Sourav Mangla

Problem 1

Scenario: Email (Managing email server for a major presidential campaign).

Assumptions:

- The campaign email server is on the cloud-like AWS which is more secure than on-premise server.
- The client can access emails using SMTP or IMAP via a public network, HTTPS application protocol only.
- The server has rules to decide privileges and implemented on the firewall, OSs, and applications to minimize access and prevent unauthorized use.
- People who work to maintain this email server are trusted and have government security clearance.
- The attacker has enough computational power to perform brute force and other attacks.
- The attacker knows some information about candidates involved in the campaign so this can use in phishing and social engineering attacks.

Assets:

- **Personal information**:- Email server has all the information people who are involved in the campaign like their name, email address, mobile number, address, etc.
- **Confidential information**:- Email server has all the sensitive information about the campaign like fund information, speeches, party's agendas, etc.
- **Image of the candidate**:- Emails have much information about the candidates which can ruin the image of the candidate. for example, Hillary Clinton drew into controversy because of her emails.
- **Privacy**:- All candidate has their privacy in the emails.

Threats:

- **Unauthorized access to data**:- The first thing we need to do is establish strong password requirements to access the server. This prevents the password from being cracked via brute force, which is a universal way to bypass authentication.
- **Data leakage**:- When an email is sent via the internet, it may go through unprotected communication channels. Passwords, user names, and messages themselves can be intercepted. To prevent this, we need to encrypt both incoming and outgoing mail. SMTP, POP3, and IMAP protocols should be encrypted with SSL/TLS.
- **Spam**:- Spam is one of the biggest problems when it comes to email. It can either be sending external spam messages to your clients or Sending external spam messages to other clients. To prevent this threat, you need to use content filters. They're installed either on the mail server or on a proxy application to protect access to the server.

- **The threat of malware:-** Both servers and email clients are susceptible to malware. When an email server is infected, the stability of the whole system is compromised. Protection from malware involves both built-in tools and third-party antivirus software.
- **DoS threat**:- This threat disrupt the service for some time and it leads to unreceived and unsent emails, not to mention the time spent trying to restore the service.

Countermeasures:

- **Multiple Host**:- Running all email services on multiple hosts, block the single point of failure for all messaging services.
- **SMTP Gateway**:- Do not connect email server directly to the Internet. Instead, use an SMTP gateway that sits directly in front of the email server to serve as a proxy and frontline system that can be more easily secured from attacks.
- **Logging and Alert**:- Raise a warning message or alert if there is any malicious activity or potential intruders and all the activity must be logged.
- **Protection Software**:- Run malware or virus protection software on the server periodically.
- **2-Step Authentication**:- Enforce all the clients to use 2-step authentication to login into the email server.

Problem 2

Scenario: Store

Assumptions:

- The store does not have any security guard and the attacker(thief) knows about it.
- The attacker has full access to the products present in the store and has the computational power to do equipment malfunction.

Assets:

- **Products**:- All the product available is the main assets to the store.
- **Customers**:- Customer is also an asset to the store because they are going to buy products from the store.
- **Policies**:- Different policies regarding the product is also an asset like return policy, etc.

Threats:-

- **Theft**:- This is a serious concern in self-checkout stores. Without much supervision, customers can easily switch price tags or fail to scan some items.
- **Self-checkout System Malfunction**:- Attacker can easily access the self-checkout machine and do some malfunction to the machine for his benefit.

- **Customer Confusion and Equipment Issues**:- Sometimes customers are not able to find the right product in self-checkout if a product does not have a tag, the customer has to search for that product in the machine. Sometimes customer gets frustrated and does not buy that product and this will be a loss for the store.

Countermeasures:

- **Cameras**:- Store should have cameras covering every angle of the store which help in detecting any theft or suspicious activity.
- **Regular machine checkup:-** There should be a monthly checkup of self-checkout machines to confirm there is no malfunction in the machines.
- **Helpers:-** Some helpers should be standing around waiting to assist persons going through self-checkout. They will help the customer who is not able to do self-checkout.
- **Customer Satisfaction**:- The customer is the most important facet of any business. As the retail store manager, we need to ensure that the customer is our top-most priority. The customer should always be satisfied with the goods and services we provide.

Problem 3

Scenario: Self Destructive Messaging System

Assumptions:

- People with high-security clearance in the organization can access the system, but they must do so through a biometric or eye scan methodology.
- The attacker has a powerful technology that would allow him to fool the system into mistaking an intruder for an agent and record communications without the agent's knowledge.
- The attacker is aware that a cutting-edge system exists that would destroy the message after 5 seconds if it is opened, and he is also aware that he only has a limited amount of time to read the message and utilize it for his attack if it is opened.

Assets:

- **Confidential information**:- System has very sensitive information which will be a great loss for the organization if an attacker can access it.
- **Privacy**:- Organization has its privacy which is a big asset to the organization.
- **Computational power**:- All the computational power in the organization is an asset to the organization. Like information access mechanism hardware that involves biometric or eye scan verification.

Threats:-

- **Malware Attack**:- Attacker can intentionally cause damage to a system using malware and can manipulate or redirect the message.
- **Social Engineering attacks:-** An attacker might acquire access to the device that has this system installed by impersonating a friend.
- **Data poisoning attacks:-** Attacker can also inject as much bad data into a database as possible.
- **Dos or DDos attacks**:- By this attack, an attacker can shut down the system for some time.

Countermeasures:

- **Encryption:-** Everything is end to end encrypted provide more security to the system.
- **Firewall and antivirus:-** installing firewalls and antivirus in the system will help the system to defend against external threats.

Problem 4

Scenario: Managing personal network using the router

Assumptions:

- The attacker has enough computational power to perform attacks.
- The attacker might be able to access the router physically.
- The attacker knows how to perform all types of attacks on routers specifically session hijacking.

Assets:

- **Personal Information**:- Attacker can access the personal information of a user.
- **Identity**:- Attacker can perform identity theft or fraud which is a loss for the user.
- **Bandwidth**:- Attacker can use our network bandwidth for his work.
- **Router:-** Router itself is an asset, attacker(thief) can steal it if he can physically able to access it.

Threats:-

- **Session hijacking**:- This may occur if an attacker can insert falsified IP packets after session establishment via IP spoofing, sequence number prediction and alteration, or other methods.
- **Routing protocol attacks:-** When an attacker can forge RIP routing updates to a router to cause the router to forward packets toward the attacker.
- **Physical threat:-** If the Attacker can access the router physically, he can connect to a network without a password using WPS.

- **Botnet attacks**:- Botnets like Mirai target home routers, digital video recorders, and internet cameras and turn them into things that hack other machines and this is a self-propagating bot.

Countermeasures:

- **Update software regularly:-** Regular software updates are one of the most effective steps we can take to improve the overall security of our home networks and systems.
- **Use strong and unique passwords:-** Choose strong passwords to help secure our devices. Additionally, We should not use the same password with multiple accounts. This way, if one of your accounts is compromised, the attacker will not be able to breach any other of your accounts. Regularly update passwords.
- **Run up-to-date antivirus software**. A reputable antivirus software application is an important protective measure against known malicious threats. It can automatically detect, quarantine, and remove various types of malware, such as viruses, worms, and ransomware. CISA also recommends that all computers and mobile devices on our home network run antivirus software.
- **Install a network firewall:-** Install a firewall at the boundary of our home network to defend against external threats. A firewall can block malicious traffic from entering your home network and alert you to potentially dangerous activity.
- **Increase wireless security:-** We can also increase wireless security by using the strongest encryption protocol available, changing the default service set identifier, disabling Wi-Fi Protected Setup (WPS), reducing wireless signal strength, etc.
- **Physical security:-** Place the router in a locked room that is accessible only to authorized personnel, is free of electrostatic or magnetic interference and has controls for temperature and humidity.