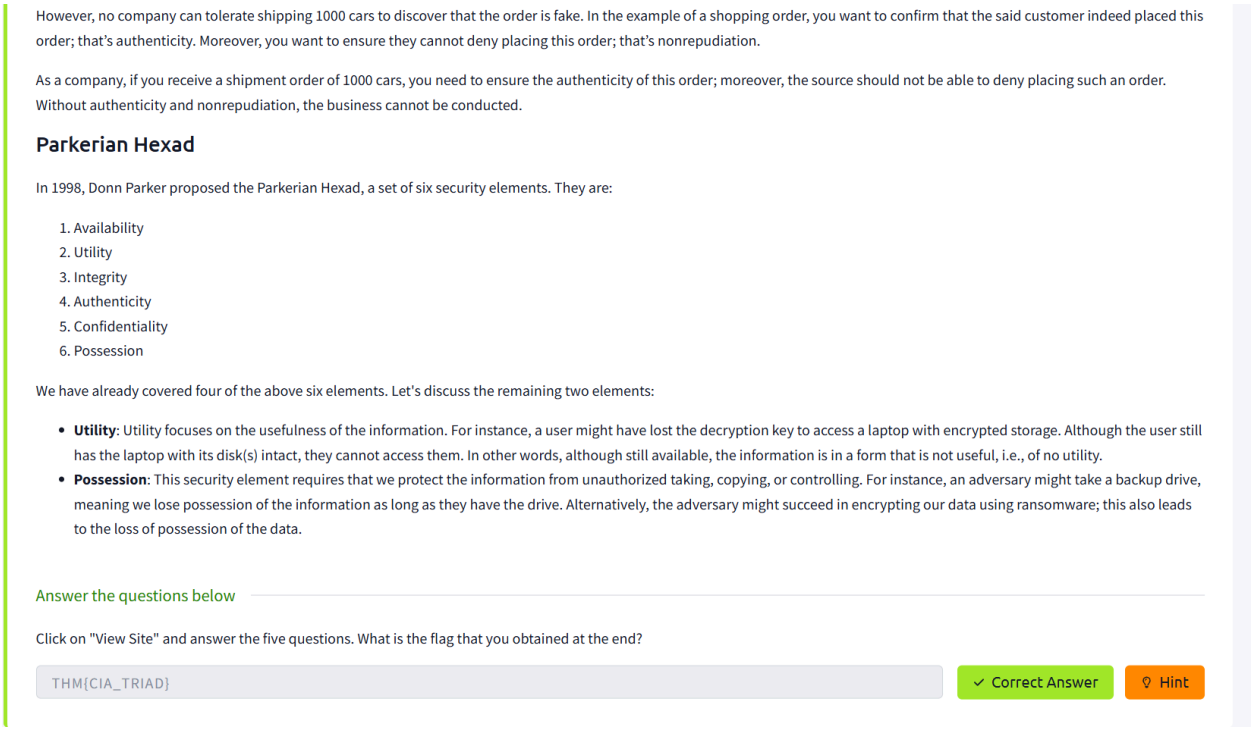
Name:Ram Haygrev S Roll no:231901039

EX 2: Security principles

Aim: To learn about security principles

ALGORITHM : N/A

Exercises:-



However, no company can tolerate shipping 1000 cars to discover that the order is fake. In the example of a shopping order, you want to confirm that the said customer indeed placed this order; that's authenticity. Moreover, you want to ensure they cannot deny placing this order; that's nonrepudiation.

As a company, if you receive a shipment order of 1000 cars, you need to ensure the authenticity of this order; moreover, the source should not be able to deny placing such an order. Without authenticity and nonrepudiation, the business cannot be conducted.

Parkerian Hexad

In 1998, Donn Parker proposed the Parkerian Hexad, a set of six security elements. They are:

1. Availability
2. Utility
3. Integrity
4. Authenticity
5. Confidentiality
6. Possession

We have already covered four of the above six elements. Let's discuss the remaining two elements:

- **Utility**: Utility focuses on the usefulness of the information. For instance, a user might have lost the decryption key to access a laptop with encrypted storage. Although the user still has the laptop with its disk(s) intact, they cannot access them. In other words, although still available, the information is in a form that is not useful, i.e., of no utility.
- **Possession**: This security element requires that we protect the information from unauthorized taking, copying, or controlling. For instance, an adversary might take a backup drive, meaning we lose possession of the information as long as they have the drive. Alternatively, the adversary might succeed in encrypting our data using ransomware; this also leads to the loss of possession of the data.

Answer the questions below

Click on "View Site" and answer the five questions. What is the flag that you obtained at the end?

THM{CIA_TRIAD}

✓ Correct Answer

Hint

Name:Ram Haygrev S Roll no:231901039

The Biba Model aims to achieve **integrity** by specifying two main rules:

- **Simple Integrity Property** : This property is referred to as “no read down”; a higher integrity subject should not read from a lower integrity object.
- **Star Integrity Property** : This property is referred to as “no write up”; a lower integrity subject should not write to a higher integrity object.

These two properties can be summarized as “read up, write down.” This rule is in contrast with the Bell-LaPadula Model, and this should not be surprising as one is concerned with confidentiality while the other is with integrity.

Biba Model suffers from various limitations. One example is that it does not handle internal threats (insider threat).

Clark-Wilson Model

The Clark-Wilson Model also aims to achieve integrity by using the following concepts:

- **Constrained Data Item (CDI)** : This refers to the data type whose integrity we want to preserve.
- **Unconstrained Data Item (UDI)** : This refers to all data types beyond CDI, such as user and system input.
- **Transformation Procedures (TPs)** : These procedures are programmed operations, such as read and write, and should maintain the integrity of CDIs.
- **Integrity Verification Procedures (IVPs)** : These procedures check and ensure the validity of CDIs.

We covered only three security models. The reader can explore many additional security models. Examples include:

- Brewer and Nash model
- Goguen-Meseguer model
- Sutherland model
- Graham-Denning model
- Harrison-Ruzzo-Ullman model

Answer the questions below

Click on "View Site" and answer the four questions. What is the flag that you obtained at the end?

THM{SECURITY_MODELS} ✓ Correct Answer

2. **Attack Surface Minimisation**: Every system has vulnerabilities that an attacker might use to compromise a system. Some vulnerabilities are known, while others are yet to be discovered. These vulnerabilities represent risks that we should aim to minimize. For example, in one of the steps to harden a Linux system, we would disable any service we don't need.
3. **Centralized Parameter Validation**: Many threats are due to the system receiving input, especially from users. Invalid inputs can be used to exploit vulnerabilities in the system, such as denial of service and remote code execution. Therefore, parameter validation is a necessary step to ensure the correct system state. Considering the number of parameters a system handles, the validation of the parameters should be centralized within one library or system.
4. **Centralized General Security Services**: As a security principle, we should aim to centralize all security services. For example, we would create a centralized server for authentication. Of course, you might take proper measures to ensure availability and prevent creating a single point of failure.
5. **Preparing for Error and Exception Handling**: Whenever we build a system, we should take into account that errors and exceptions do and will occur. For instance, in a shopping application, a customer might try to place an order for an out-of-stock item. A database might get overloaded and stop responding to a web application. This principle teaches that the systems should be designed to fail safe; for example, if a firewall crashes, it should block all traffic instead of allowing all traffic. Moreover, we should be careful that error messages don't leak information that we consider confidential, such as dumping memory content that contains information related to other customers.

In the following questions, refer to the ISO/IEC 19249 five design principles above. Answer with a number between 1 and 5, depending on the number of the design principle.

Answer the questions below

Which principle are you applying when you turn off an insecure server that is not critical to the business?

2 ✓ Correct Answer

Your company hired a new sales representative. Which principle are they applying when they tell you to give them access only to the company products and prices?

1 ✓ Correct Answer

While reading the code of an ATM, you noticed a huge chunk of code to handle unexpected situations such as network disconnection and power failure. Which principle are they applying?

5 ✓ Correct Answer

Result : Hence the exercises were completed successfully