INTROSEC HT2020

Problem 4

Define each of the following IT security related terms. Also, for each of these terms further illustrate the concept by choosing a closely connected IT security concept and explaining the relationship between the concepts. Furthermore, give an example of an application of these tools/threats/concepts. Give concrete examples wherever possible. Structure each of your answers with headings definition, relationship to [your chosen related concept], and example. Your answers to each part should contribute to evidence of your deep understanding of the concept. Related concepts and examples should be chosen and explained with care to maximise the depth of your answers.

Please note that in general a 50% complete answer will be required to obtain a pass mark for this problem

- Signature-based intrusion detection
- Asymmetric cryptosystems
- Integrity check
- Trojan horse

Solution

Signature-based intrusion detection

-Definition

It is a way to protect against already known malware/viruses. Known threats are assigned a unique identifier. So when a scan of the system is done against viruses, that number will be in a “library” in the scanner. If it is found it will be eliminated.

-Relationship to CIA

If the virus is found then we can eliminate it and secure our system once again. That way we can continue and maintain the confidentiality, integrity and availability of the system.

-Example

An exaple could be any antivirus that can take actions against those viruses.

Assymetric cryptosystems

-Definition

Assymetric cryptosystems are used for encryption and decryption of data. They refere to public key cryptography. A pair of keys is used to encrypt data. Eah user has a public key and a private key. The public key is handed to those who want to send encrypted data and the private key is kept by the one who will receive the encrypted data so he can later decrypt them. The public key as its name states can be known by everyone. The private/secrete key is the one that should be kept secrete. It is widely used nowdays and considered a very secure.

-Relationship to Confidentiality

It provides for the data not be seen by others and be read only by the appropriaty party. Meaning that it offers confidentialy gained by the encryption of the data

-Example

One example of an assymetric cryptosystem is SSH. And algorithm used for those is mainly RSA which is a block cipher consisted of two parts.

Integrity check

-Definition

It is a way to check whether data of files has been changed. Also it provides the way to see if packets over the network have been altered. For example in Ipv4 there is a checksum filed for that purpuse.

-Relationship to Integrity

In this case the relationship to integirty is clear. We check if the data is altered and if so the integrity of the data is tempered. It’s a good way to know if we obtain the integrity or not.

-Example

An example of an integrity check is the use of algorithms such as MD5 and SHA-1. Those create a hash of the original data and the put that gainst the hash of the received data to make sure that the ntegrity still remains. If the hash is the same it means the data has not been altered. Hashes are unique in the meaning that only same files have the same hash.

Trojan horse

-Definition

Trojan horse is a virus that disguises itself as something else and misleads the user of its intent. Basically a malware. They can come from email attachments and disguise as somthimg regular. When the malware is installed in the computer it can affect the computer.

-Relationship to Confidentiality

It is a malware that can monitor the computer of someone infected by it. Since it monitors the computer it can allow attackers/criminals to spy on you and get access of your data, thus violating the confidentiallity of it.

-Example

An example of it is RAT. A software that when it runs can afteward provide remote access to the system of the attacked one. That is done via backoor.