CAT-1

Information Security (BCSE317L)

F2+TF2 (Answer Key)

Q1. Imagine a smart thermostat designed to control home heating and cooling systems. The thermostat has a firmware update feature that lets it receive and apply new firmware remotely. The thermostat's firmware update process includes the following C code:

```
void firmware_update(char *update_info) { char data[256];
strcpy(data, update_info);
}
```

Identify the vulnerability and demonstrate the possible attacks. Also, explain the consequences of the attack and propose the mitigation strategies.

Answer:

(2.5 marks for each part)

- **Vulnerability** in this code is the use of strcpy, which does not perform bounds checking.
- An attacker can provide input longer than 256 bytes, causing a **buffer overflow attack**.
- **Consequences**: Compromise the device potentially allowing them to manipulate home temperature settings or access other connected devices; Further attacks on the home network since IoT devices often communicate with each other; Collecting personal data(e.g., usage patterns)
- **Mitigation**: use a safer function like strncpy and ensure it does not exceed the buffer size; Input Validation and Bounds Checking

Q2. A company's IT department receives reports of unusual activity across several computers on the network. Employees notice that their files are being corrupted, and some files are disappearing. Also, there are frequent pop-ups indicating that their antivirus is being disabled. The IT team discovers that the issue started after an employee downloaded and ran a software update from an unofficial source. Which type of threat is likely causing the issue: a virus, a worm, or a trojan? Differentiate between these malwares.

Answer:

The threat is most likely a **Trojan**. The fact that the problem started after downloading and running a ***seemingly legitimate update*** suggests that the malicious software was disguised as a harmless update (a common tactic used by trojans). Trojans often disguise themselves as legitimate software to gain access to the system and cause harm, like corrupting files and disabling security features. **(5 marks for identifying and explaining)**

(5 marks for differences)

Features	Virus	Worm	Trojan horse
Definition	Viruses are computer programs that connect to other software or programs to harm the system.	A worm is a malware program similar to a virus that doesn't interact with other system applications but instead multiplies and executes itself to slow down and harm the system's performance.	A Trojan Horse is a type of malware that steals sensitive data from a user's system and delivers it to a different location on the network.
Replication	It replicates itself.	It also replicates itself.	It doesn't replicate itself.
Execution	It relies on the transfer.	It replicates itself without human action and utilizes a network to embed itself in other systems.	It is downloaded as software and executed.
Remotely Controlled	A virus could not be remotely controlled.	It may be remotely controlled.	It may also be remotely controlled.
Infection	Viruses spread through executable files.	Worms take advantage of system flaws.	The Trojan horse runs as a program and is interpreted as utility software.
Rate of Spreading	Viruses spread at a moderate rate.	Worms spread at a quicker rate than viruses and Trojan horses.	In addition, the spread rate of Trojan horses is slower than that of viruses and worms.
Purpose	It is primarily utilized to modify or erase system data.	These are utilized to excessive using system resources and slow it down.	It may be utilized to steal user data to obtain access to the user's computer system.

Q3. A global e-commerce platform allows customers to log in using their existing social media accounts or email providers, enabling a streamlined shopping experience across different e-commerce sites.
a) Mention the key components and explain how Federated Identity Management can be used to provide this feature. (5 Marks)

b) With a neat diagram, explain the working of the appropriate user authentication protocol in this context. (5 Marks)

Answer:

(a) FIM scheme is a union of separate identification and authentication systems. While logging into the **service provider**(e-commerce website), the user would provide the credentials of their social media account or email account. These third-party services are the **identity providers**. The service provider trusts the identity provider to validate these credentials and grant access to the user. **(5 marks)**

(b) OAuth2 or SAML with diagrams **(5 marks)**

Q4. In an organisation, employees are categorized by their roles (Technician, Engineer, or Supervisor), and their certification levels (Basic or Expert), which determine their ability to operate equipment. Equipment is classified as high- risk or low-risk, and is monitored for its operational status (active, in maintenance, or idle). Access decisions

also consider environmental factors such as the time of request, and the user's location (on-site or off-site).

The organisation implements the following access control policy: "Engineers with Expert certification can access equipment in maintenance mode, but only on-site for operational safety." Also, the configuration file of every equipment in maintenance mode is encrypted and saved on a shared drive. Only authorised personnel can decrypt the file and access the content.

a) Identify the type of access control policy implemented in the organisation and justify your answer. With a neat diagram, explain the most appropriate encryption scheme. (6 Marks)

b) "Emily, an engineer having expert certification, tries to access a low-risk machine under maintenance from an off-site location." What would be the access control decision for this attempt? Justify your answer. (4 Marks)

Answer:

a) Attribute-based access control – with justification (3 marks)
   Attribute-based encryption scheme only permitting the On-Site Engineers with Expert certification to access equipment in maintenance mode. Include neat diagram and explain (3 marks)
b) Access Denied since the employee works off-site(policy says on-site) – 4 marks

Q5. "Multiprogramming Operating Systems address several functions that involve 10 computer security." Describe any five of these functions.

Answer:

Describe any 5 of the following functions **(2 marks per function)**

Enforced sharing
Interprocess communication and synchronization
Protection of critical operating system data
Guaranteed fair service
Interface to hardware
User authentication
Memory protection
File and I/O device access control
Allocation and access control to general objects