. This dependency can lead to illegal hackers and cybercriminals opening a way to steal your information and identity. Now, these illegal activities have grown into a fearful crime world.

A cyber-attack can be defined as an illegal attack or accessing of a computer or a network and stealing the data from it or trying to destroy that system or network with the help of a computer worm or malware. This kind of attack leads to loss of information or identity or even money can be referred to as cybercrime and the person who is behind a cybercrime is called **cyber-criminals**.

Broadly the cyberattacks can be divided into two types which are based on the impact of the attack that are

1. Web-based attacks
2. System-based attacks

WEB-BASED ATTACKS

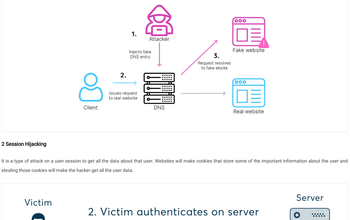
As the name suggests, web-based attack is a attacks that target websites and network components. It can make an impact on any website or web application directly or indirectly. Some of the web-based attacks are

1. DNS spoofing
2. Session Hijacking
3. Injection attacks
4. Phishing
5. Brute Force
6. Denial of Service
    1. Volume-based attacks
    2. Protocol attacks
    3. Application layer attacks
7. Url interpretation
8. Dictionary attacks
9. Man in the middle attacks

1 DNS Spoofing

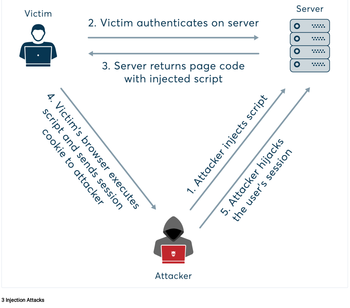
DNS is called Domain Name Server, which helps the request from the user to reach the correct IP address of the website. DNS spoofing is a method where the hacker adds data to the Name server cache that diverts the user requests to a wrong IP address or a wrong system.

This kind of attack diverts the traffic to a wrong server or a system and it can stay on the Name server cache without being caught for a long time.



2 Session Hijacking

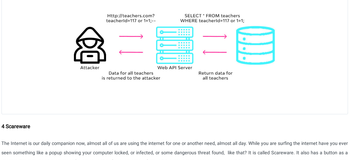
It is a type of attack on a user session to get all the data about that user. Websites will make cookies that store some of the important information about the user and stealing those cookies will make the hacker get all the user data.



3 Injection Attacks

It is a different kind of attack on a website where the hacker will inject some codes that can able to manipulate the website database and the hacker can able to get all the information from that website database.

Example: SQL Injection, XML injection, etc



4 Scareware

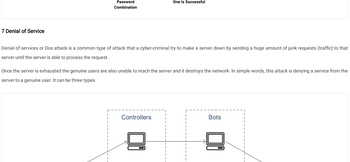
The Internet is our daily companion now, almost all of us are using the internet for one or another need, almost all day. While you are surfing the internet have you ever seen something like a popup showing your computer locked, or infected, or some dangerous threat found, like that? It is called Scareware. It also has a button as a remedy like downloading some software or asking for a payment. If you click such a download button a malicious program gets downloaded and installed called scareware in your computer that makes your computer locked until some ransom is paid or even steals data from your computer.

5 Phishing

Phishing is a type of cyber-attack that aims to steal the user's sensitive information like login information or the bank transaction details or credit card details. It is done usually through email where the hacker sends an email that will appear to be from a genuine source. It was also used to install the malware in victims' computers.

6 Brute Force

We already heard about the need for creating a strong password that includes numbers, special characters, etc. that is to regulate this type of attack called brute force. In a brute force attack, the hacker tries many combinational guesses until he finds the correct credentials. This method is also used to crack encrypted data.



7 Denial of Service

Denial of services or Dos attack is a common type of attack that a cyber-criminal try to make a server down by sending a huge amount of junk requests (traffic) to that server until the server is able to process the request.

Once the server is exhausted the genuine users are also unable to reach the server and it destroys the network. In simple words, this attack is denying a service from the server to a genuine user. It can be three types

7.1 Volume Attacks: Hackers send huge traffic to make the bandwidth of a website get exhausted.

7.2 Protocol Attacks: this type of DOS attack makes the server resources exhausted as it consumes the original server resources without any need.

7.3 Application Layer attack: Its main aim is to make the webserver

8 URL interpretation

Every server has some pages that will not be accessible to the public. In URL interpretation the hacker changes the URL and makes the server deliver the secret pages to the user.

9 Man in the Middle Attack

As the name suggests the hacker intercepts a connection and acts as an intermediary who is between a user and a server. The hacker is able to read and modify all the messages that the user and server communicate.

10 Adwares

The Internet is full of ads and that is the major revenue source of many websites running in cyberspace. But some criminals make some malware that forces the user to show the ads and redirect the user to an ads page or a product page.

SYSTEM BASED ATTACKS

The above attacks are based on a network and the internet. Now there is another type of attack, which targets the system and its resources.

1. Virus
2. Worm
3. Trojan Horse
4. Back doors
5. Bots

1 Virus

As the name suggests, it is a bit of computer code that can able to travel through the computer system and spread without the user knowledge and able to self-replicate and it contains an executable code snippet that will be capable of destroying a system or able to steal some data from the system that is infected. Some of the world's dangerous viruses are

- Morris worm
- Nimda
- ILOVEYOU
- SQL Slammer
- Stuxnet
- Cryptlocker
- Conficker
- Tinba

2 Spywares

Spywares are some malicious program codes, which are being installed in the target system without the user's knowledge that is able to steal the sensitive information from that system and send that information to a remote server. Usually, the browsing pattern and interests of a user are sent to the server.

More dangerous spyware includes keyloggers, which can able to access our password that we type on our keyboard and send the data to the server. Usually, malware will get installed while installing freeware that we download from an unknown source.

3 Worms

Worms are a kind of virus that aims to steal sensitive information or to destroy a network or a system. Unlike the virus, a worm does not need any human activity to spread from one infected system to another system in a network. Worms replicate and spread through the network using email or the loopholes in an operating system. It also uses the resources of the network or a system making it slow or unusable for authentic users.

4 Trojan horse

Trojan horses are an old war structure that hides the folders inside a huge horse that has a backdoor and it attacks from inside the enemy territory. Like that Trojan horse is a code snippet that pretends to be authentic software from an authentic source but can able to make unexpected changes to the host system. Trojans will run as a normal program but it will destroy the data in the host system and make it vulnerable to attack like opening a backdoor for a remote system to control this host system. Trojans can able to make many host computers to be controlled by a master computer and it forms a network of such zombie computers. Trojans are less dangerous than worms and viruses because they cannot replicate or spread to another system in a network.

5 Backdoors

It is a method of bypassing an authentication process, it is usually done by the developers to access some applications. But cybercriminals use this method to crack many paid software, even the operating systems.

Introduction to cyber crimes

The Internet began to use in 1960. In the beginning time, it was not an issue to deal with cyber crimes as it is not accessible to the public. Only the defense systems of a country and the top officials of a country uses the privilege of the internet and the scenario was smooth and good.

In the late 1990s, the internet was more developed and it was the beginning that the public was given access to the internet and the internet started to spread its wings in the public. In every good, there will be a hidden bad thing inside it. The Internet was not different from that as the criminals started using the internet to steal others' personal and sensitive data and even destroy a system in a network. It varies from simple adware to complex viruses that are able to destroy a system and steal all its data.

At the beginning of the 2000's the cybercrime rate increased and every country's law enforcement started to deal with cybercriminals. Packet tracing and packet tampering and stealing data using middle man attacks and much more complex threats come into the picture. The focus of cybercrime definition changes from destroying a computer to destroying or manipulating or stealing data in a computer or from a network.

Classification of Cyber Crimes

Now cyber crimes are increasing and it is expected that millions of people are getting impacted by cybercrimes every day around the globe. So we classify the cybercriminals as inside or outside criminals for an organization.

Inside Attack

An insider attack can be defined as an attack that is performed by an authorized person in that organization. Mostly this happens from an employee who has a criminal mind or is highly dissatisfied in the organization who has all the authorization to access all the networks of that organization.

The inside attack is an easy process for the attacker and it can make a high impact on the network or the system as the attacker knows about the network and its security and its easy to make a huge impact from the attacker to make the network crash. Installing intrusion detection internally is the only way to reduce the internal attack.

Key sources of inside attackers

Outside Attack

It can be defined as an attack from an outsider with or without the help of an insider of the organization. This attack can be fatal as it not only causes financial loss and loss of sensitive information, also the loss of the organization's reputation and trust.

An external attacker will be monitoring the network for some days before the attack to get much information so the only chance to block him is to make a strong firewall and gateway and also hire a network professional and if needed ask the help of an ethical hacker to respond to the attack.

Another classification in cyber crimes as structured and unstructured attacks that is classified according to the level of knowledge of the hacker or the level of impact of the attack. It can be simple to fatal depending on the attacker's skill and experience.

Unstructured Attacks

These types of attacks are done by amateurs who don't have any skill or experience in the field of networks. it has only a negligible impact on the network. the major reasons behind such attacks may be fun or trying a new hack tool or trying to get some money or to impress someone.

Structured Attacks

These types of attacks can be fatal and make much loss for the organization because it is done by professional hackers who have much skills and experience in network security and its layers. They have a well-defined aim and have perfect skills and tools to open the firewall and network security. They can able to mask intrusion detection and such criminals are dangerous mostly by some rival country or from terrorist groups, etc.

Now in this modern world cyber crimes are becoming a low-cost investment and secret method to make a high income. So Understand about cyber security and making precautions for cyber crimes are almost all country's responsibility, even every individual must know about basic cyber security to protect themselves.

Causes of Cyber Crime boom

1. **Money**: immense amounts of money are involved to attract criminal minds.
2. **Revenge**: it is an easy and safe way to take revenge upon an organization or a person.
3. **Fun**: amateurs do the cyber crimes just for fun or to impress someone
4. **Easy Availability**: Many tools for attack are now readily available on the internet.
5. **Anonymity**: There are many tools that hide a criminal in cyberspace making criminals anonymous and can do anything without being caught.

Types Of Cyber Attackers

From the previous tutorials, we got knowledge about the internet and the attacks happening in cyberspace, also about cybercrimes. Now we are discussing the different kinds of people who are behind these cyber-attacks and cybercrimes. We call them Cyber Attackers or Cyber Criminals.

We can define them as an entity which may be a person or a group of persons or even an organization who are doing some malicious job to attack a system or network with the aim of stealing information, gaining access, or even destroying that network or system.

As we know the internet is growing so fast and more and more people are coming to this cyber world and spending more time and their activities here. Attackers are using different methods and tools which are readily available in the deep web or dark web for doing such criminal activities.

In broadly we can divide the cyber attackers are of four types,

1. Cyber Criminals
2. Hackers
3. State-sponsored attackers
4. Inside attackers

CYBERCRIMINALS

Cybercriminals can be defined as a group of people or an individual who is working with the aim of stealing some sensitive information or accessing some sensitive computer or network or anything that is mentioned in crime crimes. They are dangerous and skilled and are able to use sophisticated tools and methods to destroy network security. They are able to make a lot of revenue from this method.

We can divide the criminals who are in the cyber world as

1. Attackers who attack other systems and try to destroy that system or steal some information from that system.
2. Attackers who are doing crimes like gambling fraud or spam use their system for such activities.
3. Attackers who use the computer to steal some data illegally

Refer to the cybercrime tutorials to know more about cybercrimes and criminals

HACKTIVISTS

These are people who are not included in cybercriminals as they are not doing any criminal activity such as destroying a computer or stealing sensitive information but they work and do some malicious activities for promoting some agenda which they believe may be political or religious or anything. They are using cyberspace to promote their interest and try to make their followers. We can call hacktivism digital disobedience.

STATE-SPONSORED ATTACKERS

Every nation has its own interest and has its own secrets in military and political and commercial areas. It is the government's duty to protect such secrets from all threats outside or inside the nation. Every nation has a highly skilled team of hackers who are working for the government and checking the security of every government secret. These hackers help the government to protect the secrets and block all the other hackers and attackers from inside or outside the nation. They are highly capable of attacking any other hackers or attackers as they are using huge resources of the nation.

INSIDER ATTACKS

Insider attack comes within the organization which is done by some employee or former employee who has knowledge about the network and its security measures and also has the credential for the login. These types of attacks have more precision and impact. We already discussed the insider attack in cybercrime introduction but here we are looking into it more deeply.

We can classify the insider attackers as

1. Malicious
2. Accidental
3. Negligent

MALICIOUS

These are serious types of attackers who are doing such harm to the organizations as destroying the system or network stealing sensitive information and gaining access to deep security areas. Mostly the aim of such attacks will be revenge or some financial gain. These attacks are highly precise and targeted so they can cause serious damage. Installing intrusion detection systems can help up to an extent.

In some cases, the inside attacker will pretend to be an outside hacker and it is not easy to track such criminals who are working inside.

ACCIDENTAL

As the name suggests, these attacks are not intentional. These attacks happen if anyone deletes a serious file accidentally manipulates the data inside a file or accidentally discloses some important information to an outside organization.

NEGLIGENT

These types of attacks are not intentionally thought to harm the organization but some employees are negligent to the policies of the organization and cause harm to the organization due to their negligence. For example, if the organization has a strict policy of file sharing, some employees are neglecting the company policy and an external hacker got that data from such negligence. Another example is using the company login credentials in an unsafe environment to help the hackers to get access to the organization gateway.

Cyber Security Principles

The increase in the usage of the internet compels the governments of different nations to make good security for the internet. The companies in the United Kingdom first recognized the need for some guidelines in using the internet. The use of such guidelines is to help the common people securely use cyberspace and limit cybercrimes and attacks. Cyber security includes the protection of sensitive information, systems, and networks from cybercriminals.

We talk about the guidelines that are made to protect and inform the clients of different internet providers. These guidelines are made with the coordination of government and internet providers who have a wide variety of clients whose needs are different from each other.

Now let us check the guidelines one by one in detail

1. Make a Risk Management system
2. Economy
3. Secure all Configurations
4. Fail-safe defaults
5. Manage User privilege
6. Open Design
7. Monitoring
8. Complete mediation
9. Prevention of Malware
10. Privilege separation
11. Least common mechanism
12. Psychological Acceptance
13. Removable Media Controls
14. Wok factor
15. Compromise reading

1 Risk Management System

Risk and attacks are inevitable in an organization which is the same in the case of the internet. An organization must have a set of rules and policies which will be followed in case of an attack called a risk management system.

This set of rules and policies are made with the help of high experts and the organizations-related peoples analyzing all the possibilities of the risk occurrence and prioritizing them to make the perfect rules.

Once the risk management system is ready, all the employees and the people related to that organization must know about that system and act according to the rules inside that system in case of a risk.

2 Economy

The security process must be simple and easy to implement. We must simplify the design and reduce the implementation process because in a simple design, it will be easy to correct the errors and there will be less chance for the errors to happen in simple models. Also, the testing for errors will be easy and cost-effective in a simple model. We also are careful to have simple interfaces of different modules in the security system which helps to reduce the wrong assumptions.

3 Secure All Connections

This principle states that we have to secure all the configurations of computers and the network while we configure the system and network. If we are securing it at the time of configuring the computer we can reduce the risk factors in the system. This process includes disabling autorun, managing security breaches, and removal of all unwanted functions to remove all the risk factors.

4 Fail-safe Defaults

This principle is simple and easy to understand as it says that a default configuration of a system or a network should have protection from all other accesses. It also states that the permissions granted by the new systems must be limited. The access to the security modules and sensitive areas must be limited for new systems or users.

For example, suppose we have a system in which we access the admin privilege. One day another user came and asked to use your system for some days, you will not allow him to access the admin account. According to the principle, we must create a guest account for that user with fewer privileges than the admin for the security of that system.

5 Manage User Privilege

This principle states that the permissions that are granted to any user must be for a task and it should be allowed only for completing that task duration. This privilege control is to control the user privileges for a maximum short time and is allowed only if it is needed.
For example, suppose you are working as a network administrator and one of your coworkers needs access to the network. In such case, you must check his need and calculate the privileges he needs to complete the task and allow that privileges only the duration to complete his task

6 Open Design

This principle states that the security implementation need not need much secrecy and complexity in its design, it means more secrecy or complexity doesn't mean that it is more secure. It can be applied to not only the credentials or network also to the computer systems

An example of this principle is the Content scrambling method that is used in CD.

7 Monitoring

Every organization must have installed intrusion detection and prevention facilities, but in some cases, it may fail to detect and prevent an intrusion. In such scenarios this principle works, it states that organizations have a monitoring policy, which gives an eye over the security activities happening in that firm.

Monitoring is done by monitoring each system and the network and the user activities also, it must have good backing up policies.

8 Complete Mediation

On the internet, there will be caching of information which is done to make the process easy and fast like saving the login information of the previous login so that the next login will be easy and fast. But complete mediation principles state that no such caching of data is allowed in a network which means we have to check the privileges of the user every time when the user needs to access a network or object.

This makes the process a bit complex and time taking, which reduces the performance a little, but it is essential for security as the login rights and privileges can change at any time. So each user has to log in for every access to the objects in the network to check the privileges of the user.

For example, in online banking, each user has to log in every time and for doing every transaction, even the backspace will not work in that scenario.

9 Prevention of Malware

Malware is one of the major and common issues faced by almost all organizations around the world. It may come in many forms and ways. Malware doesn't have a common form or way to infect so a unified approach will not work to prevent malware.

Mostly it comes through email and network. Use good spam detection in email. Use email thread protection to prevent email from phishing attacks. Install good firewalls and intrusion detection in networks. Use a good updated antivirus in each system in the organization.

10 Separation of Privilege

This is one of the important principles as it states that two-step verification is needed. In general, we can say that the system allows permission only when more than one condition is satisfied. It implies that one condition is not enough to grant a user the privilege to the network object.

11 Least Common Mechanism

This principle is for sharing of resources as it implies limiting the sharing of resources. It states that the resources shared between the users must be minimum.

12 Psychological Acceptability

It is a psychological effect that the security mechanisms for a resource should not be much complicated. Suppose we have a computer where its security measures are so complicated then the users will not take necessary precautions before using the sensitive information.

13 Removable Media Controls

Removable media will act as a hub for a wide range of viruses, worms, Trojans, and malware. It can easily infect a system when a removable media is connected to a system and it can spread from that system to the entire organization network.

Every organization must have a strict policy in using removable media and it must have a good antivirus where we are going to connect the removable media.

14 Work Factor

This is a factor that is not directly related to cyber security but it is needed for making a good design in a cyber security model. According to this principle, the expense that is needed to make a security system must be comparable to the resources available for an attacker to make a plan to attack the network.

In some scenarios, it will be highly complex to find the cost and it is used to calculate the cipher strength.

15 Compromise Recording

It is a simple principle which states that we should record all the intrusions and trials for the intrusions because it can help us to make better security measures as we get an idea about the ways of intrusion.

An example of this is the cyber-connected cameras that monitor all the details.

Data Security

Data or information is the most valuable asset in this modern age. An expert attacker can do anything with the data or information. It is the users, organizations, or even government duty to protect data from any of illegal activities like stealing of data, manipulating data, illegal access, and even deletion of sensitive data.

Data security refers to the security of data from all the attacks on the data like stealing of data, illegal access of data, modifying sensitive data or even deleting the data. Data security needs a strong infrastructure and a team of good system administrators to secure the data from the attackers.

For designing a perfect security system for data protection, we need to preserve some basic things of data like

1. Integrity of data
2. Privacy of data
3. Prevent unauthorized deletion of data

For the proper design of data security from all type of attacks like intrusion, modification or deletion of data, and to maintain these three basic principles of data we have to consider some aspects stated below

1. Do Proper Encryption on data
2. Need proper Data Backups
3. Anti-malware protection
4. Need good Archival Storage
5. Use a proper firewall
6. Efficient Disposal of Data
7. Follow Principle of Least Privilege.

Data Encryption

Data encryption is a security method where we encode data means changing that data from the readable form to an unreadable form using a key. It can be converted back using another key and that process is called decryption or decoding the data. Data, which is encrypted, is called a ciphertext that a middleman attacker cannot read or understand.

Cyber security prefers to encrypt the data while storing the data and transporting the data. As you know all the electronic messages are now in encrypted forms like email or WhatsApp. It helps to protect the data from cyber attackers even if they got access to the data. Every bank transaction including the credit card using the encryption technique. Software, which is used for encrypting data, is called an encryption algorithm.

Types of encryption

Encryption can be broadly divided into two types depending on the key that is used for encryption. That is

1. **Symmetric**: In symmetric, the data is encrypted and decrypted using the same key. That means we need only one secret key that the sender and receiver know to encode and decode the data. Examples, AES, DES, IDEA, RC4, etc
2. **Asymmetric**: In Asymmetric encryption, the data is encrypted using a key, which the sender used to encrypt the data called a public key. And there will be another key the receiver use to decode the data known as the secret key. Examples, RSA, DSS, ECC, TLS, etc

Backup of Data

Backup of data is one of the basic and oldest methods in data security. It is the process of making one or more duplicate copies of the data and saving such copies in different mediums like cloud storage or in physical devices like hard disks is commonly termed as a backup of data.

We have to do the backup of data on a regular interval basis as it helps us to recover the data, if the original data is lost or corrupted either accidentally or by some malicious attacks. Below are the advantages of data backup

- Loss of data accidentally or intentional attacks
- Loss of data from a cyber-theft
- Keep data reliable, which will be authentic and accurate.

Now we have to decide how many copies of data have to make for a secure backup. For perfect backup security, there is an international method which is the 3-2-1 rule.

- Make three copies of the data
- Use two different mediums for storing the data like HDD or disk
- Must have server backup, which means having a copy of data in the server where the website is hosted.

Now we have to think about the mediums, which we use to backup data. The popular mediums for backing up of data are

- The hard disk which may be external or internal
- Server
- Cloud storage
- Cd or DVD backups
- USB flash drive
- University Archives

Finally, we have to follow some important things before making the backup regarding the security of the medium where we are going to save the backup of data

- Must have data encryption while storing and transferring data
- Must have user access right depending on their role
- Must save in medium with a good firewall
- Must have a good antivirus and user authentication
- Use Linux systems for the backup as preferably SElinux

Anti-Malware protection on data

Malware is the short form of malicious software that is a program that is designed to infect and spread in computers, networks, etc, and can able to manipulate or steal data or information and also can able to destroy a system or a network.

Malware is not easy to identify as it can be found in almost all places like email, the internet, websites, etc. Malware includes viruses, worms, Trojans, scareware, adware any of them, which are hidden in a system or network.

We must use an updated antimalware detection system in the place we store our data as we are under malware threat. Use a good updated antivirus and must do the periodic scan for any infections be careful using the system while accessing email and surfing.

Follow Proper Data Archive

Data archiving is storing data in a secure medium for a long time. In some organizations, there will be a huge amount of data and a huge amount of that data will not be actively useful for the day-to-day operations of the organization but will have to keep that data securely which is called data archiving.

For example, in a bank, there will be plenty of accounts and their history. Many of the accounts will not be active at that time but the bank saves all the records of the accounts even it is not functional, which is called archiving of data. It is essential for an organization for any future needs. A good data archive must be secure and indexed also have a good search option to find any needed data without any effort and cost.

Now we all will think about the difference between data archiving and data backup. Data backup means we are saving a copy of data, which is actively using the system for the data security to use in any kind of loss or corruption.

Where, data archiving is the process of saving the data, which is not actively used by any organization but needed for any future reference. Data archiving in proper intervals helps to reduce a load of active data and its cost.

We can archive data in different mediums such as in the cloud or offline or online like hard disk or servers. Wherever we are archiving the data it must be secure, safe, accessible and fast.
Consider the following things for the best data archive and for long-term usability.

1. **Storage medium**: Archiving of data is to store the data for a long time securely, so we must select the best storage medium, which can able to hold our data for a long time
2. **Storage Device**: Selecting the storage device depends on the accessibility of data. If we need to access or refer to the data often we must select a medium that can able to do that. All above choose a device that can able to hold our data securely for a long time
3. **Revisiting old archives**: Policies about the archiving and the archiving options will change in time as the technology is changing also the policies. So we have to revisit the old archives to check is there any change needed in the archive.
4. **Data Usability**: As we said data we archive must not be used for data to day activities but we need that archive for future references, so we must use a format that can easily make the data usable for referring without much cost and effort.
5. **Selective archiving**: In some cases, we don't need all of the data to be archived and it will make a huge cost and effort for storing all the data. In that situation, we must be selective in which data need to be archived and which part of data is to be avoided from archiving.
6. **Space considerations**: Many organizations like banks, governments, and IT sector firms have a huge amount of data to archive. It is essential to consider the space needed for the archive and that too becomes cost-effective. Tapes are the best portable medium.
7. **Offline or online**: Next is to decide the archive is stored online or offline. If you are deciding to be online as a cloud, it is easily accessible but vulnerable to attackers and corruption. On the other side offline medium like portable tapes, it is secure but not easy to access the data.

Types Of Cyber Security Threats

As we discussed, cyber-attacks are increasing day by day and it is estimated around 6 trillion US dollars will be lost in cyber-attacks by the year 2021. Strengthening cyber security and cyber laws are the only way to reduce this kind of loss.

At this time, it is hard to think of a day without the internet, not only entertainment but also financial, economic and even medical fields will be dependent on the internet. Can you imagine a day without a smartphone; the answer will be a NO for most of us. Modern generation is fully dependent on the internet so a strategic and well-designed method is needed for cyber security.

In this tutorial, we are discussing five major types of cyber security that help users and organizations be safe from cyber criminals and their attacks.

Critical Infrastructure Cyber security

This cyber security method is used for the systems and the networks that have critical infrastructure. These systems and networks are very important for the public as the public mostly depend upon them in their day-to-day activities. For example, traffic lights, Electricity, water supply, cameras in shopping malls, hospitals etc. Cyber criminals will attack these systems to get a point to enter into the network for attacking other systems in that network.

For controlling such cyber attacks on critical infrastructure the organization who works behind these systems and network must check the weak points in their systems and network where the intruder can enter. Also installs intrusion detection and prevention software.

Network Security

The Internet is a network of networks, we can have a public network, what we call the internet and there will be a private network that will be inside an organization. Network security help to secure the organization network from cyber attackers, and malwares.

We know we are accessing different websites for different needs from an organization or personal. The attackers are looking for a chance to get intrude inside a organization and steal the sensitive information.

Another example is the websites that using different cookies that may be even from a third party for their business but will make the users be targeted for frauds and sexual exploitation.

To tackle such situations, the organization must have installed security mechanisms, intrusion detection, a good firewall, and gateway for accessing public networks from the internal network of the organization. Also they must employ a good network professional and can ask for help from ethical hackers.

To upgrade the cyber security in a organization we can have these following

1. Extra logins
2. Password change at intervals
3. Use a antivirus
4. Install a good firewall
5. Private mode browsing
6. Monitor all the internet activities
7. Use a good encryption

Cloud Security

We know the next revolution is in AI. And many companies have already started using Artificial Intelligence (AI) for their operation which helps to improve their business in different aspects like high performance and good customer satisfaction. The issue is the huge amount of data and its maintenance is not an easy task for an organization as it is able to store such huge data in physical form and securely in the organization. Another problem with this huge amount of data is the authenticity of every data cannot be proved so there will be risk of cyber-attack.

To tackle such a situation the cloud storage is introduced which will be fast and secure; also, it can store any amount of data. Cloud systems have their own security measures and tools that make the data secure.

Internet of Things Security

A number of machines and devices are connected through internet and can be used through internet, which is termed as IoT, or Internet of Things. Iot will be the next revolution in the IT sector. With the help of proper cyber security measures IoT can offer wide range of devices and services to the users.

The major threat in implementing IoT is the risk from the cyber attackers. The scientist are trying to integrate the cyber security system to IoT systems also with many embedded system to assure the security.

Application Security

There are different users who are using a wide range of applications. We secured the network and system and we can't leave the application security. Many cyber attackers and malwares are attacking a user from the application and even stealing data from the applications.

Application security states that different security measures must be taken to protect the application and the user data using hardware and software while developing the application. With the application security, the companies are able to find the sensitive data and secure them.

Following are application security methods that organization implements

1. Firewall
2. Antivirus
3. Encryption

Other types of cyber security are

Information security

It is for the keeping the privacy and integrity of data by installing strong mechanisms for storing and transport of sensitive data.

Operational security

This security is involved in the operation of dealing the data assets. It involves the decision making tool.

Mobile security

Nowadays most of the data is on portable devices like smartphones or tablets or like other devices. Mobile security is involved in securing the mobile data from malicious attacks. Like stealing or unauthorized access etc.

OSI Model Layers and Protocols in Computer Network

As we know the computers are connected through each other and it forms a network of computers. The communication and data transfer in the network is by using packets. A packet have a header and a data part where the header contains the sender and receiver information and the data part contains data. There are many protocols and layers included in sending and receiving these packets.

OSI or the Open System Interconnection model, which can be called as a reference model that describes these layers and protocols, associated in sending and receiving the packets of data. It starts from the question How an application of one computer send and receive a packet through the layers to the physical medium to the application of another computer.

OSI model is developed in 1984 by the ISO organization, which consists of seven layers, and each layer is independent and has its own function in sending and receiving a packet of data.

Why OSI Model is needed?

It has many different points describing the need of a reference model in network that are

1. Easy to learn and understand each layer functions
2. Easy to maintain and troubleshoot of functions
3. Easy to add the new technologies that are developed
4. Can able to check a comparison of functions of layers.

Characteristics of OSI model

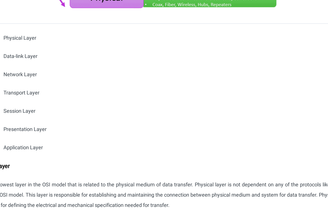
OSI model is an international model in network so it must be made as per international guidelines.

Each layer must be independent in functionality so that changes in one layer may not make the changes in another layer.

Make different functions in different layer and there should not be different functions in the same layer. Also do not make too many layer to make the architecture complex.

Total layers in a OSI model are divided into two which is application layers, which are the upper layers, and other network layers, which are lower layers.

Application layers are close to a user or an application, which is doing all the application related issues. Mostly application layers are dealing or communicating with the applications that are running in the systems in network.



The lower layers of the OSI model are designed with the network and physical medium of data transfer. Physical layer is the lower-end of the OSI model, which deal with all physical medium issues.

History of OSI Model

It was started in 1970 where the ISO conduct a seminar for making some international standard rules in networking

The need for higher level protocols was identified in 1973 in an experiment in packet switch system.

In 1983 the first model of OSI was initially developed but in 1984 the ISO accepted the OSI model architecture.

Responsibilities of OSI Model Layers

As we said, different layers are independent and assigned different function in the data transfer. Let us examine the OSI layers and its functions in detail that is essential to know about network and cyber security.

OSI Model Layers

1. Physical Layer
2. Data-link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Physical Layer

This is the lowest layer in the OSI model that is related to the physical medium of data transfer. Physical layer is not dependent on any of the protocols like the higher layer in the OSI model. This layer is responsible for establishing and maintaining the connection between physical medium and system for data transfer. Physical layer is responsible for defining the electrical and mechanical specification needed for transfer.

Responsibilities of Physical layer

1. It helps us to connect one or more devices physically.
2. It define how the data is transferred from one device to the other in the network, it can be Simplex, Half Duplex, Full duplex
3. It helps us to know the topology of the network, which means how the devices are arranged in a network.
4. It defines the signal type that is used in data transfer.

Data Link Layer

This is the next layer above the physical layer so the data from a physical layer enters the data link layer where the error free transfer of data frames happens.

Data link layer makes a format for data and establishes a protocol for the data transfer and communication of devices in the network.

From this layer we have the IP address of a device to identify each unique device (logical addressing) in the network.

For easy understanding the functions of data link layer it is divided into two sub layers that are

1. Logical link control layer
2. Media Access control layer

Logical Link Control Layer

1. It help us to do the flow control and error detection
2. This layer is involved in packet transfer to the receiver.
3. It check the header of the packet to find the address of network layer protocol

Media Access Control

1. It is the duty of this layer to transfer data over networks
2. It helps us to control how the devices that gaining to the physical medium and transfer data.

Functions of Data Link Layer

1. **Framing:** this layer is responsible for making the packets for data transfer that have header, trailer and data part.
2. **Physical Addressing:** Data link layer adds the address to the header part of the packet which is receiver address
3. **Flow Control:** Data send and receive must be at the same rate, maybe the data send rate must match with receiver processing power, else, the data will get corrupted. Data link layer is responsible for maintaining the flow of data and checking the rate of transfer.
4. **Error Control:** Data link layer is responsible for error check by CRC, which is cyclic redundancy check. The trailer that is added by this layer is for doing the error check. If the data is not perfect, the receiver sends the acknowledgement as a trailer for resending.
5. **Access Control:** It helps us to control the access that has the control that time, if more than one device is connected to the same channel.

Network Layer

Network layer is the third layer of the OSI model that is above the data link layer. Network layer is responsible for proper routing and forwarding the data.

This layer can able to find and locate the devices in a network and able to send the data using the best routes to reach the receiver after analyzing the network conditions.

In this layer, we are using the protocols such as IP, IPV4 and IPV6 for proper routing of packets that are called network protocols.

Functions of Network Layer

Addressing: Network layer adds the sender and receiver address in the header of the data frame.

Routing: As we said, routing is a process to find the perfect path to send data to the receiver. There are different routing protocols used in this layer

Internetworking: It makes a network by giving a logical connection to all the objects in a network

Packetizing: By using the IP protocols, the network layer makes the packets that it receives from the upper layers called packetizing.

Transport layer

Transport layer is the 4th layer of the OSI model and also called the heart of the OSI model. Transport layer is responsible for sending the data completely without any loss.

This layer makes sure that the data is transmitting in the perfect order as that send without any duplicate content.

Transport layer is the layer, which makes an end-to-end connection with the sender, and receiver to assure the data is send reliably.

Transport layer divides the data packets into smaller parts which can be called as data segments.

As we said this transport layer is responsible for end-to-end connection and data transfer without any loss or duplication. There are two different protocols used in this layer.

1. TCP
2. UDP

Transmission Control Protocol TCP:

TCP is a protocol that helps the data to be sent over the networks and it allows the devices in a network to communicate. It makes a connection and maintains the connection between the sender and receiver.

How is the data sent using TCP protocols?

In TCP protocols, the data is divided into different small parts that we call as segments; these segments are sent to the receiver using the best route. Different segments take different routes and reach the receiver in different order. The TCP reorder them to get correct data.

User Datagram Protocols UDP

UDP is another protocol used in transport layers but it is not a reliable protocol so it is not much used as TCP.

The problem with UDP protocol is that the receiver will not have the acknowledgement mechanism to inform the sender that the data is reached correctly. This lack of acknowledgement makes this UDP less reliable.

Functions of Transport Layer

Port Addressing: In a system, multiple process needs to send data to another system like browsers, ftp, etc which are using different ports or service points. It is the responsibility of the transport layer to transmit data from one process to another process.

Transport layer adds a port address to reach the packet that contains the address of the sender and receiver process so that it can reach the process of different computers correctly.

Segmentation and reassembly: As we already discussed, the transport layer divide the data into different segments with a sequence number before it is send to the receiver. The receiver will reassemble these segments using the sequence number before sending to the upper layers.

Connection Control: Transport layer can make 2 connections

1. Connection oriented: In this connection there will be a solid connection between the transport layers of sender and receiver and packets travel through single route.
2. Connectionless: here each packet is considered as a single free packet and it can take any route to reach the receiver.

Flow Control: It maintain the flow of data packets from end to end connection

Error Control: It performs he error check using the end to end connection. Transport layer make sure that all the data packets reach the receiver without any error.

Session Layer

Session layer is above the transport layer and this layer is more closely related to applications and processes running on the system.

Session layer is important to make and maintain the connections and communications between the sender and receiver applications.

Session layer is responsible for handling all the login and its credentials.

Responsibilities of Session Layer

Synchronization: Session layer is responsible for adding some checkpoints in the data while transfer the data. The usage of such checkpoints is to resend the data from that checkpoint if any error or loss of data is happened during the transfer.

Communication control: Session layer is responsible for allowing communication between two process of sender and receiver systems.

Session make and maintain and close the sessions.

Presentation Layer

Presentation layer is above the session layer, which is also called the syntax layer because it mainly concerns the syntax and semantics of the data that is transferred.

Presentation layer is a part of the Operating system that will convert the data from one format to another format before sending it to the receiver that is called as encryption.

Functions of Presentation Layer

Translation: The sender and the receiver system may not be using the same type of encoding. Presentation layer convert the data from the source-encoded format to a general format and this general format is translated back to the receiver format by receiver presentation layer.

Encryption: Encryption is processing of converting the data from one form another form for maintain the privacy and security of data. Presentation layer is behind the data encryption while transmitting the data.

Compression: Compression is process of making the sending of data little simple (reduce the bits in data) mainly used in multimedia transfer. Presentation layer is responsible for data compression.

Application Layer

This is the top most layer in the OSI model which will act as an interface to the user and the process to use the network. This layer's responsibility includes transparency and resource allocation. This layer offers services to end users for using the network for example are file transfer, email, remote login, etc.

Functions of Application layer

File transfer, Access and management: Application layer is responsible to allow the user to access the file in a remote system. Also manage and interact with another process in another system.

Mail: Application layer is behind the email services to happen in network

It allows remote login and use that system and also offers a large amount of database sources on the internet.

Security Techniques in Cyber security

The Internet is a booming technology now and every organization uses the internet for their day-to-day activities. Cyber security is a major concern in the present technology world. With the rapid growth in the internet there will be a lot of tools and techniques readily available for cyber attackers to attack any system or network.

Every institution in the internet is now vulnerable to attackers as they are using public cyberspace. Everyone is concerned to protect their network and system from the attacks. The three main measures that the institutions follow in cyberspace is

1. Preventive measures
2. Detective measures
3. Corrective measures

In cyber security, the organizations must know many techniques and technologies that help them to keep the attacker at bay without getting attacked. These techniques will help to maintain these three measures in cyber security

1. Encryption
2. Firewall
3. VPN
4. Intrusion Detection
5. Access control (authorization & authentication)
6. Antivirus

Encryption

We already discussed the method of encryption in our previous tutorials. Encryption is a cyber-security method that helps us to store and send sensitive information across the internet without losing privacy and security.

The process of changing the information to another format using a secret key is called encoding or encryption and the information that is changed into such format is called ciphertext.

The process of converting back to this cipher text using the secret key to the readable format is called decryption or decoding. And the information that is decrypted is called decipher text.

Encryption is of different types like those that are symmetric and asymmetric based on the key in which symmetric uses only one key for encoding and decoding, where asymmetric uses two keys one is public and other is secret for encoding and decoding the text.

Why is Encryption Important?

1. Data transit is vulnerable
2. Security threats are evolving
3. Many applications expose data
4. Hacking is highly profitable business

Firewall

Like that name, firewalls act as a wall of fire which helps to secure a private network from the vast ocean of networks in the public internet. Firewall can be defined as a network security system which can be hardware or software or combination of both that protects a private network from the unauthorized access and usage of private network resources from the outside public network.

When a Fire is installed all the data packets that are leaving or coming to a private network should pass the firewall and the firewall check each packet for any malicious activity.

Firewalls can be classified on different criteria, where we disucss only the important aspects.

1. Processing mode
2. Deployment area
3. Architectural Implementation

We can divide the firewalls based on processing mode such as

1. Packet filtering
2. Application gateways
3. Circuit gateways
4. Mac layer firewalls
5. Hybrid

Packet Filtering

Each data in the internet is travelled as packets from one network computer to another network. These packets have a header that contains the sender and receiver details and a data part which contains the data that to be transferred.

Firewall will act as a wall that checks each packet header for the sender and receiver information and validates the packet. Firewalls take the decision depending on the authenticity of a packet, whether to forward the packet or drop it there.

There will be a well set of rules inside the firewall to take the decision and it scans the network packets for any malicious activity in the packets. Most of the firewall will work on the rules combination such as

1. IP source address and destination
2. Direction
3. TCP and UDP port requests.

In detail packet filtering can be divided into different yes such as

1. Static filtering: In this type the rules in a firewall are decided by a administrator
2. Dynamic filtering: In this type the rules for the firewall are made by the firewall itself.
3. Stateful inspection: Helps to track the connections from internal and external systems.

Application Gateways

What is an application gateway?

Gateways are the place where a packet enters or leaves the system or a network. It is a firewall proxy, which provides network security for a system, which needs high security. It provides a secure communication between the user and server. This application gateway helps us to protect the data at the application level, which means it can filter some specific data from some applications like bittorrent, FTP, telnet, etc. This firewall will be the middleman between the requested user and the server which blocks malicious packets.

For example, when a user request a data from a server, the connection is firs establish between the user and proxy server and then the proxy make the connection with real server

Circuit Gateways

Circuit level gateways are the firewall, which works in the transport layer. Transport layer handles the TCP and UDP connections which mean these circuit gateways can able to handle the packets in a TCP or UDP connection.

These circuit gateways act in between the transport and application layers called session layer, which can handle and monitor packets and handshaking in TCP or UDP connections. This gateway can also act as Virtual private networks.

MAC Layer Firewalls

MAC layer firewalls will work in the media access control layer. It can able to filter the MAC address of the users who make requests with the server and is able to block a user if any malicious activity is found.

This layer will have a list of entries that include the MAC address of some of the systems, which act as host, and that list is called Access Control List. This list act as an important role in deciding which packet has to be sent to the host system.

Hybrid Firewalls

A firewall is the combination of all the firewalls we mentioned above so it can have all the features of the firewalls we discussed above.

Now another classification of firewall is based on the place where that firewall is intended to use like,

1. Commercial Appliances
2. Small Office
3. Home software

We have to choose a firewall configuration for an organization depend on some factors, that includes

1. Objective of network
2. Ability to implement the firewall
3. Cost affordability

We can divide the firewall configuration into 4 types according to these principles

1. Packet filtering routers
2. Screened host firewalls
3. Dual homed host firewalls
4. Screened Subnet firewalls

VPN

We all heard about VPN and other proxy methods to surf the internet to access any of the website without losing our privacy. A VPN stands for Virtual Private Network; It is a cyber-security technique to transfer files and sensitive information across the internet using a safe and secure tunnel.

How VPN achieve a secure transmission?

A VPN makes a connection from a user need system to a network that is encrypted and safe. This connection can be used for transmitting data and sensitive information without any eavesdropping or illegal accessing. Using a VPN can hide our IP and our geographical information so we can access any website that is restricted geographically.

VPN is like a firewall but protecting the user data and information in the internet. End user must have a login to enter the VPN servers and there the secure tunnels begin. Once the user enters the VPN server hey can send the sensitive information through these tunnels securely with privacy.

Intrusion Detection System (IDS)

Intrusion Detection System is a security technique in cyber security, which monitors the system and the network of an organization. IDS help the system administrator to find the attack that originated from outside or inside the organization.

Firewall is a security measure for an organization that helps us to filter the outside traffic to check the malicious activity from outside the organization, the IDS helps the system admin to protect the firewall as it give alarm to the system admin if anyone tries to break the firewall.

Intrusion detection system has different types that are the following

1. NIDS
2. HIDS
3. Signature based
4. Anomaly based

NIDS

It monitors the network traffic to find all the anomalies or attacks that originates from inside or outside the organization.

HIDS

HIDS stands for Host Intrusion Detection System, which runs on almost all the computers and networks in the organization. HIDS helps to monitor all the internal traffic and its anomalies. It also detects the traffic anomalies which the NIDS security monitoring failed to catch.

Signature Based Intrusion Detection

This is another monitoring system which is able to detect patterns that are malicious in nature. It helps to detect all the anomalies that come from internal or external sources. This helps to detect all the known patterns such as malwares but will fail to detect new threats.

Anomaly Based Detection System

It is used to monitor the threats that are unknown to the current scenario as the malwares are increasing a lot. It senses the malicious activity and informs the administrator.

Access Control (Authentication & Authorization)

Access control is a method of restricting access to a place or a system for unauthorized persons. Access control is a process for reducing the security risk from unauthorized access to sensitive information.

According to this principle, the privileges for accessing a resource will be given only to the required entities for the essential time required for them to complete the task.

For example consider a employee needs to access a system which have sensitive information for complete a assigned task for him. The system admin has to give him only the essential privileges to that information he needed and revoke the access after he complete his task.

Access control is a combination of two components Authorization and Authentication. Authentication is a process, which is done by the user with his credentials. For example, the username and password of a Gmail account. Authorization is a process that is done by an admin who gives access to the users.

Access control is of two types, which are

1. **Physical Access Control:** This is the access control, which is in physical form like access to a building, inside a bank etc.
2. **Logical Access Control:** Logical Access is like accessing a Gmail account, login to a computer etc.

Antivirus

Antivirus is a software which helps to protect a system from all types of threats like virus, worms, Trojans, adwares, malwares and many more. We have different methods to protect a network but we need an antivirus in every system to make them protected and always make sure the virus database is updated.

Antivirus software has a virus database which has the patterns and features all known viruses and threats. Antivirus scan all the files in our system for checking these kinds of patterns or features present and remove such programs into a vault and delete fro that vault. So We must use only an updated antivirus database for efficient results.

Cyber Security Policies

What is a security policy?

Security policies are defined as a set of high level rules that an organization issues by the high officials and security experts for all the employees of that organization who have access to the organization's sensitive information. It has the rules defining the way of accessing the information.

These rules are the non-changeable document in the organization which is responsible for all the information security from all the inside and outside threats. Security rules are a never ending document, which will be updated all the time where new technology and threats arrive.

For example, almost all the organizations have specific rules for accessing the documents and using the external devices in the company systems. In addition, most of the organization has written documents that employees are not allowed to take websites that are not secure.

What is the need for cyber security policies?

There are attackers everywhere that may be from inside or outside. For the smooth functioning and security of an organization, it must have some policies in handling the information. Some of the other needs for perfect security policies are

1. **Increases efficiency:** This can be quite helpful to avoid accidental and intentional damages while accessing the information of the organization. It can reduce the cost of many security systems if the employees know what they are allowed to use and not allowed to do inside the organization.
2. **Increases discipline and Accountability:** This will help the organization to increase its discipline as the organization has clear written rules for employees what they are allowed to do and don't. It helps to reduce the mistakes and make all employees more disciplined as the company is able to take action if an employee makes any mistake.
3. **Helps to make more business**: An organization which has very good security policies will increase the trust factor of that organization which will make the clients more confident to make business deals with those organizations that keep its information secure.
4. **Increases employees knowledge:** In an organization, it is not a mandatory requirement that all employees know about cyber security. If the organization has well written policies about cyber security, it will be helpful for the employees to know about it and helps to make strong credentials.

What are the cyber security types?

Every organization has its own criterias to make the security policies and discussing all of them is beyond our scope. Some of the important security types are

1. **Organizational security policy**: Organizational security policies is the overall security measures that the employees should follow inside the organization. This will be the basic security policy of that organization, from which other specific security policies are derived.
2. **System Specific Policies:** Inside the organization there will be different systems like customer applications, payroll systems, etc. system specific policies is the security rules for specific systems.
3. **Issue Specific Policy**: Issue specific policies are the rules which we have to follow when are specific issue is created inside an organization

What are the different security recommendations?

Some of the important cyber security recommendations are here,

Virus and Spyware protection

Virus and spyware are very important threats for an organization which is able to steal all the information and even can destroy systems in that organization. Virus and spyware policy provides the following protection,

1. It helps to detect and remove all the viruses and helps to repair the system damage caused by the virus impact.
2. It helps to detect the threats in files and applications that are malicious or suspicious.

Firewall Policy

Firewall is a gateway that helps to detect and block all the external threats from the cyber attackers. Firewall policy includes the following protection

1. It blocks all the unauthorized access and malicious packets coming from the internet.
2. Firewall can able to detect all the attacks from external criminals

Intrusion Prevention

Intrusion is the illegal access of the organization information and tries to corrupt or steal the information from the organization. Intrusion prevention helps to stop all the attacks which are coming from outside or from inside of an organization.

It detects and stops all the attackers and protects applications from malwares and vulnerabilities.

Application and Device control

This policy includes the protection of physical devices such as organizations computers and other devices and also deals with the protection of applications that run on the devices.

Exceptions Policy

Some organizations have some applications which are not included under this security scans such applications and data are included in exceptions policy. These applications or data don't come under security.

Host Integrity Policy

Every organization has clients who have access to the organization's data and applications. In such a scenario, this host integrity policy helps the organizations to enforce or define some policies that the client computer must have to access the resources of the organization. For example, a client must have an antivirus installed.

Which all issues are addressed in the cyber security policies?

Organizations' need for security policies will be different for each organization but there are some important issues that must be addressed by almost all organizations while making the policies of cyber security.

1. **Physical security:** These policies include the physical securities that organizations must provide to their physical devices and networks like datacenter, servers, systems, etc. it includes the access control, monitoring etc.
2. **Data Retention:** Organizations need a huge amount of data for the proper working. Data retention includes policies regarding how much data collects, where to store the data, how long it should be stored etc.
3. **Data Encryption**: Data encryption includes encryption methods that are going to be used to store and transmit the data.
4. **Access control:** It defines who all have the rights to access the data. In addition, it defines how long access should be given for a specific user on a specific resource.
5. **Risk Management:** Risk management policies include the risk assessment, and the organization strategy on a risk situation. In addition, who is in charge of such a situation?

Tools used for Cyber Security

In our present situation, we are hearing a lot of news about cyber-attacks and cyber-crimes. Our world is changing and almost all the transactions and our daily life depend on cyber space. It is very essential to protect the cyber space and IT environment for every organization and individual.

There are a huge number of threats are in cyber space that every organization must know to understand how much risk is associated with every step in this cyber world.

Viruses, Hackers, malware, Trojans, Worms, Scareware, Ransomwares, and a huge number of threats are there in cyber space so organizations irrespective of their size must know the methods and essential tools to protect themselves from such cyber-attacks.

Every organization now has a special team that can handle cyber-attacks and cyber criminals. In the present time, there are different tools that every organization should use to make itself protected.

Let us discuss the important General categories of cyber security tools

Firewalls

Firewalls are the basic and effective security measure, which acts as a wall of defense between the organization's internal network and the outside network. Firewalls filter each packet of data that is moving in and out of the organization's network and filter the malicious packets.
Firewalls can be implemented as software or as hardware depending on the need and importance of the data to be secured. Every packet of data has to pass through a firewall and be filtered. Nothing in the cyber world can assure 100 percent protection as the hackers can able to make data packets that act as genuine but malicious inside and it can overcome the firewall filtering. An overall firewall is the best defense that can be useful to protect from cyber criminals and cyber-attacks.

Antivirus program

This is the second most effective security system that every system needs to protect itself from attacks. An antivirus is a program that is developed for detecting and filtering all types of malicious programs that are running in a system without our knowledge.

Antivirus programs are effective in protecting our systems and network devices from many threats caused by viruses, Worms, Trojans, Spywares, Botnets, Adware, Ransomware, Keylogger, and many more.

Antivirus must be installed and it must be updated to make sure that it can handle all types of new and improved types threats. Each antivirus has a vault that contains the threats information and that must be up to date.

Public Key Infrastructure

Public key Infrastructure or PKI is a tool that is used for verifying the identity of the receiver and helps to send and receive the data securely. It helps to distribute and identify the public encrypting keys.

Normally PKI is associated with the SSL and TLS technology which helps to secure the information transfer between the sever and user using the HTTPS.

Uses of PKI

1. Enable the authentication and access control
2. Create digital signatures
3. Verify the sender identity and encrypt emails
4. Helps to protect the code by digitally sign

Penetration Testing

Penetration testing is the method of checking the security systems quality by identifying any of the security vulnerabilities are there in the system. Normally an Ethical hacker will do the job for the organization.

Ethical hackers try to penetrate the security system of the organization like a hacker to check if he can find any vulnerable points to enter into the security system. They are using the same methods and tricks an original hacker will do to penetrate into a cyber-security system.

If they succeed in penetration, the ethical hackers will make the solution to close that vulnerability by discussing with the cyber security team of the organization.

MDR

MDR stands for Managed Detection and Response Service. It is the most modern type of security system that can help in treating detection, threat intelligence, monitoring, threat analysis, and attack response with the help of Artificial Intelligence and machine learning.

In the latest times, the attackers are using the best tools and methods for hacking and other malicious activities. The need for the best defense also arises because of such cyber criminals. In addition, MDR is the answer for that.

MDR has the following characteristics

1. MDR is focused on threat detection.
2. MDR is highly dependent on the analytics and event management
3. It makes a combination of humans and artificial intelligence work

The other categories of cyber security tools include

- Network monitor tools
- Encryption Tools
- Web vulnerability scanning tools
- Defense Wireless tools
- Packet sniffers

Now let us check the latest tools that are used in cyber security inside the categories we discussed above.

MOST POPULAR AND COMMONLY USED TOOLS FOR CYBER SECURITY

To discuss all the tools used in cyber security is beyond our scope, so we are here discussing some important tools that we use for cyber security presently

Kali Linux

A Linux operating system provides a number of tools for scanning a network, auditing the security, and scanning for any malicious activity in the system. The most important advantage of the Kali Linux operating system is that it offers tools for all levels of cyber security experts.

It is easy to use kali operating system tools for even a beginner. It offers tools that are easily executable, monitor, and detect the network of the organization.

Cain and Abel

Cain and Abel are the cyber security tools that run on windows, which help to detect the password strength in the applications and machines that run on windows. It helps the security experts to find password security vulnerabilities. It is one of the free and old security tools used in the case of password recovery on windows.

Metasploit

Metasploit is a set of tools that are used in penetration testing. It is the best tool for ethical hackers to check and analyze the vulnerabilities of the security system and helps in improvement while doing penetration testing.

It can able to check even the upcoming vulnerabilities and detect the chance of being vulnerable in the future. It helps in analyzing the web products and servers too.

Wireshark

Wireshark is an open-source, a network security tool that is used for packet sniffing and auditing passwords. The Wireshark tool is used to monitor the network traffic and sniff the packets in real-time. It also helps to check the network protocols and increase security.

Security experts use this cyber security tool to analyze the traffic and to check the features of a packet by capturing the data packet from the network traffic.

John the Ripper

John the Ripper is a password strength check tool that helps to check weak passwords. It helps to analyze the complex encryption and ciphers for any presence of weak passwords. It works in almost all operating systems.

NIKTO

NIKTO is a cyber-security tool that is used for websites and web-related products, which can detect vulnerabilities and can able to make the steps to solve such vulnerabilities.
NIKTO has a huge database that contains all the details about 6400 threats and the cyber security experts are updating more and more vulnerabilities into the database so that it can identify new threats easily.

Forcepoint

Forcepoint is a cyber-security tool mainly for cloud users. It helps to block different types of intrusion attempts. It also helps to monitor the network traffic and detect any malicious activity in the traffic and make necessary actions to prevent them.

PAROS proxy

A web-based security tool is used to monitor real-time network activities. It also helps to analyze and detect web products vulnerabilities. PAROS proxy is a core java based cyber security tool.

NMAP

NMAP is also called Network Mapper. It can able to scan the network and identify any untrusted devices. Cyber security professionals are using NMAP for scanning a network for vulnerabilities and untrusted devices.

Truecrypt

Truecrypt as the name suggests, is one of the most commonly used and most popular cyber security tools for encryption. It can easily encrypt a part or even a full storage media and can make virtually encrypted disks.

Truecrypt is one of the best encryption tools that has been used for years without any change or update. It helps cyber security experts to make layered encrypted content.

TOR

TOR is a powerful cyber security tool that is been used for browsing and checking the network without anyone detects it. TOR is mainly used to protect the privacy of the users while accessing the web. It is efficient in protecting users from cyber security threats. We usually heard of TOR browsers related to deep and dark web access.

LifeLock

A security tool helps us to protect our data from stealing. Lifelock can able to lock our sensitive data with a single click. It helps to protect our home devices, can able to provide VPN services, Can easily lock the data from stealing, can able to scan and alert about the emails.

Bitdefender

Bitdefender is a popular antivirus program that can able to scan our systems and devices on request. It can able to protect our systems from various threats that include viruses, Worms, Trojans, Spywares, Adware, Keylogger, etc. Bitdefender can also provide security to our emails and online activities. It helps in providing VPN and secure banking while using the system.

Malwarebytes

As the name suggests, Malwarebytes is a cyber-security tool that provides security from malware, adware, ransomware, and websites which contain malicious activities.
Malwarebytes offers secure accessing the internet and can able to clean the infected devices and systems.

VIPRE

VIPRE is another cyber security tool that helps us to protect from spam emails and malware. It blocks such messages, emails, and websites so that helps to provide safe browsing.
VIPRE helps in removing all the traces of a file permanently and also monitors the network traffic. With the help of VIPRE, you can clean your browsing history and all the information.

SiteLock

Sitelock is a cyber-security tool that is been used by websites to protect themselves and their visitors from cyber-attacks. Sitelock offers services like malware detection and protection from SQL injection.

With Sitelock we can scan as many web pages as you need and it can monitor the blacklist of Google. Sitelock produce a weekly report on scanning and information.

Mimecast

Mimecast is a cyber-security tool that gives protection to emails services. It also helps to safeguard from the websites that contain malicious activity. Mimecast can able to detect all types of cyber-attacks easily and efficiently, block such attacks before it infects our systems and network.

Solar Winds Security Event manager

Solar winds security event manager is a cyber-security tool that helps to monitor and analyze the host traffic for any intrusions. It can able to monitoring, report, and take necessary action in real-time in case of intrusions and cyber-attacks.

It has a huge database and it will be always updated. Solar winds can be easily used in cloud systems too. It has incorporated a well-defined set of reporting tools.

There is a huge collection of cyber security tools available in the market, which comes under the categories we discussed above, and mentioning all of them is beyond the scope of this tutorial.

Common eCommerce Security Threats

Ecommerce is a very common name in our present life. We are using an e-commerce platform for various purposes in daily life. What is the definition of E-commerce? E-commerce can be defined as the activity that we conduct using the internet that involves commercial transactions. Also includes the activity of buying and selling through the internet and payments that we doing through the internet.

In our present situation, we cannot define all the situations in which we are using the E-commerce platform but some of them are mobile commerce, internet marketing, online transfers, online purchase, Electronic fund transfers, online selling, and many more.

How a threat is caused by E-commerce? It is the same as some criminals or people who are using the e-commerce platform for illegal and unfair activities like stealing of user sensitive information, Fraud, and security breaches. There are mainly three methods that a security breach happens in E-commerce that is,

1. Accidental
2. Purposeful
3. Human error

Electronic Payments System

Electronic payment system is the backbone of e-commerce, electronic fund transfer, and buying and selling through the internet. We already know the use of online stores like Amazon or Walmart, which helps to save our time and money with a huge number of selections.

With the online stores, customers can select different items from different sellers and it helps to get more quality items. Let us come to our point, all the transactions in E-commerce are done through payment systems.

It is a revolutionary concept that helps to make transactions without paper money. It helps to make our ecosystem better by conserving the trees, every government promotes e-payment.
With E payment system, business owners can reduce labor costs and transaction time, and efforts. It takes less time than traditional paper money. It also helps the customers not to carry an amount in their pockets but rather a credit or debit card.

While this concept is very good and has high potential, there are some risks associated with this electronic payment system. They are,

Probability of Frauds

Electronic payment systems have a huge risk of fraud transactions because of the authorization system. Mostly almost all the payment systems authorize a client to use a password and or a security question.

It does not give any other means to authorize the person on the other side is genuine or not. If any cyber-criminal gets a user's password and matches a security question, all the electronic payment security is compromised an attacker can easily steal the money using that payment system.

Difficulty in Tax collection

Every country has a tax system and each business owner should submit the truncations and business financial records to the tax department. In the Electronic payment system, they don't give a clear picture to the department about all the transactions which makes the tax collection complicated and frustrating.

Probability in Payment conflicts

We know that humans do not handle electronic payment systems, it is controlled and processed by machines, which is prone to errors when it is assigned to handle a huge amount of transactions in a short time. We have to be careful using such payment transactions when a huge amount of transactions is happening because it can result in conflicts.

E-cash

E-cash is the latest method of transaction using cash that is paperless, it is a virtual concept of cash that may be stored in an account or a card that can able to use for transactions and shopping. For example, Google pay, Paytm, PayPal, etc. E-cash is designed using four major components which are,

1. **Issuers**: The entity that creates the E-cash that may be a bank or non-bank institution.
2. **Customers**: The end users who are supposed to use the E-cash or their transactions
3. **Merchants or Traders**: These are the vendors who are ready to accept the E-cash transactions
4. **Regulators**: These are the state or country entities who are supposed to regulate the E-cash flow in the market.

E-cash is virtual cash that is stored on a computer or in the internet, which has the risk of being attacked by cybercriminals. Some of the main known types of attacks in E-cash system are,

1. **BACKDOOR THREATS**: it is a common type of attack in which the attacker can able to bypass all the security mechanisms and can access to the user account and able to do transactions.
2. **DENIAL OF SERVICE ATTACKS**: It is a popular attack is called a DOS attack where the attacker makes the network resources busy by sending junk requests thereby preventing the genuine users to do their transactions.
3. **DIRECT ACCESS ATTACKS**: It is a physical attack where the attackers use the computer of the user and install malware to steal their passwords and use such systems for transactions.
4. **EAVESDROPPING**: in this method, the attacker silently interferes in the network and overhears the communications that are happening in the network. Eavesdropping is a silent attack where the sender or receiver cannot able to detect the attacker's presence.

Credit or Debit card fraud

A credit card is a type of card that is issued by banks to the users in which the users can able to borrow money from the bank to doing a purchase. Every card has a limitation for the amount which varies according to the users. The payment that users borrow from the bank has to pay back at the specified time with some additional cost.

A debit card is also a card that is issued by banks, which can be used by the users for doing transactions. The difference is, using the debit card the users can access only the amount that is in their account.

Some of the major risks associated with the credit or debit cards are,

1. **ATM**: Automated teller Machines are the place we can take the money using our cards which is the favorite spot for attackers to access the sensitive information from our cards. Cybercriminals use many methods for accessing our card details and some of them are,
2. **SKIMMING**: It is a method that which the attackers attack a machine to the card reader that can able to get the details of the user card to attackers.
3. **UNWANTED PRESENCE**: In this method, the attacker tries to overlook through our shoulders to get the card details while we are accessing the ATM machine
4. **PHISHING**: It is the method that which an attacker gets sensitive information from the user by sending emails or messages.

Top challenges in cyber security

In the present world, technology is advancing very fast, Individuals, organizations and even the government are depending on the internet and cyberspace for different activities that range from viewing a video to making a bank transfer. It is very difficult for many organizations, individuals, and government to protect their sensitive information and assets from cyber-attacks. Cyber security is doing that job for them to protect their data from cybercriminals.

In the present situation, cyber security is playing one important role in safeguarding organizations and even a nation's economic and sensitive information and devices. Nowadays there are a huge number of challenges are happening related to cyber security as the attackers are more efficient and many readily available tools are available on the internet. Each organization needs a cyber-security analyst to make sure they are protected.

Cyber security challenges are in different forms and ways like Ransomware, Malware attacks, Phishing attacks, and many more that may even affect a country's economic conditions. In these cyber security tutorials, we are going to know about 10 top cyber security challenges.

1. Ransomware attacks
2. IoT attacks
3. Cloud attacks
4. Phishing attacks
5. Blockchain & cryptocurrency attacks
6. Software vulnerabilities
7. Machine learning and Artificial intelligence attacks
8. Insider attacks

Ransomware attacks

Ransomware attacks are one of the modern cyber-attacks that almost all organizations around the globe are facing. According to the data, around 60 to 70 percent of IT and related institutions are the victims of ransomware attacks.

Ransomware is a kind of malware that attacks a system and lock the system and its data. Hackers behind the ransomware will ask for a ransom and they release the lock only if they are paid. Some of the hackers never release the system even after the payment is made as they ask for more payments.

The infected system is locked and all the data inside the system cant be accessed until the payment is made. It makes a huge loss for IT companies and financial institutions if the data is lost. Ransomware attacks are increasing day by day

In the present condition, the DRaaS solution is the best strategy to secure ransomware. In this method, we should take a backup automatically at regular intervals and once the system is infected we have to restore the clean version of the backup and use the system.

IoT Attacks

IoT is the short form for the Internet of Things; It is the most modern revolution in the technology world, as it is a system of so many devices that are interconnected through the internet and works using the internet for data transfer. IoT devices are working with the help of a UID number and it can transfer data using that UID. The operating system and the software, which is used in the IoT devices, are susceptible to a cyber-attack making a window for attackers to access the sensitive information.

According to the latest data around 20 billion IoT devices are connected through the internet in 2022 and it is increasing at a high rate. Protecting these devices is challenging for a cyber-security team and it must be protected to safeguard the sensitive information inside these devices. Every organization must have a cyber-security team to make security for passwords, session handling, user verification, multi-factor authentication, etc.

Cloud Attacks

Cloud storage services are an upcoming trend in storage. Most individuals and organizations are using cloud services for storage and access. This upward trend in the usage of cloud storage and services makes cybercriminals focus on the cloud.

We all have heard about an attack on cloud storage called the I-cloud hack which exposed the photos of many celebrities and famous people. In the current scenario data stealing from the cloud is one of the big challenges in cyber security.

Once the cloud security is compromised, it will make a disaster like a huge amount of sensitive information are now in cloud storage. This can make organizations, even governments fall.

Phishing and Spear-Phishing Attacks

Phishing attacks are common attacks that cybercriminals use to gain information from the victims about their bank details, credit card details, and other sensitive information. In a phishing attack, the hackers will use websites or emails that may look legitimate but contain malicious code that will take your details to the hacker's database.

How phishing attacks are different from ransomware is both are taking the user's sensitive information but in phishing attacks, the hacker will not lock the victim's data but rather use that sensitive information for illegal activities like stealing money from their account, etc until the victim knows about it and take necessary countermeasures.

In the case of spear phishing, cybercriminals use emails and other messages targeted at specific victims. In this case, the hackers will study their victims and their interests and make the trap according to that like malicious emails or messages.

As millions of new users are using the bank's online services and the internet without proper knowledge and precautions, phishing attacks and spear-phishing attacks are becoming one of the main challenges in cyber security.

Blockchain and Cryptocurrency revolution

Blockchain is one of the latest technology revolutions that laid the building base of cryptocurrencies like Bitcoin, Etherium, etc. Blockchain technology is offering a digital medium for transactions without a third party that we call peer-to-peer transactions. As we know the blockchain is a global platform that makes the concept of Bitcoin which can make transactions without a third party like financial institutions.

It is difficult to predict the security of the blockchain. It is not clear what level of security this technology is offering. Different cyber security experts are predicting that it offers worthy security and it has passed the infancy stage but not cleared its advanced security stage.

Making this technology secure is one of the challenges of cyber security in these times as some DDOS attacks, Sybil, and Eclipse attacks are targeted such as blockchain and cryptocurrencies.

Machine Learning and AI revolution

Machine learning and Artificial intelligence are booming a lot. John McCarthy who is known as the father of AI stated that Artificial intelligence is a combination of science and engineering that make intelligent machines.

Machine learning and AI has huge application-level opportunities that include problem-solving, pattern recognition, take intelligent decisions, etc, even these technology is highly used in cyber security to analyze the threat from the huge amount of data and take the necessary steps.

Even the AI and ML are doing a great job, it is also vulnerable to cyber-attacks from professional-level cyber attackers. This technology is taking the decisions depending on the huge data set; any manipulation in the dataset will make dangerous decisions from the AI. So it is again a challenge for cyber security.

Software and Apps Vulnerabilities

We are all using software and apps for different activities in our systems and in mobile devices. Even if this software is perfect and secure, there must have some vulnerabilities inside it, which can make the hackers penetrate into, the software can steal the data.

Usually, organizations and individuals are not making their software up to date because of ignorance, and some use illegal versions. It may cause negative results as this software has patches and vulnerabilities and the developers remove such things in the update. So every software must be up to date.

Using software and apps without much concern is one of the challenges in cyber security at the current time.

Insider attacks

Till now we have discussed the challenges for cyber security professionals which are coming from external sources and he has to protect the organization from them. In some cases, the employees who have illegal interests will try to attack the organization from the inside. It will be leaking sensitive data or making some important machines nonfunctional.

This type of inside challenge also has to take care of by cyber security by using a firewall for monitoring both inside and outside traffic. Limiting the access to the employees to only their department and additional access will be allowed only if it is necessary.