Unit-4:

4.1 Concepts of Cyber Security:

Cyber security is the protection to defend internet-connected devices and services from malicious attacks by hackers, spammers, and cybercriminals.
Or
Cyber security is a discipline that covers how to defend devices and services from electronic attacks by nefarious actors such as hackers, spammers, and cybercriminals.

cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes and Cyber security has been used as a catch-all term in the media to describe the process of protection against every form of cybercrime, from identity theft to international digital weapons.

4.1.1 Types of Threats

- Cyber terrorism. This threat is a politically-based attack on computers and information technology to cause harm and create widespread social disruption.
- Malware. This threat encompasses ransomware, spyware, viruses, and worms. It can install harmful software, block access to your computer resources, disrupt the system, or covertly transmit information from your data storage.
- Trojans. Like the legendary Trojan Horse of mythology, this attack tricks users into thinking they're opening a harmless file. Instead, once the trojan is in place, it attacks the system, typically establishing a backdoor that allows access to cybercriminals.
- Botnets. This especially hideous attack involves large-scale cyber attacks conducted by remotely controlled malware-infected devices. Think of it as a string of computers under the control of one coordinating cybercriminal. What's worse, compromised computers become part of the botnet system.

- Adware. This threat is a form of malware. It's often called advertisement-supported software. The adware virus is a potentially unwanted program (PUP) installed without your permission and automatically generates unwanted online advertisements.
- SQL injection. A Structured Query Language attack inserts malicious code into a SQL-using server.
- Phishing. Hackers use false communications, especially e-mail, to fool the recipient into opening it and following instructions that typically ask for personal information. Some phishing attacks also install malware.
- Man-in-the-middle attack. MITM attacks involve hackers inserting themselves into a two-person online transaction. Once in, the hackers can filter and steal desired data. MITM attacks often happen on unsecured public Wi-Fi networks.
- Denial of Service. DoS is a cyber attack that floods a network or computer with an overwhelming amount of "handshake" processes, effectively overloading the system and making it incapable of responding to user requests.

4.1.2 Advantages of Cyber Security

Without solid cyber security defenses, it would be easy to destroy modern-day essentials like the power grids and water treatment facilities that keep the world running smoothly.
Simply put, cyber security is critically important because it helps to preserve the lifestyles we have come to know and enjoy.

CIA Triad

The security of any organization starts with three principles: Confidentiality, Integrity, Availability. This is called as CIA, which has served as the industry standard for computer security since the time of first mainframes.

Fig: CIA triad

- Confidentiality: The principles of confidentiality assert that only authorized parties can access sensitive information and functions. Example: military secrets.
- Integrity: The principles of integrity assert that only authorized people and means can alter, add, or remove sensitive information and functions. Example: a user entering incorrect data into the database.

- Availability: The principles of availability assert that systems, functions, and data must be available on-demand according to agreed-upon parameters based on levels of service.

Ref: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security

4.2 Basic Terminologies:

4.2.1 IP Address, MAC Address

What is a MAC Address?

The term MAC address is an acronym for Media Access Control Address. The MAC Address refers to a unique identifier that gets assigned to a Network Interface Card/ Controller (NIC). It has a 64-bit or 48-bit address linked and connected to the concerned network adapter. The MAC Address can exist in a hexadecimal format. This type of address exists in six separate sets of two characters/ digits – separated from each other using colons.

What is an IP Address?

The term IP Address is an acronym for Internet Protocol Address. An IP Address refers to the address that assists a user in identifying a network connection. It also goes by the Logical Address name provided to individual connections in the present network. An IP address lets us understand and control the way in which various devices communicate on the Internet. It also defines the specific behavior of various Internet routers.

Difference Between MAC Address and IP Address

Parameters	**MAC Address**	**IP Address**
Full-Form	The term MAC address is an acronym for Media Access Control Address.	The term IP Address is an acronym for Internet Protocol Address.
Number of Bytes	It is a hexadecimal address of six bytes.	This address is either an eight-byte or a six-byte one.
Protocol Used for Retrieval	You can retrieve a device attached to the MAC address using the ARP protocol.	You can retrieve a device attached to the IP address using the RARP protocol.
Provider	The Manufacturer of NIC Cards provides a device with its MAC address.	An ISO (Internet Service Provider) provides a device's IP address.
Use	The primary use of a MAC address is to ensure the physical address of a given device/ computer.	The IP address, on the other hand, defines a computer's logical address.
Operation	The MAC address primarily operates	The IP address primarily

	on the data link layer.	operates on the network layer.
Alteration and Changes	This address does not alter or change with the passing time and change of environment.	This address gets modified depending on the change in environment and time.
Third-Party Access	Any third party can find out a device's MAC address.	The IP address stays hidden from display in front of any third party.

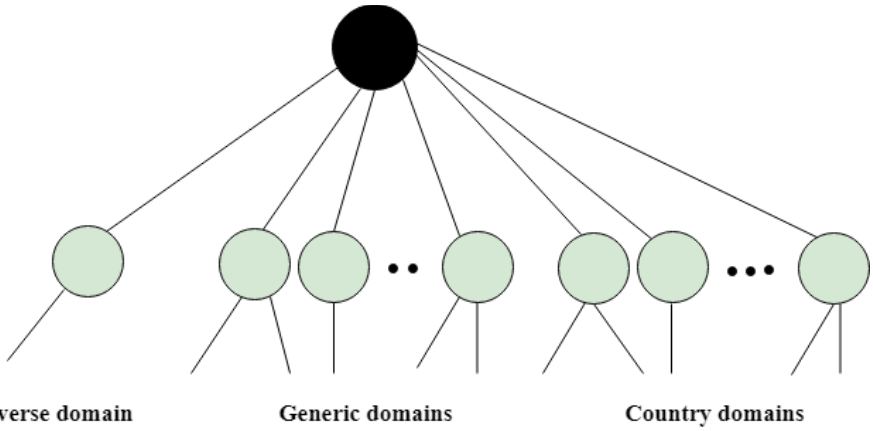
Ref: https://byjus.com/gate/difference-between-mac-address-and-ip-address

4.2.2 Domain name Server(DNS)

(Although many people think "DNS" stands for "Domain Name Server," it really stands for "Domain Name System.") DNS is a protocol within the set of standards for how computers exchange data on the internet and on many private networks, known as the TCP/IP protocol suite. Its purpose is vital, as it helps convert easy-to-understand domain names like "howstuffworks.com" into an Internet Protocol (IP) address, such as 70.42.251.42 that computers use to identify each other on the network. It is, in short, a system of matching names with numbers.

DNS

- An application layer protocol defines how the application processes running on different systems, pass the messages to each other.
- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.
- DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.



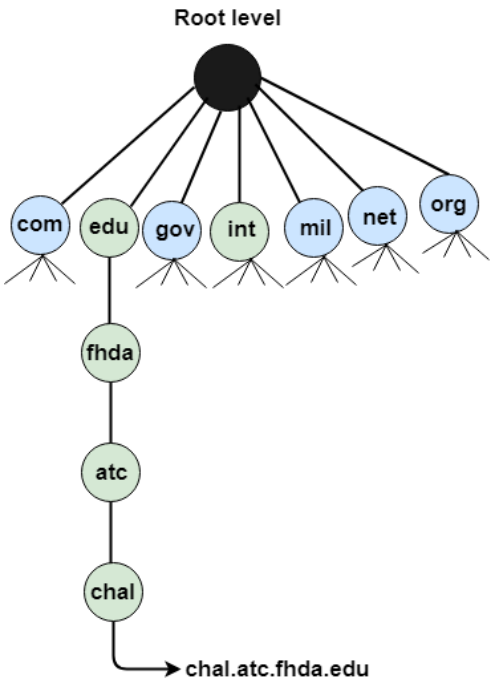
Generic Domains

It defines the registered hosts according to their generic behavior.

Each node in a tree defines the domain name, which is an index to the DNS database.

It uses three-character labels, and these labels describe the organization type.

Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms
com	Commercial Organizations
coop	Cooperative business Organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International Organizations
mil	Military groups
museum	Museum & other nonprofit organizations
name	Personal names
net	Network Support centers
org	Nonprofit Organizations
pro	Professional individual Organizations



Country Domain

The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

Inverse Domain

The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

Working of DNS

DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.

Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.

DNS implements a distributed database to store the name of all the hosts available on the internet.

If a client like a web browser sends a request containing a hostname, then a piece of software such as DNS resolver sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

Ref: https://www.javatpoint.com/computer-network-dnsand https://computer.howstuffworks.com/dns.htm

4.2.3 DHCP, Router, Bots

DHCP:
Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF) standard based on Bootstrap Protocol (BOOTP), a protocol with which DHCP shares many implementation details. DHCP allows hosts to obtain required TCP/IP configuration information from a DHCP server.

Why use DHCP?
Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources. **Without DHCP, IP addresses for new computers or computers that are moved from one subnet to another must be configured manually**; IP addresses for computers that are removed from the network must be manually reclaimed.

With DHCP, this entire process is automated and managed centrally. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.
The network administrator establishes DHCP servers that maintain TCP/IP configuration information and provide address configuration to DHCP-enabled clients in the form of a lease offer. **The DHCP server stores the configuration information in a database**

Benefits of DHCP

- Reliable IP address configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.
- Reduced network administration. DHCP includes the following features to reduce network administration:
- Centralized and automated TCP/IP configuration.
- The ability to define TCP/IP configurations from a central location.
- The ability to assign a full range of additional TCP/IP configuration values by means of DHCP options.
- The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable devices that move to different locations on a wireless network.
- The forwarding of initial DHCP messages by using a DHCP relay agent, which eliminates the need for a DHCP server on every subnet.

Routers:
• A device that forwards data packets (units of info) from one network to another.
• Based on routing tables (lists of addresses, permissions etc) and routing protocols, routers read the network address in each transmission and make a decision on how to send it based on the most expedient route (determined by traffic load, line costs, speed, bad lines)
• Routers are used to segment networks to balance and filter traffic for security purposes and policy management

• They are also used at the edge of the n/w to connect remote offices
• Router can only route a message that is transmitted by a routable protocol (e.g. Internet Protocol)
• Routers have to inspect n/w address in the protocol, so they process data and thus add overhead.
• Most routers are specialized computers that are optimized for communications
• Router functions can also be implemented by adding routing software to file server. (e.g. Windows 2000 include routing software)
• The operating system can route from one n/w to another, if each is connected to its own n/w adapter (or NIC), in the server.

Bots:
An autonomous program on the internet or another network that can interact with systems or users.

or

A 'bot' – short for robot – is a software program that performs automated, repetitive, pre-defined tasks. Bots typically imitate or replace human user behavior. Because they are automated, they operate much faster than human users. They carry out useful functions, such as customer service or indexing search engines, but they can also come in the form of malware – used to gain total control over a computer.
Internet bots can also be referred to as spiders, crawlers, or web bots.

Bots can be:

Chatbots
Bots that simulate human conversation by responding to certain phrases with programmed responses.

Social bots
Bots which operate on social media platforms, and are used to automatically generate messages, advocate ideas, act as a follower of users, and as fake accounts to gain followers themselves. As social networks become more sophisticated, it is becoming harder for social bots to create fake accounts. It is difficult to identify social bots because they can exhibit similar behavior to real users.

Shop bots
Bots that shop around online to find the best price for products a user is looking for. Some bots can observe a user's patterns in navigating a website and then customize that site for the user.

Spider bots or web crawlers
Bots that scan content on webpages all over the internet to help Google and other search engines understand how best to answer users' search queries. Spiders download HTML and other resources, such as CSS, JavaScript, and images, and use them to process site content.

Malicious bots /Web scraping crawlers
Bots that scrape content, spread spam content, or carry out credential stuffing attacks

Bots that read data from websites with the objective of saving them offline and enabling their reuse. This may take the form of scraping the entire content of web pages or scraping web content to obtain specific data points, such as names and prices of products on e-commerce websites.
In some cases, scraping is legitimate and may be allowed by website owners. In other instances, bot operators may be violating website terms of use or stealing sensitive or copyrighted material.

Knowbots
Bots that collect knowledge for users by automatically visiting websites to retrieve information which fulfils certain criteria.

Monitoring bots
Bots used to monitor the health of a website or system. Downdetector.com is an example of an independent site that provides real-time status information, including outages, of websites and other kinds of services.

Transactional bots
Bots used to complete transactions on behalf of humans. For example, transactional bots allow customers to make a transaction within the context of a conversation.

Download bots
Bots that are used to automatically download software or mobile apps. They can be used to manipulate download statistics – for example, to gain more downloads on popular app stores and help new apps appear at the top of the charts.
They can also be used to attack download sites, creating fake downloads as part of a Denial of Service (DoS) attack.

Ticketing bots
Bots which automatically purchase tickets to popular events, with the aim of reselling those tickets for a profit. This activity is illegal in many countries, and even when not against the law, it can be a nuisance to event organizers, legitimate ticket sellers, and consumers. Ticketing bots are often sophisticated, emulating the same behaviors as human ticket buyers.

Why do cybercriminals use bots?
1. To steal financial and personal information
2. To attack legitimate web services
3. To extort money from victims
4. To make money from zombie and botnet systems

4.3 Common Types of Attacks:
A cyberattack is a malicious attempt by an organization or individual to breach a network containing sensitive data of individuals or organizations. Attackers use a variety of different methods to exploit their victims' networks. Here are some of the most common types of cyber attacks:

- Brute force attack
- Advanced persistent threat (APT)

- Ransomware
- Denial-of-service (DoS) and distributed denial-of-service (DDoS)
- Phishing
- Credential stuffing
- Man-in-the-middle attack
- SQL injection
- Cross-site scripting (XSS)

4.3.1 Distributed Denial of Service

A DoS attack is an attack that makes computer systems inaccessible to their legitimate users by flooding the target site with multiple requests that trigger a crash. DDoS attacks are similar, but instead of using one device, multiple connected devices are used to attack the target site.

4.3.2 Man in the Middle, Email Attack

Man in the middle:

Just as the name suggests, the man-in-the-middle is like an eavesdropper between two sessions where the communication between two parties is monitored and intercepted. The goal of such an attack is to steal financial or login information of users.

To help prevent man-in-the-middle attacks:

Enable encryption on your router. If your modem and router can be accessed by anyone off the street, they can use "sniffer" technology to see the information that is passed through it.
Use strong credentials and two-factor authentication. Many router credentials are never changed from the default username and password. If a hacker gets access to your router administration, they can redirect all your traffic to their hacked servers.
Use a VPN. A secure virtual private network (VPN) will help prevent man-in-the-middle attacks by ensuring that all the servers you send data to are trusted.

Email attack:

This is one popular example of an email cyberattack, which has just used email as an attack vector to steal the user's credentials and other sensitive or personal data so it can be leveraged for malicious intent.

Types of Email Attacks

1. **Phishing**
   Phishing is a type of deception. Cybercriminals utilize email, instant messaging, and other social media to impersonate a trusted individual to obtain information such as login credentials.When an evil entity sends a false email that appears to be from a legitimate, trustworthy source, it is known as phishing. The goal of the message is to deceive the receiver into downloading malware or disclosing personal or financial information. Spear phishing is a form of phishing attack that is very specific in its approach. While phishing and spear-phishing use emails to contact their victims, spear-phishing delivers personalized emails to a single individual. Before sending the email, the criminal researches the target's interests.
2. **Vishing**

It is a type of phishing that employs voice communication technologies. Using voice-over IP technologies, criminals can fake calls from legitimate sources. Victims may also get a recorded message that purports to be from an official source. Criminals are attempt to steal the victim's identity by obtaining credit card numbers or other personal information. Vishing takes advantage of people's faith in the telephone system.

3. **Smishing**
   It is a sort of phishing that uses mobile phones to send text messages. To earn the victim's trust, criminals imitate a legitimate source. A smishing attack might, for example, send the victim a webpage URL. Malware is installed on the victim's phone when they access the page.
4. **Whaling**
   A phishing assault that targets high-profile targets within a business, such as senior executives, is known as whaling. Politicians and celebrities are also possible targets.
5. **Pharming**
   Pharming is the impersonation of a reputable website to dupe individuals to submit their personal information. Pharming leads consumers to a phony website that appears to be legitimate. Victims then provide their data under the impression that they have reached a legitimate website.
6. **Spyware**
   It is software that allows a criminal to collect data about a user's computer activity. Activity trackers, keystroke collecting, and data capture are all standard features of spyware. A spyware frequently adjusts it security settings in an attempt to circumvent security measures. Spywares often come along with legitimate applications or Trojan horses. Many shareware sites are infested with spyware.
7. **Scareware**
   It is software that uses fear to encourage the user to execute a specified action. Scareware creates pop-up windows that seem like those found in operating systems. These windows display fake messages claiming that the system is in danger or requires the execution of a specific program to resume regular operation. In actuality, there are no issues, and malware infects the user's PC if they agree and permit the indicated program to run.
8. **Adware**
   Adware generates cash for its makers by displaying unpleasant pop-ups. By tracking the pages visited, the malware may be able to determine the user's interests. It can then send relevant pop-up advertisements to those websites. Adware is installed by default in some software versions.
9. **Spam**
   Unsolicited emails are referred to as spam (also known as junk mail). Spam is almost always a form of advertising. Spams can contain hazardous links, viruses, or false content. The ultimate goal is to collect sensitive data like a social security number or bank account details.

The majority of spams originate from numerous computers connected to a network infected with a virus or worm. These infected computers send out as many spam emails as they can.

Ref: https://www.tutorialspoint.com/types-of-email-attacks
https://www.acronis.com/en-us/blog/posts/email-cyber-attack/

4.3.2 Password Attack, Malware

Password Attacks

Because passwords are the most commonly used mechanism to authenticate users to an information system, obtaining passwords is a common and effective attack approach. Access to a person's password can be obtained by looking around the person's desk, ''sniffing'' the connection to the network to acquire unencrypted passwords, using social engineering, gaining access to a password database or outright guessing. The last approach can be done in either a random or systematic manner:

- Brute-force password guessing means using a random approach by trying different passwords and hoping that one work Some logic can be applied by trying passwords related to the person's name, job title, hobbies or similar items.
- In a dictionary attack, a dictionary of common passwords is used to attempt to gain access to a user's computer and network. One approach is to copy an encrypted file that contains the passwords, apply the same encryption to a dictionary of commonly used passwords, and compare the results.

In order to protect yourself from dictionary or brute-force attacks, you need to implement an account lockout policy that will lock the account after a few invalid password attempts. You can follow these account lockout best practices in order to set it up correctly.

Preventing Password Attacks

The best way to fix a password attack is to avoid one in the first place. Ask your IT professional about proactively investing in a common security policy that includes:

Multi-factor authentication. Using a physical token (like a Yubikey) or a personal device (like a mobile phone) to authenticate users ensures that passwords are not the sole gate to access.

Remote access. Using a smart remote access platform like OneLogin means that individual websites are no longer the source of user trust. Instead, OneLogin ensures that the user's identity is confirmed, then logs them in.

Biometrics. A malicious actor will find it very difficult to replicate your fingerprint or facial shape. Enabling biometric authentication turns your password into only one of several points of trust that a hacker needs to overcome.

Ref: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks
https://www.onelogin.com/learn/6-types-password-attacks
https://www.manageengine.com/log-management/cyber-security-attacks/common-types-of-cyber-attacks.html

Malware:

Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for "malicious software." Examples of common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware.

Types of Malware Attacks

- Most malware types can be classified into one of the following categories:
- Virus: When a computer virus is executed, it can replicate itself by modifying other programs and inserting its malicious code. It is the only type of malware that can "infect" other files and is one of the most difficult types of malware to remove.
- Worm: A worm has the power to self-replicate without end-user involvement and can infect entire networks quickly by moving from one machine to another.

- Trojan: Trojan malware disguises itself as a legitimate program, making it one of the most difficult types of malware to detect. This type of malware contains malicious code and instructions that, once executed by the victim, can operate under the radar. It is often used to let other types of malware into the system.
- Hybrid malware: Modern malware is often a "hybrid" or combination of malicious software types. For example, "bots" first appear as Trojans then, once executed, act as worms. They are frequently used to target individual users as part of a larger network-wide cyber attack.
- Adware: Adware serves unwanted and aggressive advertising (e.g., pop-up ads) to the end-user.
- Malvertising: Malvertising uses legitimate ads to deliver malware to end-user machines.
- Spyware: Spyware spies on the unsuspecting end-user, collecting credentials and passwords, browsing history and more.
- Ransomware: Ransomware infects machines, encrypts files and holds the needed decryption key for ransom until the victim pays. Ransomware attacks targeting enterprises and government entities are on the rise, costing organizations millions as some pay off the attackers to restore vital systems. Cyptolocker, Petya and Loky are some of the most common and notorious families of ransomware.

Over the years, malware has been observed to use a variety of different delivery mechanisms, or attack vectors. While a few are admittedly academic, many attack vectors are effective at compromising their targets. These attack vectors generally occur over electronic communications such as email, text, vulnerable network service, or compromised website, malware delivery can also be achieved via physical media (e.g. USB thumb drive, CD/DVD, etc.).

Prevention:
Typically, businesses focus on preventative tools to stop breaches. By securing the perimeter, businesses assume they are safe. Some advanced malware, however, will eventually make their way into your network. As a result, it is crucial to deploy technologies that continually monitor and detect malware that has evaded perimeter defenses. Sufficient advanced malware protection requires multiple layers of safeguards along with high-level network visibility and intelligence.

How to Prevent Malware Attacks
- To strengthen malware protection and detection without negatively impacting business productivity, organizations often take the following steps:
- Use anti-virus tools to protect against common and known malware.
- Utilize endpoint detection and response technology to continuously monitor and respond to malware attacks and other cyber threats on end-user machines.
- Follow application and Operating System (OS) patching best practices.
- Implement the principle of least privilege and just-in-time access to elevate account privileges for specific authorized tasks to keep users productive without providing unnecessary privileges.
- Remove local administrator rights from standard user accounts to reduce the attack surface.

- Apply application greylisting on user endpoints to prevent unknown applications, such as new ransomware instances, from accessing the Internet and gaining the read, write and modify permissions needed to encrypt files.
- Apply application whitelisting on servers to maximize the security of these assets.
- Frequently and automatically backup data from endpoints and servers to allow for effective disaster recovery.

Ref:
https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html
https://www.cyberark.com/what-is/malware/
https://www.rapid7.com/fundamentals/malware-attacks
https://www.cisco.com/c/en_in/products/security/advanced-malware-protection/what-is-malware.html

4.4 Hackers:

4.4.1 Various Vulnerabilities:

What is Vulnerability in Cyber Security?

Vulnerability in cyber security refers to any weakness in an information system, system processes, or internal controls of an organization. These vulnerabilities are targets for lurking cybercrimes and are open to exploitation through the points of vulnerability.

These hackers are able to gain illegal access to the systems and cause severe damage to data privacy. Therefore, cybersecurity vulnerabilities are extremely important to monitor for the overall security posture as gaps in a network can result in a full-scale breach of systems in an organization.

Examples of Vulnerabilities

Below are some examples of vulnerability:

- A weakness in a firewall that can lead to malicious hackers getting into a computer network
- Lack of security cameras
- Unlocked doors at businesses

Types of Vulnerabilities

Below are some of the most common types of cybersecurity vulnerabilities:

- System Misconfigurations
  Network assets that have disparate security controls or vulnerable settings can result in system misconfigurations. Cybercriminals commonly probe networks for system misconfigurations and gaps that look exploitable. Due to the rapid digital transformation, network misconfigurations are on the rise. Therefore, it is important to work with experienced security experts during the implementation of new technologies.
- Out-of-date or Unpatched Software
  Similar to system misconfigurations, hackers tend to probe networks for unpatched systems that are easy targets. These unpatched vulnerabilities can be exploited by attackers to steal sensitive information. To minimize these kinds of risks, it is essential to establish a patch management schedule so that all the latest system patches are implemented as soon as they are released.
- Missing or Weak Authorization Credentials
  A common tactic that attackers use is to gain access to systems and networks through brute force like guessing employee credentials. That is why it is crucial that employees be

educated on the best practices of cybersecurity so that their login credentials are not easily exploited.

- Malicious Insider Threats

  Whether it's with malicious intent or unintentionally, employees with access to critical systems sometimes end up sharing information that helps cyber criminals breach the network. Insider threats can be really difficult to trace as all actions will appear legitimate. To help fight against these types of threats, one should invest in network access control solutions, and segment the network according to employee seniority and expertise.

- Missing or Poor Data Encryption
  It's easier for attackers to intercept communication between systems and breach a network if it has poor or missing encryption. When there is poor or unencrypted information, cyber adversaries can extract critical information and inject false information onto a server. This can seriously undermine an organization's efforts toward cyber security compliance and lead to fines from regulatory bodies.

- Zero-day Vulnerabilities
  Zero-day vulnerabilities are specific software vulnerabilities that the attackers have caught wind of but have not yet been discovered by an organization or user.

In these cases, there are no available fixes or solutions since the vulnerability is not yet detected or notified by the system vendor. These are especially dangerous as there is no defense against such vulnerabilities until after the attack has happened. Hence, it is important to remain cautious and continuously monitor systems for vulnerabilities to minimize zero-day attacks.

Vulnerability Remediation

To always be one step ahead of malicious attacks, security professionals need to have a process in place for monitoring and managing the known vulnerabilities. Once a time-consuming and tedious manual job, now it is possible to continuously keep track of an organization's software inventory with the help of automated tools, and match them against the various security advisories, issue trackers, or databases.

If the tracking results show that the services and products are relying on risky code, the vulnerable component needs to be located and mitigated effectively and efficiently.

The following remediation steps may seem simple, but without them, organizations may find themselves in a bit of difficulty when fighting against hackers.

Step 1: Know Your Code – Knowing what you're working with is crucial and the first step of vulnerability remediation. Continuously monitoring software inventory to be aware of which software components are being used and what needs immediate attention will significantly prevent malicious attacks.

Step 2: Prioritize Your Vulnerabilities – Organizations need to have prioritization policies in place. The risk of the vulnerabilities needs to be evaluated first by going through the system configuration, the likelihood of an occurrence, its impact, and the security measures that are in place.

Step 3: Fix – Once the security vulnerabilities that require immediate attention are known, it is time to map out a timeline and work plan for the fix.

Ref: https://intellipaat.com/blog/vulnerability-in-cyber-security/#no1
https://www.upguard.com/blog/vulnerability#top