Text

Description automatically generated

1. Cybersecurity is the protection of things that are connected to the internet, like hardware, software, and data, from cyberthreats. Individuals and enterprises used this method to protect against unauthorized access to data centers and other computer systems. Cybersecurity is also important in preventing attacks that try to stop or slow down a system or device's work.
2. - Unauthorized user try to get into the system and try to change the data from the system

- Unauthorized user try to get the sensitive data from the system

- Use viruses or malware that are sent through a hacked or spoofed website.

- Use viruses or malware that are sent through an email

Graphical user interface, text, email

Description automatically generated

a) i) When the information is a record of people's personal actions, such as in cases involving personal and financial information of clients of firms like Google, Amazon, Apple, and Walmart, secrecy is paramount.

ii) Access control mechanisms such as two-factor authentication, password less sign-on, and other access restrictions all promote confidentiality, but it's not just about letting authorized people in; it's also about keeping some files inaccessible.

b) i) By using authentication. Authenticating incoming packets is key to preventing spoofed packets that are used to perpetrate IP spoofing or MAC address spoofing attacks. Use standards and protocols that provide authentication.

ii) Network monitoring. Security teams should constantly monitor networks for abnormal activity by using intrusion detection systems or endpoint detection and response software. Security teams should also use the same sniffer programs that nefarious actors use to detect vulnerabilities on the network.

Graphical user interface, text, application, email

Description automatically generated

1. Software flaws, especially buffer overflows, are often exploited to gain control of a computer, or to cause it to operate in an unexpected manner.

b)

A picture containing text, air conditioner, appliance, microphone

Description automatically generated

c) Security policy

* To clear, comprehensive, and well-defined plans, rules, and practices that regulate access to an organization's system and the information includedin it.

Security mechanism  
 - Technical tools and techniques that are used to implement security services.

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |

1. Discretionary (DAC) is a type of security access control that allows or denies object access based on an access policy that is set by an object's owner group and/or its subjects.
2. Mandatory Access Control (MAC) a security strategy that limits the power each resource owner has to grant or deny access to resource objects in a file system

Graphical user interface, text

Description automatically generated with medium confidence

Bell-LaPadula preserve the confidentiality of information by using mandatory access control to make sure the multi-level security policy is being followed. For someone to be able to get information, he must have a clear need to know and meet or exceed the level of classification of the information. Subject can only read object if security clearance of object is lower than security clearance of object and has the permission to read. The information flows are Reads Up disallowed, Read Down allowed and vice versa for the write operation.

Diagram

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

a)

A picture containing diagram

Description automatically generated

Simple security property subject cannot read object of higher sensitivity and star property subject cannot write to object of lower sensitivity.

a clearance of Top Secret, then you cannot write messages to someone with a Secret clearance. This is known as No Write Down.

Simple Security Property: “No read up”, a subject at a specific clearance level cannot read an object at a higher classification level. Subjects with a Secret clearance cannot access Top Secret objects, for example.

b) The Simple Security Property states that there is no read up; that is, a subject at a specific classification level cannot read an object at a higher classification level. Subjects with a secret clearance cannot access top secret objects, for example.

\* Security Property (Star Security Property)

The \* Security Property states that there is no write down; that is, a subject at a higher classification level cannot write to a lower classification level.

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |

i)Fauzi cannot read WP file because he is not cleared enough and he does not have Troops or Planes clearance. Chong also cannot read it because he does not have Troops or Subs clearance. Chong can read RN file while Fauzi cannot. Fauzi cannot read SR file because he only has Subs clearance at the Secret level. However, he can read the TO file because he has Subs clearance at Secret level.

ii) Chong has a higher clearance.

Iii) Neither because both is not comparable.