DOMS | Page No.
Date / /

CYBER SECURITY

Introduction :

Cyber Security: The technique of protecting internet connected systems such as computers, servers, mobile devices, electronic systems, networks and data from malicious attacks / Cyber thefts is known as cyber security.

We can divide cybersecurity into two parts one is cyber and the other is security. Cyber refers to the technology that includes systems, networks, programs and data. And security is concerned with the protection of systems, networks, application and information. In some cases, it is also called electronic information security or information technology security. Example of cyber security is implementing strong, unique passwords and enabling two-factor authentication to protect online accounts from unauthorized access.

DOMS | Page No.
Date / /

Ques 1 What is difference between security and cyber security?

Ans

Security	Cyber Security
It is a broad term encompassing measures taken to ensure safety and protection against various risks, threats or damagers. It can relate to personal safety, financial security or the safe-guarding of physical assets.	It specifically focuses on protecting digital system, networks and data from unauthorized access, attacks or damage. It deals with the security of information technology and the prevention of cyber threats such as hacking, malware and other cyberattacks. In essence, cyber security is a subset of overall security, concentrating on the digital realm.

Ques 2 Explain cyber security a problem.

Ans Cyber Security is a critical concern due to the increasing frequency of cyber treats. As our lives become more digital, the potential for data breches, identity theft, and other malicious activities grows. Organizations and individuals face

challenges in safeguarding sensitive information, leading to a constant cat-and-mouse game with cyber criminals who exploit vulnerabilities in system and networks. The evolving nature of cyber threats makes it challenging to stay ahead, requiring continuous efforts to enhance defenses and protect against cyber risks.

⇨ Targets and attacks

There are two general reasons a particular computer system is attacked: either it is specifically targeted by the attacker, or it is an opportunistic target.

Specific Target: The attacker has chosen the target not because of the hardware or software the organization is running but for another reason; perhaps a political reason.

Opportunistic Target: An attack against a target of opportunities is conducted against a site that has software that is not safe to a specific exploit.

DOMS | Page No.
Date / /

⇒ Security Management

Security management covers all aspects of protecting an organization's asset - include computers, people, buildings and other assets - against risk.

Types of Security Management

1. Information Security Management: It include implementing security best practices and standards designed to mitigate threats to data like those found in the ISO/ISE 27000 family of standard

2. Network Security Management :-
- Implement data loss prevention
- Use aproxi on wifi.
- Educate your employees.
- Keep software up to date.
- Perform regular data backups.
- Watch out for engineering attacks.

3. Cyber Security Management: It is a set of policies, procedures and technologies designed to protect computer networks, system and data from unauthorized access, theft or damage.

DOMS | Page No.
Date / /

⇒ Confedential: The data is only available to authorized (authority) parties when information has been kept confidential it means that it has not been compromised by other parties.

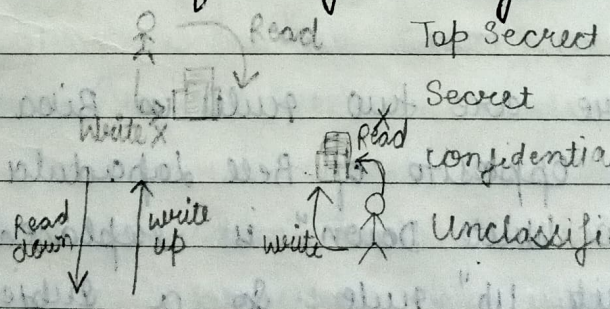
⇒ Authorisation: The process of varifying the identity of a user, process, or device often as a prerequisite to allowing access to resources in an information system.

⇒ Integrity: That data ~~is~~ accurate, real and safeguarded ~~for~~ from unauthorised user.

Security Model according to CIA.

1. Bell-LaPadula Model for Confidentiality:

- Top Secret
- Secret
- Confidential
- Unclassified



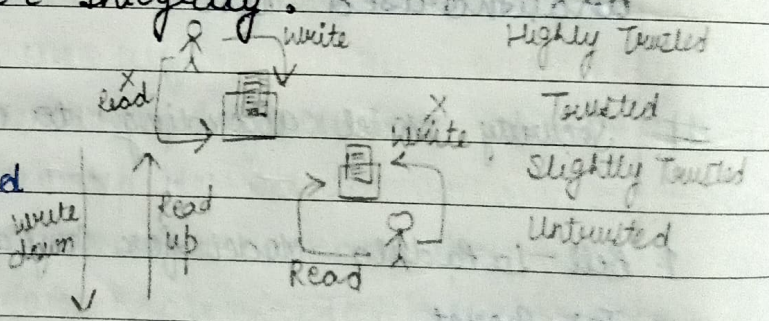
There are two major rules in this model. The first rule is "No Write Down". It means that subjects are not allowed to write objects that have a lower security clearance.

In other words, a Top Secret agent is not allowed to write an unclassified, confidential or secret document. Simply to avoid top information only to top secret agents have from leaking.

Since Bell-Lapadula was designed for military use, subjects that have an unclassified security clearance are not allowed to read secret information. This rule is called "No Read Up". It means that subjects are not allowed to read objects that have a higher security clearance.

2. Biba Model for Integrity:

- Highly Trusted
- Trusted
- Slightly Trusted
- Untrusted



There are two rules in Biba Model, which are the opposite of Bell Lapadula rules. The "No Write Down" is replaced by the "No Write Up" rule. So a subject can only write to objects with an equal or lower level of integrity. Since the goal here is integrity, we want to ensure that highly trusted documents are not tampered by Untrusted subjects.

The "No Read Up" rule is replaced by the "No Read Down" rule. Subjects can only read objects with an equal or higher level of integrity. To avoid highly trusted subjects getting untrusted information they will then write in highly trusted documents.

Low Water Mark policy for subject and Object.

3. Clarke Wilson Security Model
- Subject: It is any user who is requesting for data items.
- Constrained Data Items (CI): It cannot be accessed directly by the subject. These need to be accessed via Clarke Wilson Security Model.
- Unconstrained Data Items (UI): It can be accessed directly by subjects.
- Transformation Process (TP): Here, the subjects request to access the constrained data items is handled by TP which then convert it into permissions and then forwards it to IVP.
- Integration Verification Process (IVP): The IVP will perform authentication and authorization. If that is successful, then the subject is given access to CI.

DOMS | Page No.
Date / /

- **Website defacing**: It is an attack on a website that changes the visual appearance / orginality of a website or a web page.

- Ways to minimize the chances of attacks:
1. Create Backups
2. Keep your system and software updated.
3. Use strong passwords, Authetication - one step, two step verification
4. Pay close attention to physical security.
5. Install Firewalls → patches.

- **Hactivist attack**: It is a type actimism that involves the act of hacking to bring attention to a cause or to protest an issue often for politically motivated purpodes. eg → Distributed DOS, Website Displacement, use of social media to spread awareness.
(That attack which is used to stop negative attack.)

- Ethics: It defines right and wrong actions in specific situations and is fundamental to society.

Monday

Ethics serves as a guidepost for cybersecurity professionals. It helps identify the type of online behavior and conduct that harms individuals and businesses.

Ethical principles are what separate cyber-security professionals from hackers. for eg. while the latter tries to steal data, the former tries to protect it. When hacker access data, they use it for evil purposes. On the other hand, cybersecurity professionals, who have access to the same data, use their skills to ensure that the data is safe and secure.

Importance of Cyber Security:

Cybersecurity professionals deal with many threats. These unethical online activities have a profound impact on people and business. for eg. a hacker may steal a company's data, an act that can compromise customer data. A cybercriminal can then take that data and sell it on the dark web. Cyber Security is vital to preserve privacy and guard against identity theft.

Cyber Security also protect people from cyber-crimes such as financial fraud. for eg. consumers

exchange their data with banks and financial institutions when conducting online banking. Cybersecurity helps secure financial transactions, safeguarding bank accounts and credit card information.

Ethical Responsibilities of Cybersecurity Professionals:
Organizations hire cybersecurity professionals to protect their sensitive information from cyber threats, and hiring decisions for cybersecurity roles don't come lightly. Frameworks for cyber ethics and code of conduct may vary from organization.
For cybersecurity professionals, keeping systems secure often means using privileged access to data to perform activities such as white hat hacking, also known as ethical hacking. White hat hacking describes penetrating protected system using hacking tools and techniques to test the security of systems, networks & software.
White hat hacking offers an eg. of cyber-security ethical issues in the profession. A white hat hacker must be trustworthy enough to safeguard the confidentiality of the information they encounter. A solid ~~be~~ ethical foundation can serve as the bedrock to help employees make the right decisions as they face some key cybersecurity ethical issues.

Note:
A "deepfake" is an image, a video, voice or text created by AI. The "deep" is from "deep learning", a method of training computers on massive amounts of data to perform human like tasks. The "fake" indicates that its computer generated and difficult to distinguish from human generated media.

Security Models:-
An organization can take several approaches to implement its security model.

1. No Security: In this case, the approach could be a decision to implement no security at all.

2. Security through obscurity: In this, System is secure simply because nobody knows about its existence and content. This approach cannot work for too long, as there are many ways an attacker can come to know about it.

3. Host Security: This is a solution installed directly on your computer or server and act as a firewall to protect the rest of your network. With this kind of security, the software is installed on the device you want to secure, so it only protect one computer. For eg. a virus scanner is a typical

host based security solution. A host based security solution typically protects individual devices but not your network as a whole.

4. Network Security: It is designed to protect your entire network. This type of security uses a central server to protect all of the devices on your network. The server will scan all of your devices and protect them from viruses, malware and other threats. This type of security allows your organization to have a higher level of protection, as it covers all of your devices. It can also be used to secure your internet facing devices. This is useful if you are trying to protect your devices from cyber attacks.

Basics Security Terminology:

The operational Model of Computer Security:

For many years, the focus of security was on prevention. If we could prevent everyone who did not have authorization from gaining access to our computer systems and networks, then we assumed that we had achieved security. No matter how well we seem to do in prevention technology, somebody always seems to find a way around our safeguards. When this happens, our system is left unprotected. Thus, we need

multiple prevention techniques and also technology to alert us when prevention has failed and to provide ways to address the problem.

The result in a modification to our original security equation with the addition of two new elements — detection and response. Our security equation thus becomes:
Protection = Prevention + (Detection + Response).

Security Approaches:
Host Security, Network Security [already Explained]

Security Principles:

1. Least Privilege: One of the most fundamental principles in security is least privilege. This concept is applicable to many physical environments as well as network and host security. least privilege means that a subject (which may be user, application or process) should have only the necessary rights and privileges to perform its task with no additional permissions. Limiting an object's privileges limit the amount of harm that can be caused, thus limiting an organization's exposure to damage. Users may have access to the files on their workstation and a select set of files on a file server, but no access to critical data that is held within the database.

DOMS | Page No.
Date / /

Separation of Privilege:

Separation of duties specifies that for any given task, more than one individual needs to be involved. The task is broken into different duties, each of which is accomplished by a separate individual. By implementing a task in this manner, no single individual can abuse the system for his or her own gain. A simple example is a system in which one individual is required to place an order and a separate person is needed to authorize the purchase.

Complete Mediation:

It refers to that all accesses to objects be checked to ensure that they are allowed. Whenever a subject attempts to read an object, the operating system should mediate the action. First, it determines if the subject is allowed to read the object. If so, it provide the resources for the read to occur. If the subject tries to read the object again, the system should check that the subject is still allowed to read the object.

Economy of Mechanism:
This principle simplifies the design and implementation of security mechanisms. The principle of economy of mechanism states that security mechanisms should be as simple as possible. If a design and implementation are simple, fewer possibilities exist for errors. The checking and testing process is less complex, because fewer components and cases need to be tested. Complex mechanisms often make assumptions about the system & environment in which they run. If these assumptions are incorrect, security problems may result.

Principle of Psychological Acceptability:
The principle of psychological acceptability is interpreted to mean that the security mechanism may add some extra burden, but that burden must be both minimal and reasonable. eg. When you enter a wrong password, the system should only tell you that the user id or password was wrong. It should not tell you that only the password was wrong as this gives the attacker information.

Defense in Depth:
It is a cyber security strategy that uses multiple security practices to safeguard an

organization's network, web properties and resources. It is sometimes used interchangeably with the term 'layered security' because it depends on security solutions at multiple control layers - physical, technical and administrative - to prevent attackers from reaching a protected network.

Diversity of Defense:
It involves making different layers of security dissimilar so that even if attackers know how to get through a system that compromises one layer, they may not know how to get through a different type of layer that employs a different system for security.

Access Control:
Access Control is the ability to control whether a subject (such as an individual or a process running on a computer system) can interact with an object (such as a file or hardware device). Authentication, on the other hand, deals with verifying the identity of a subject. To understand the difference consider the example of an individual attempting to log into a computer system.
Authentication is the process used to verify to the computer system or network

that the individual is who they claim to be. The most common method to do this is through the use of a user ID and password. Once the individual has verified their identity, access controls regulate what the individual can actually do on the system.

Just because a person is granted entry to the system does not mean that they should have access to all data the system contain.

Authentication verifies the user's identity, ~~and access control uses this identity,~~ and access control uses this identity to grant or deny access. Access control mechanisms determine which operations the user can or cannot do by comparing the user's identity to an access control list (ACL).

Access controls encompass:

- File permissions, such as the right to create, read, edit or delete a file.
- Program permissions, such as the right to execute a program.
- Data permissions, such as the right to retrieve or update information in a database.

DOMS | Page No.
Date / /

Authentication Mechanisms:

Hardware or Software based mechanisms that force users to prove their identity before accessing data on a device.
There are three general factors commonly used in authentication.

In order to verify your identity you can provide

Something you know (knowledge factor):

The most frequently used example of this is the common User ID (or username) and password.

Something you have (possession factor):

Such as a magnetic stripe card that contains identifying information.

Something about you:

Use something about you for identification purposes, such as your fingerprint or the geometry of your hand. Obviously, for the second and third mechanisms to work, additional hardware devices need to be used (to read the card, fingerprint or hand geometry).

DOMS | Page No.
Date / /

Authentication and Access Control Policies :

- Group Policy : Operating System such as windows & Linux allow administrators to organize users into groups, to create categories of users for which similar access policies can be established. Using groups saves the administrator time, as adding a new user will not require the administrator to create a completely new user profile; instead, the administrator can determine to which group the new user belongs and then add the user to that group. Eg. of groups commonly found include administrator, user and guest. Take care when creating groups and assigning users to them so that you do not provide more access than is absolutely required for members of that group.

- Password Policy : A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong password and use them properly. Password should not be less than 8 character. It must include Alphanumeric character + Special Symbols. A password get changed after sometime and for creating new password user must know his old password.