

UNIT II

Cyber Crime issues and Cyber Attacks

Definition of cyber crime

- cyber crime can be defined as a crime or an unlawful act where the computer is used either as a tool, a target or both. In other terms, cyber crimes in India can be defined as an unauthorized access to some computer system without the permission of rightful owner or place of criminal activity and include everything from online cracking to denial of service attacks. Some examples of cyber crime include phishing, spoofing, DoS (Denial of Service) attack, credit card fraud, online transaction fraud, cyber defamation, child pornography, etc.

- Cyber criminals always choose an easy way to make big money. They target rich people or rich organizations like banks, casinos and financial firms where the transaction of a huge amount of money is made on an everyday basis and hack sensitive information. Catching such criminals is difficult. Hence, that increases the number of cyber-crimes. Computers are vulnerable, so laws are required to protect and safeguard them against cyber criminals

DIFFERENT KINDS OF CYBER CRIMES

2.1. Unauthorized Access to computer:

- Unauthorized access means any kind of access without the permission of either of the rightful or person in charge of the computer, computer system or computer network. Hacking means an illegal intrusion into a computer system and/or network.
- In simple words, hacking is an act committed by an intruder by accessing your computer system without your permission. Hackers (the people doing the 'hacking') are basically computer programmers, who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons.

2.2 Computer Intrusion

- Computer intrusion occur when someone tries to gain access to any part of your system.
- Computer intruders or hackers typically use autometed computer programs when they try to comprmise a computer security.
- These are several ways try to gain access to your computer.They Can:
 -

1. Access your computer to view ,change,delete information on your computer.
2. crash or slow down your computer
3. Access your private data by examining the files on your system:
4. Use your computer to access the other computer on the internet.

2.3 Computer virus and Malicious code

- 2.3.1 Malicious code
 - Malicious code is unauthorised files or programs which can cause damage to computer system data, programs and files. Various classification of malicious code include viruses, worms and Trojan horses.
1. Viruses – A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.

- 2. Worms – Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.

3. A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, and audio files.

2.3.2 What is a Computer Virus?

- A computer virus is a type of harmful program. When it runs, it makes copies of itself and adds its code to other programs and files on your computer. These viruses come in different types, and each type can affect your device differently. Simply put, a computer virus changes how your computer works and aims to spread to other computers. It does this by attaching itself to normal programs or documents that can run code, known as macros.

Common Signs of Computer Viruses

- Speed of system. A computer system running slower than usual is one of the most common signs that the device has a virus.
- Pop-up windows.
- Programs self-executing.
- Accounts being logged out.
- Crashing of the device.
- Mass emails being sent from your email account.
- Changes to your homepage.

Types of computer virus

1. Boot Sector Virus.
2. Direct Action Virus.
3. Overwrite virus.
4. Resident Virus.
5. Space filter Virus.
6. Polymorphic Virus.
7. File Infector Virus.
8. Multipartite Virus.
- 9. Macro virus.

1.Boot Sector Virus

- One of the easier viruses to avoid, this virus hides out in a file on a USB drive or email attachment. When activated, it can infect the system's master boot record to damage the system.

2.Direct Action

- This virus targets a specific file type, most commonly executable files (.exe), by replicating and infecting files. Due to its targeted nature, this virus type is one of the easier ones to detect and remove.

3. Resident Virus

- Resident viruses set up shop in your RAM and meddle with your system operations. They're so sneaky that they can even attach themselves to your anti-virus software files.

4. Multipartite Virus

- This virus infects the entire system – multipartite viruses spread by performing unauthorized actions on your operating system, folders, and programs.

5. Overwrite Virus

- As the name implies, overwrite viruses overwrite file content to infect entire folders, files, and programs.

6. Polymorphic Virus

- Spread through spam and infected websites, the polymorphic virus are file infectors which are complex and tough to detect.

File Infector

- By targeting executable files (.exe), file infector viruses slow down programs and damage system files when a user runs them.

8.space filler virus

- It is rare type of virus which fills in the empty spaces of a file with viruses. It is known as cavity virus.
- It will neither affect the size of the file nor can be detected easily.

9. Macro virus

A macro virus is a type of malicious software that hides within macros, which are small programs embedded in documents or spreadsheets.

Internet Hacking and Cracking

Q.1 Explain Internet Hacking and its types.

What is hacking

- Hacking is the activity of identifying weakness in a computer system or network to exploit the security to gain access to personal data or business data.
- An example of computer hacking can be :using a password cracking algorithm to gain access to computer system.

- System hacking means the exploitation of computers to commit fallacious acts like fraud, privacy invasion, stealing corporate/personal knowledge, etc.
- Cyber-crimes cost several organizations several bucks every year. Businesses are compelled to defend themselves against such attacks.

- System hacking means the exploitation of computers to commit fallacious acts like fraud, privacy invasion, stealing corporate/personal knowledge, etc.
- Cyber-crimes cost several organizations several bucks every year. Businesses are compelled to defend themselves against such attacks.

Type	Description
White Hat Hacking: (Ethical Hacking)	Authorized hacking to find and fix security flaws. Used in cybersecurity testing.
Black Hat Hacking:	Unauthorized and illegal hacking to steal, damage, or disrupt systems.
Grey Hat Hacking:	Unethical but not harmful; often done without permission but not with malicious intent.

Types of Hacking



Types Of hacking

1. Phishing –

In this type of hacking, the hacker intends to steal critical information of users like account passwords, MasterCard details, etc. For example, hackers can replicate an original website for user interaction and can steal critical information from the duplicate website the hacker has created.

Sending fake emails or websites to steal login details.

2.Virus –

- These are triggered by the hacker entering the filters of the website once they enter the website filters it. The purpose is to corrupt the information or resources on the net website.
-

3. UI redress –

In this technique, the hacker creates a pretend interface and once the user clicks with the intent of progressing to a particular website, they are directed to a special website.

4. Cookie theft –

Hackers access the net websites exploiting malicious codes and stealing cookies that contain tips, login passwords, etc. Get access to your account then will do any factor besides your account.

5. Distributed Denial-of-service(DDoS) –

This hacking technique is aimed at taking down a website so that a user cannot access it or deliver their service. Gets the server down and stops it from responding, which may cause a condition error constantly.

6. DNS Spoofing –

This essentially uses the cache knowledge of an internet website or domain that the user might have forgotten to keep up to date. It then directs the data to a distinct malicious website.

7.Social Engineering –

Social engineering is an attempt to manipulate you to share personal info, sometimes by impersonating a trustworthy supply.

8. Missing Security Patches –

- Security tools will become outdated as a result of the hacking landscape advancement and need frequent updates to protect against new threats.

- Malware-Injection Devices –
- Cyber-criminals will use hardware to sneak malware onto your pc. You would have detected infected USB sticks which can allow hackers remote access to your device when it is connected to your pc.
-

- Cracking Password –

Hackers will get your credentials through a technique known as keylogging.

What is Cracking?

Cracking is a subset of hacking that focuses on breaking into software or systems, often by removing protections or security features..

Types of Cracking

- Password Cracking
- Software cracking
- Network cracking

1. Password Cracking

- Password cracking refers for Finding password from stored data. This is the most typical techniques for password cracking.
- Brute force cracking: Until it finds a match the cracking algorithm outputs random sequences of characters.
- Dictionary cracking: This is similar to brute-force cracking dictionary tracking restrict itself to words rather than utilising random letters.
- Rainbow table cracking : It is used to determine the encryption used to hash a password, a rainbow table leverages previously computed hashed values.

Software Cracking

- Software cracking is the process of modifying software to completely or partially eliminate one or more of its functions. At least one of the following tools or methods is used in the majority of software cracking.

- Keygen: A keygen, which stands for “key generator,” is a programme that a cracker creates to produce legitimate serial numbers for software products.
- Patch: Patches are compact pieces of code that alter already-running applications. Every day, software fixes are released by developers. They can also be created by crackers, and when they do, the patch’s task is to change the way the software functions by eliminating the undesirable characteristics.
- Loader: The function of a loader is to prevent the software’s security features from being activated. While some loaders are used to get around copy controls, others are used by players who want to cheat in online multiplayer games.

Network Cracking

- Network cracking is when a LAN, or “local area network,” is breached by an outsider. A wireless network can be cracked considerably more easily than a cable one since the cracker only has to be in close proximity to the wireless signal. The Wi-fi system in your house is a typical illustration of a wireless LAN. Cracking a wired network requires a direct connection, but cracking a wireless network is much more convenient, because the cracker just needs to be close to the wireless signal.

Virus and worms

- 1. Worms :
- Worms are similar to a virus but it does not modify the program. It replicates itself more and more to cause slow down the computer system. Worms can be controlled by remote. The main objective of worms is to eat the system resources. The WannaCry ransomware worm in 2017 exploits the Windows Server Message Block (SMBv1) which is a resource-sharing protocol.

- 2. Virus : A virus is a malicious executable code attached to another executable file that can be harmless or can modify or delete data. When the computer program runs attached with a virus it performs some action such as deleting a file from the computer system. Viruses can't be controlled by remote. The ILOVEYOU virus spreads through email attachments.

Difference between Worms and Virus :

Difference between Worms and Virus

1. Definition:

WORMS:

A Worm is a form of malware that replicates itself and can spread to different computers via Network.

- VIRUS:

A Virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data.

2.Objective

- WORMS

The main objective of worms is to eat the system resources. It consumes system resources such as memory and bandwidth and made the system slow in speed to such an extent that it stops responding.

- VIRUS

The main objective of viruses is to modify the information.

3. Host

- WORMS

It doesn't need a host to replicate from one computer to another.

- VIRUS

It requires a host is needed for spreading.

- 4.Harmful

WORMS

- It is less harmful as compared.

VIRUS

It is more harmful.

5.Detection and Protection

WORMS

Worms can be detected and removed by the Antivirus and firewall.

VIRUS

- Antivirus software is used for protection against viruses.

6. Controlled by WORMS :

- Worms can be controlled by remote.

VIRUS:

- Viruses can't be controlled by remote.

7. Execution

WORMS

Worms are executed via weaknesses in the system.

Virus

Viruses are executed via executable files.

8.Symptoms

Worms

- 1.Hampering computer performance by slowing down it
- 2Automatic opening and running of programs
- 3.Sending of emails without your knowledge

- Virus:
 1. Pop-up windows linking to malicious websites
 2. Hampering computer performance by slowing down it
 3. After booting, starting of unknown programs.

Software Piracy

- Software piracy is the unauthorized use, copying or distribution of copyrighted software. It may take many forms, including:
Unauthorized copying of software programs purchased legitimately, sometimes known as "end-user" piracy.

Software piracy is the unauthorized copying, distribution, or use of copyrighted software. It encompasses various illegal activities, including making unauthorized copies, distributing software without permission, or using software beyond the scope of the license. This illegal practice harms software developers and can expose users to security risks and other issues.

intellectual property rights

- Intellectual property (IP) pertains to any original creation of the human intellect such as artistic, literary, technical, or scientific creation. Intellectual property rights (IPR) refers to the legal rights given to the inventor or creator to protect his invention or creation for a certain period of time.

- A mail bomb is a form of a denial-of-service (DoS) attack designed to overwhelm an inbox or inhibit a server by sending a massive number of emails to a specific person or system. The aim is to fill up the recipient's disk space on the server or overload a server to stop it from functioning.

What is a mail bomb?

- Also known as email bombs and letter bombs, mail bombs inconvenience not only the intended target but everyone who uses the server. When a server is unresponsive, it can degrade network performance and potentially lead to downtime.

What Is an Exploit?

- An exploit is a program, or piece of code, designed to find and take advantage of a security flaw or vulnerability in an application or computer system, typically for malicious purposes such as installing malware. An exploit is not malware itself, but rather it is a method used by cybercriminals to deliver malware.

Stalking and Obscenity in Internet,

- In Cyber Stalking, a cyber criminal uses the internet to threaten somebody consistently. This crime is often done through email, social media, and other online mediums. Cyber Stalking can even occur in conjunction with the additional ancient type of stalking, wherever the bad person harasses the victim offline. There's no unified legal approach to cyber Stalking, however, several governments have moved toward creating these practices punishable by law. Social media, blogs, image-sharing sites, and lots of different ordinarily used online sharing activities offer cyber Stalkers a wealth of data that helps them arrange their harassment.

What is Cyberstalking?

- Cyberstalking is the use of the internet or digital tools to repeatedly harass, threaten, or stalk someone. It includes sending unwanted messages, hacking accounts, or spreading lies online. The goal is often to scare or distress the victim. Cyberstalkers often use social media, email, or other online platforms. Cyberstalking involves using digital platforms to intimidate or control someone by continuously monitoring or harassing them online, they can track the victim's online activity.

Some of the Examples of Cyberstalking are as follows

- Repeated Unwanted Messages
- False Profiles
- Tracking Online Activity
- Hacking Accounts
- Posting Private Information
- Threatening Comments
- Monitoring via GPS or Spyware

Types of Cyber Stalking

1. Webcam Hijacking: Internet stalkers would attempt to trick you into downloading and putting in a malware-infected file that may grant them access to your webcam. the method is therefore sneaky in that it's probably you wouldn't suspect anything strange.
2. Observing location check-ins on social media: In case you're adding location check-ins to your Facebook posts, you're making it overly simple for an internet stalker to follow you by just looking through your social media profiles.

3.Catfishing: Catfishing happens via social media sites, for example, Facebook, when internet stalkers make counterfeit user-profiles and approach their victims as a companion of a companions.

4. Visiting virtually via Google Maps Street View: If a stalker discovers the victim's address, then it is not hard to find the area, neighbourhood, and surroundings by using Street View. Tech-savvy stalkers don't need that too.
5. Installing Stalkerware: One more method which is increasing its popularity is the use of Stalkerware. It is a kind of software or spyware which keeps track of the location, enable access to text and browsing history, make an audio recording, etc. And an important thing is that it runs in the background without any knowledge to the victim.

6.Looking at geotags to track location: Mostly digital pictures contain geotags which is having information like the time and location of the picture when shot in the form of metadata. Geotags comes in the EXIF format embedded into an image and is readable with the help of special apps. In this way, the stalker keeps an eye on the victim and gets the information about their whereabouts.

How to Help Protect Yourself Against Cyberstalking

1. Develop the habit of logging out of the PC when not in use.
2. Remove any future events you're close to attending from the social networks if they're recorded on online approaching events and calendars.
3. Set strong and distinctive passwords for your online accounts.

4. Cyber Stalkers can exploit the low security of public Wi-Fi networks to snoop on your online activity. Therefore, avoid sending personal emails or sharing your sensitive info when connected to an unsecured public Wi-Fi.
5. Make use of the privacy settings provided by the social networking sites and keep all info restricted to the nearest of friends.
6. Do a daily search on the internet to search out what information is accessible regarding you for the public to check.

Cybercrime prevention methods

- In day-to-day life, everyone is leading their life with technology. Our daily life depends on technology. So, nowadays everybody knows the internet and is aware of it. The Internet has everything that a man needs in terms of data. So, people are becoming addicted to the Internet. The percentage of the population using the internet are increasing day-by-day. National security is in some way getting dependent on the internet. But the new technologies which have arrived also brought unusual threats and Cyber-Crime is one such concept. Cyber-Crime is a crime that uses a computer for an attack like hacking, spamming, etc.

- To earn a huge amount of money, Cyber-criminals always choose an easy way. Banks, casinos, companies, and, financial firms are the prosperous organizations and their target centers where an enormous amount of money runs daily and has diplomatic information. It's very difficult to catch those criminals. Hence, the number of cyber-crimes are increasing day-by-day across the globe. We require so many laws to protect and safeguard them against cyber-criminals since the devices we use everyday for businesses and communication might have vulnerabilities that can be exploited

How to prevent Cyber-Crime?

- To prevent cyber-crime successfully, set up multidimensional public-private collaborations between law enforcement organizations, the information technology industry, information security organizations, internet companies, and financial institutions. A far apart from the real world, Cyber-criminals do not combat one another for predominance or authority. Rather, they do their tasks together to enhance their abilities and even can help out each other with new opportunities. Therefore, the regular ways of fighting the crime cannot be used against these cyber-criminals

There are some ways to prevent cyber-crimes are explained below:

1. By Using Strong Passwords: Maintaining different password and username combinations for each of the accounts and withstand the desire to write them down. Weak passwords can be easily broken. The following password combinations can make password more prone to hacking:

Using keyboard patterns for passwords. e.g. – wrtdghu

Using very easy combinations. e.g. – sana1999, jan2000

Using Default passwords. e.g. – Hello123, Madhu123

Keeping the password the same as the username. e.g. –
Madhu_Madhu

2. Keep social media private: Be sure that your social networking profiles (Facebook, Twitter, YouTube, etc.) are set to be private. Once be sure to check your security settings. Be careful with the information that you post online. Once if you put something on the Internet and it is there forever.
3. Protect your storage data: Protect your data by using encryption for your important diplomatic files such as related to financial and taxes.

4. Protecting your identity online: We have to be very alert when we are providing personal information online. You must be cautious when giving out personal ids such as your name, address, phone number, and financial information on the Internet. Be sure to make that websites are secure when you are making online purchases, etc. This includes allowing your privacy settings when you are using social networking sites.
5. Keep changing passwords frequently: When it comes to password, don't stick to one password. You can change your password frequently so that it may be difficult for the hackers to access the password and the stored data.

6. Call the right person for help: Try not to be nervous if you are a victim. If you come across illegal online content such as child exploitation or if you think it's a cyber-crime or identity theft or a commercial scam, just like any other crime report this to your local police. There are so many websites to get help on cyber-crime.
7. Protect your computer with security software: There are many types of security software that are necessary for basic online security. Security software includes firewall and antivirus software. A firewall is normally your computer's first line of security. It controls that who, what and where is the communication is going on the internet. So, it's better to install security software which is from trusted sources to protect your computer.

Application security (Database, E-mail, and Internet)

Data Security Consideration

- Data security is the protection of programs and data in computers and communication systems against unauthorized access, modification, destruction, disclosure or transfer whether accidental or intentional by building physical arrangements and software checks. It refers to the right of individuals or organizations to deny or restrict the collection and use of information about unauthorized access. Data security requires system managers to reduce unauthorized access to the systems by building physical arrangements and software checks.

- Data security uses various methods to make sure that the data is correct, original, kept confidentially and is safe. It includes-
- Ensuring the integrity of data.
- Ensuring the privacy of the data.
- Prevent the loss or destruction of data.

- Data security consideration involves the protection of data against unauthorized access, modification, destruction, loss, disclosure or transfer whether accidental or intentional. Some of the important data security consideration are described below:

Backups

- Data backup refers to save additional copies of our data in separate physical or cloud locations from data files in storage. It is essential for us to keep secure, store, and backup our data on a regular basis. Securing of the data will help us to prevent from-
 - Accidental or malicious damage/modification to data.
 - Theft of valuable information.
 - Breach of confidentiality agreements and privacy laws.
 - Premature release of data which can avoid intellectual properties claims.
 - Release before data have been checked for authenticity and accuracy.

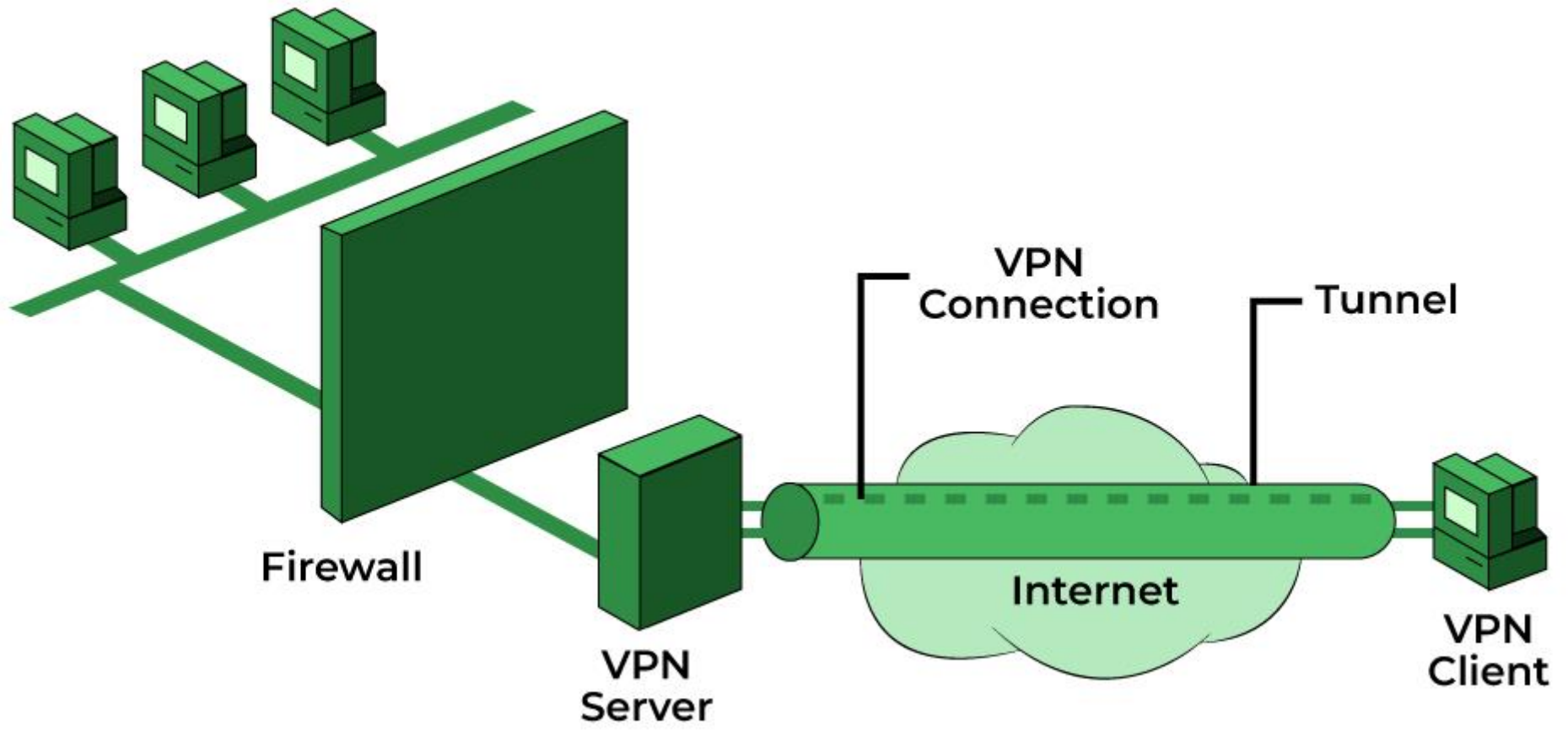
- Keeping reliable and regular backups of our data protects against the risk of damage or loss due to power failure, hardware failure, software or media faults, viruses or hacking, or even human errors.
- To use the Backup 3-2-1 Rule is very popular. This rule includes:
 - Three copies of our data
 - Two different formats, i.e., hard drive+tape backup or DVD (short term)+flash drive
 - One off-site backup, i.e., have two physical backups and one in the cloud

- Some important backup options are as follows-
- Hard drives - personal or work computer
- Departmental or institution server
- External hard drives
- Tape backups
- Discipline-specific repositories
- University Archives
- Cloud storage

- Some of the top considerations for implementing secure backup and recovery are-
- Authentication of the users and backup clients to the backup server.
- Role-based access control lists for all backup and recovery operations.
- Data encryption options for both transmission and the storage.
- Flexibility in choosing encryption and authentication algorithms.
- Backup of a remote client to the centralized location behind firewalls.
- Backup and recovery of a client running Security-Enhanced Linux (SELinux).
- Using best practices to write secure software.

Security Technology-Firewall and VPNs

- Nowadays, technology plays a vital role in our day-to-day life activities Which promotes the World to bring new innovation in the field of modernization, and globalization. Although we know that technology has improved people's life but it also has demerits which include Plagiarism, Digital fraud, Phishing, Pharming, etc. To protect a network we can use VPN or firewall.



VPN:

- A VPN (a virtual private network), changes your network address(IP) by conducting your computer address through a remote server into another location or shielding you from getting your private data leaked. This makes it a secure choice for companies whose employees work from home or a remote location. To read more about VPNs please refer to the article Virtual Private Network (VPN).

Firewall:

- Nowadays, Increased use of Internet-related activities in day-to-day activities has shown us that it also has its demerits. So, In order to protect us, we came up with the term known as Firewall. To read more about firewalls you can refer to the article [Introduction of Firewall](#).
- A firewall is a very well-known solution for all these activities. Its main objective is to obstruct the legitimate-looking site which tends to acquire the user's personal information. It plays a salient role in protecting users' digital data by creating a layer of protective walls.

Relation between VPN and Firewall:

- By using a firewall, you can access the Internet effectively, but unknown site penetration access is blocked by the firewall. By using the VPN service, remote access and networks are encrypted. The Following relation between VPN and Firewall is listed below.
- Firewalls prevent cyber attacks by building a strong protective wall to protect user's confidential data. On the other hand VPN keep your location unknown to others by creating a proxy network for secure connection.
- VPN allows you to access the restricted sites with a secure connection, while firewall can only create a layer of restrictions that you have accessed.
- Firewalls use your choice to block access to certain sites. While using a VPN, one can access the same site over a long period of time.
- Firewalls focus on blocking websites. While VPN, Focuses on a private connection.

Hardware Protection and Type of Hardware Protection

- In this article, we are going to learn about hardware protection and its types. So first, let's take a look at the type of hardware which is used in a computer system. We know that a computer system consists of hardware components like processor, monitor, RAM and many more. The important thing is, that the operating system ensures that these devices are not directly accessible by the user.
- Basically, hardware protection is divided into 3 categories: CPU protection, Memory Protection, and I/O protection. These are explained as follows:

- 1. CPU Protection:
- CPU protection ensures that, a process does not monopolize the CPU indefinitely, as it would prevent other processes from being executed. Each process should get a limited time, so that every process gets time to execute its instructions. To address this, a timer is used to limit the amount of time, which a process can occupy from the CPU. After the timer expires, a signal is sent to the process for relinquishing the CPU. Hence one process cannot hold the CPU forever.

- 2. Memory Protection:
- In memory protection, we are talking about that situation when two or more processes are in memory and one process may access the other process memory. To prevent this situation we use two registers which are known as:
 - 1. Base register
 - 2. Limit register
- So basically Base register store the starting address of program and limit register store the size of the process. This is done to ensure that whenever a process wants to access the memory, the OS can check that – Is the memory area which the process wants to access is privileged to be accessed by that process or not.

-

- 3. I/O Protection:
- With I/O protection, an OS ensures that following can be never done by a processes:
- Termination I/O of other process – This means one process should not be able to terminate I/O operation of othe processes.
- View I/O of other process – One process should not be able to access the data being read/written by other processes from/to the Disk(s).
- Giving priority to a particular process I/O – No process must be able to priorotize itself or other processes which are doing I/O operations, over other processes.

Operating System Security

- Protection refers to a mechanism that controls the access of programs, processes, or users to the resources defined by a computer system. We can take protection as a helper to multiprogramming operating systems so that many users might safely share a common logical namespace such as a directory or files.

- Security can be attacked in the following ways:

- Authorization
- Browsing
- Trap doors
- Invalid Parameters
- Line Tapping
- Electronic Data Capture
- Lost Line
- Improper Access Controls
- Waste Recovery
- Rogue Software