4.1 Concepts of cyber security

Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

Cyber Security is the process and techniques involved in protecting sensitive data, computer systems, networks, and software applications from cyber attacks.

4.1.1 TYPES OF THREATS(ALREADY DISCUSSED)

4.1.2 What are the benefits of cybersecurity?

- Cyber security will defend us from critical cyber- attacks.
- It helps us to browse the safe website.
- Cyber security will defend us from hacks & virus.
- The application of cyber security used in our PC needs to update every week.
- Internet security processes all the incoming & outgoing data on our computer.
- It helps to reduce computer chilling & crashes.
- Gives us privacy.
- Business protection against cyberattacks and data breaches.
- Prevention of unauthorized user access.
- Improved recovery time after a breach.
- Protection for end users and endpoint devices.
- Regulatory compliance.
- Business continuity.
- Improved confidence in the company's reputation and trust for developers, partners, customers, stakeholders and employees.

4.2 Basic Terminologies:

4.2.1

IP ADDRESS

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

MAC ADDRESS

A media access control address (MAC address) is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.

4.2.2 DNS

The Domain Name System (DNS) is the hierarchical and distributed naming system used to identify computers reachable through the Internet or other Internet Protocol (IP) networks.

DNS is a hostname for IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers

There are various kinds of DOMAIN:

Generic domain: .com(commercial) .edu(educational) .mil(military) .org(non profit organization) .net(similar to commercial) all these are generic domain.

Country domain .in (india) .us .uk

Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping. So DNS can provide both the mapping.

4.2.3 Dynamic Host Configuration Protocol

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture.

DHCP does the following:

- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.

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.

Advantages – The advantages of using DHCP include:

- centralized management of IP addresses
- ease of adding new clients to a network
- reuse of IP addresses reducing the total number of IP addresses that are required
- simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client

Disadvantages – Disadvantage of using DHCP is:

- IP conflict can occur

What is a Router?

The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets.

Bots – meaning & definition

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.

An Internet bot, web robot, robot or simply bot, is a software application that runs automated tasks (scripts) over the Internet, usually with the intent to imitate human activity on the Internet, such as messaging, on a large scale

Bots can be:

Chatbots: Bots that simulate human conversation by responding to certain phrases with

programmed responses

Web crawlers (Googlebots): Bots that scan content on WebPages all over the Internet

Social bots: Bots that operate on social media platforms

Malicious bots: Bots that scrape content, spread spam content, or carry out credential stuffing

attacks

4.3 Common types of attacks:

4.3.1DDOS(ALREADY DISCUSSED)

4.3.2

Man in the Middle

A man-in-the-middle, monster-in-the-middle attack is a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other, as the attacker has inserted themselves between the two parties.

One example of a MITM attack is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them

believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones

Email attack

Electronic mail (email) is a digital messaging system that allows users to send and receive messages via the Internet. Email communications are sent and received by email servers, available from all Internet Service Providers (ISP).

Emails are sent between two separate server folders: the senders and the recipients. A sender saves, transmits, or forwards email messages, whereas a recipient accesses an email server to view or download emails.

Types of Email Attacks

Phishing :Phishing occurs when a malicious party sends a fraudulent email disguised as being from an authorized, trusted source. The message intent is to trick the recipient into installing malware on his or her device or into sharing personal or financial information.

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. In an attempt to overcome security measures, spyware often modifies security settings. Spyware often bundles itself with legitimate software or with Trojan horses.

Adware: Adware typically displays annoying pop-ups to generate revenue for its authors. The malware may analyze user interests by tracking the websites visited. It can then send pop-up advertising relevant to those sites. Some versions of software automatically install Adware.

Spam: Spam (also known as junk mail) is unsolicited email. In most cases, spam is a method of advertising. However, spam can send harmful links, malware, or deceptive content. The end goal is to obtain sensitive information such as a social security number or bank account information. Most spam comes from multiple computers on networks infected by a virus or worm. These compromised computers send out as much bulk email as possible

4.3.3

Password Attack

It’s a type of cyberattack where hackers attempt to access a file, folder, account, or computer secured with a password.

It’s generally done with the help of software that expedites cracking or guessing passwords.

Common password attack types:

Spear Phishing

You’re directed to click or download a link in an email from a known sender. The link takes you to a malicious look-a-like website where you log in, inadvertently sharing your password with threat actors.

Brute Force Attacks

In a brute force attack, hackers steal passwords with the hit-and-try method using special software. You can prevent this by using a secure password manager.

Dictionary Attacks

Here, bad actors use a list of common words and phrases from a dictionary. This is the opposite of a brute force password attack as they don't use character-by-character attempts.

These lists often include names of famous movie characters, pet names, and public online info like birthdays etc.

Keylogger Attacks

Attackers use malware to attempt keylogger or keystroke logger password attacks. In cybersecurity, These attacks are among the most dangerous as they reveal even the strongest and most secure passwords. Hackers record keystrokes when you enter them.

This way, they can obtain other information as well. So, you must use encryption methods to maintain your overall digital and physical data security.

What is a malware attack?

A malware attack is a common cyberattack where malware (normally malicious software) executes unauthorized actions on the victim's system. The malicious software encompasses many specific types of attacks such as spyware, command and control, and more.

Malware (a malicious software) is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interferes with the user's computer security and privacy

4.4 Hackers

A hacker is a person who breaks into a computer system. The reasons for hacking can be many: installing malware, stealing or destroying data, disrupting service, and more. Hacking can also be done for ethical reasons, such as trying to find software vulnerabilities so they can be fixed. A hacker is a person skilled in information technology who uses their technical knowledge to achieve a goal or overcome an obstacle, within a computerized system by non-standard means.

4.4.1 What is Vulnerability in Cyber Security?

A 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 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 in an organization.

4.4.1.1 Injection attacks

This type of attack allows an attacker to inject code into a program or query or inject malware onto a computer in order to execute remote commands that can read or modify a database, or change data on a web site.

Format String Attack

Alters the flow of an application by using string formatting library features to access other memory space.

In this type of attack, data provided by users might be used as formatting string input for certain C/C++ functions (for example: fprintf, printf, sprintf).

SQL Injection

Takes advantage of the SQL syntax to inject commands that can read or modify a database, or compromise the meaning of the original SQL query.

In this type of attack, an attacker can spoof identity; expose, tamper, destroy, or make existing data unavailable; become the Administrator of the database server.

OS command injection

Web applications may occasionally need to execute system commands in the underlying operating system. If the application has an OS command injection vulnerability, attackers are able to provide their own operating system commands in user inputs. Successful command injection (shell injection) can be extremely dangerous, as it can allow attackers to obtain information about the operating system and server configuration, escalate their permissions, or even execute arbitrary system commands to fully compromise the system.

Code injection (remote code execution)

If attackers are able to provide application code as user input and get the server to execute it, your application has a code injection vulnerability (aka remote code execution, or RCE). For example, if the vulnerable application is written in PHP, attackers can inject PHP code that gets executed by the PHP interpreter on the web server.

Note that code injection is different from OS command injection because you are injecting application code, not system commands. If the attacker manages to get remote code execution, the target system should be considered compromised, so this is a critical vulnerability.

Changes in security setting

Changes in security settings: Security misconfiguration is the lack of proper security in server or web apps, opening up your business to cyber threats. This kind of misconfiguration runs rampant,commonly occurring when levels of the application stack are upgraded while others are left untouched,as the default settings may have included insecurities that go unaddressed.

• Running an application with debug enabled in production
• Having directory listing (which leaks valuable information) enabled on the server
• Running outdated software (think WordPress plugins, old PhpMyAdmin)
• Running unnecessary services
• Not changing default keys and passwords (which happens more frequently than you'd believe)
• Revealing error handling information (e.g., stack traces) to potential attackers

4.4.1.2.Expouser of sensitive data

What is Sensitive Data Exposure?

Sensitive data is anything that should not be accessible to unauthorized access, known as sensitive data.

Sensitive Data Exposure occurs when an organization unknowingly exposes sensitive data or when a security incident leads to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to sensitive data. Such Data exposure may occur as a result of inadequate protection of a database

Sensitive Data Exposure can of the following three types:

- Confidentiality Breach: where there is unauthorized or accidental disclosure of, or access to, sensitive data.
- Integrity Breach: where there is an unauthorized or accidental alteration of sensitive data.
- Availability Breach: where there is an unauthorized or accidental loss of access to, or destruction of, sensitive data. This will include both the permanent and temporary loss of sensitive data

Data Exposure

Data exposure is when sensitive information is lost due to unintentional exposure. This differs from a data breach which occurs when an unauthorized individual or group takes private information during an attack.

Example The 2021 LinkedIn Data Hack

Attackers reportedly orchestrated a breach to expose the data of up to 700 Million (92%) of LinkedIn's users. While doing so, attackers used scraping tools to collect user data and sell it online

Best Practices to Prevent Sensitive Data Exposure

The proliferation of information-driven applications has made cybercriminals shift their focus from web applications and servers to sensitive data. Some best practices to mitigate sensitive data exposure vulnerabilities include:

Identify and Classify Sensitive Data

It is important to determine and classify sensitive data with extra security controls. This data should then be filtered by the sensitivity level and secured with the appropriate security controls.

Apply Access Controls

Security teams should focus their energy on the authentication, authorization, and session management processes by provisioning a robust Identity and Access Management (IAM) mechanism. With the right access controls in place, organizations must ensure that only the intended individuals can view and modify sensitive data.

Perform Proper Data Encryption with Strong, Updated Protocols

Sensitive data should never be stored in plain text. It is important to ensure that user credentials and other personal information are protected using modern cryptographic algorithms that address the latest security vulnerabilities.

Disable Caching and Autocomplete on Data Collection forms

While caching and autocomplete features help improve user experience, they contain security risks that may attract attackers. Hackers may rely on a user's browser to easily log in to an account since the autocomplete feature fills in the credentials.

Caching stores sections of web pages for easier loading in subsequent visits, which allows attackers to use it to map out a user's movements. As a best practice, it is recommended that caching and autocomplete of forms are disabled by default and only activated as needed.

4.4.1.3 Breach in authentication protocol

An **authentication protocol** is a type of computer communications protocol or cryptographic protocol specifically designed for transfer of authentication data between two entities. It allows the receiving entity to authenticate the connecting entity (e.g. Client connecting to a Server) as well as authenticate itself to the connecting entity (Server to a client) by declaring the type of information needed for authentication as well as syntax. It is the most important layer of protection needed for secure communication within computer networks.

With the increasing amount of trustworthy information being accessible over the network, the need for keeping unauthorized persons from access to this data emerged. Stealing someone's identity is easy in the computing world - special verification methods had to be invented to find out whether the person/computer requesting data is really who he says he is. The task of the authentication protocol is to specify the exact series of steps needed for execution of the authentication

Broken authentication is an umbrella term for several vulnerabilities that attackers exploit to impersonate legitimate users online. Broadly, broken authentication refers to weaknesses in two areas: session management and credential management.

Session Management Flaws Open the Door to Attacks. Session management is part of broken authentication, but the two terms are often listed side by side so people don't assume that "authentication" refers only to usernames and passwords. Since web applications use sessions and credentials to identify individual users, attackers can impersonate them using either mechanism.

4.4.2 Types of Hackers: White hat and Black hat

Main types of hackers: Black hat hacker, White hat hacker and Gray hat hacker.

1) Black Hat Hacker - Evil Doer

The black hat hacker is the one who hacks for malicious intent - he is the bad guy. This type of hacker uses his or her skills to steal money or data, knock a computer system offline, or even destroy them. Some of these hackers love to see their work and name in the news, so they would try to target big name organizations and companies. For instance, they might change the front page of a company website.

Black hats also try to break into computer systems to steal credit card information and possibly steal valuable information to sell on the black market. They may even lock out the computer and network system from the owners and then hold them for ransom.
The black hat works outside of the law. This is the hacker that we as a society are most familiar with. Some black hats have cost companies hundreds of millions of dollars in damages for credit card and social security information theft. They can work alone, in that case known as a lone wolf, or with a team. They work slowly and methodically, since the black hat knows it takes patience to compromise a computer or a network system in order to a hit a big payoff and not be caught.

2) White Hat Hacker – Ethical Hacker

White hat hackers are cyber security professionals who are authorized or certified to hack organizational networks and computer systems. They use their expertise and skills to find vulnerabilities in systems. A white hacker is also known as Ethical Hacker.
Typically, large organizations, businesses, and governments hire white hat hackers to identify security vulnerabilities before black hat hackers can. White hat hackers spot and fix the weaknesses in the security systems and safeguard them against external attacks and data breaches. They are also known as ethical hackers.
Ethical hackers, thus, do not intend to harm a system. Instead, they find loopholes in a system as a part of penetration testing and vulnerability assessments.
White hat hackers usually have a good degree of technical expertise and broad skills in programming, networking, and IT.

3) Gray hat hackers

Gray hat hackers may not have the criminal or malicious intent of a black hat hacker, but they also don't have the prior knowledge or consent of those whose systems they hack into. Nevertheless,when gray hat hackers uncover weaknesses such as zero-day vulnerabilities, they report them rather than fully exploiting them. But gray hat hackers may demand payment in exchange for providing full details of what they uncovered