HW1- Deep Ruparel

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

Assumptions:

- The people who have been thoroughly interviewed by the preparation team, have had background checks and have gained security clearance can be trusted with sensitive information.
- People without the security clearance like interns, part time helpers of the campaign and similarly people with low security clearances should have access to all the basic functions of email server, all the functions should be locked for them.
- All the emails are end to end encrypted and few emails containing sensitive information can be accessed by people with security clearance above a certain threshold.
- Attacker knows the team of the candidate running for the presential candidate and by doing a bit of research he can easily know which person in the campaign team has what type of security clearance and what he can target.
- Attacker has plethora of resources which allows the attacker to find backdoors in the current server, enough computational power to perform brute force attacks for password cracking etc.
- The attacker can have support from different nations, terrorist organization, opponent presidential candidate who can have a dedicated set of teams which could help the attacker to carry out the attacks.

Assets:

- Database which consists of all the emails, username, passwords, employee name, employee phone number, employee email id and similar employee information.
- Backup cloud which is backed up with all the new incoming emails every few hours to prevent the loss of information in case of an attack. It also backups the changes made about the employee information to have a copy of such changes.
- Dedicated databases are set up in two parts of the country one on the east coast and west coast, which contain the same information but allow to provide redundancy and to provide extra redundancy cloud servers are maintained in the country and some other continent as well.

Threats:

- Phishing attacks can be used to trick campaign workers into using their email credentials to login to the innocent looking website and when they do the confidential data can be achieved by the attacker.
- Social Engineering attacks can be used by the attacker to manipulate some members of the campaign in giving out their confidential information thus allowing the attacker to gain access to the email server and exploit it to the fullest.
- DDOS attacks can also be used by the attacker to temporarily disrupt the email server thus causing a delay in receiving and sending emails. This could lead to wasting the precious time and slow the campaign down.

Countermeasure.

- Installing of anti-virus, anti-phishing software on all the computers in the office to prevent falling into the trap created by the attackers.
- Organize workshops to educate the campaign workers against such attacks, how they can identify such attacks and what steps must be taken by them.
- Using dual factor authentication when logging into the email server to add an extra layer of security and prevent easy hijacking of the email accounts on the server.
- Making use of VPN when not accessing the server within the organization to encrypt all the traffic making it difficult for the attacker to get access to the information.

2) Scenario:
   - Managing twitter account for POTUS.

Assumptions:

- POTUS twitter account is very important account on twitter, any tweet shared by the account could provide critical information regarding the country, world to the people. On top of that, since twitter is very common messaging application it has a dense number of users and POTUS is very popular target. Hence protecting the account of POTUS is very important.
- Since this is a very important twitter account, people in the social media team of the POTUS are to be trusted only when all the team members are thoroughly interviewed and have successful background checks performed on them. Any other person should not be trusted.
- Attacker knows the location, username of the twitter account. Attacker also has knowledge of the security parameters of the twitter architecture. Attacker also knows the previous instances when twitter accounts were compromised and the way they were compromised.
- Attacker has resources which include systems with high computational power and also knows how to perform different sophisticated cyberattacks on different platforms. They might also have a dedicated teams which are financed by terrorist organizations, other countries etc.

Assets:

- Personal computers that are present in the White House out of which the POTUS twitter account is managed.
- People working in your team are also your assets because they might know some confidential information that the attacker can use.
- Password of the POTUS twitter account.

Threats:

- Backdoors that were previously exposed to attack twitter or newly found backdoors can be used by attacker to gain access to the account and post some unwanted tweets from the account causing panic among people.
- Social Engineering attacks can be used on the people in the management team to trick them into giving out some confidential information which can be useful to the attacker.
- Spear phishing attacks to get the password of the account can be employed by the attacker.

- Malware can that be downloaded on the computer which can collect information that is present on the computer out of which account is managed.

Countermeasures:

- Extra security measure like an additional otp or a password can be employed specially for the POTUS account. This provides extra security.
- VPN can be employed so that all the data is encrypted so that it is difficult for attacker to decipher it.
- Educating the people in the account management team about the different attacks which can be used, how to identify them and what you should do once under attack.
- Keep changing the passwords of the twitter accounts and all these passwords must be difficult to guess.
- Recording the audit logs and monitoring them to see if any unwanted user is trying to attack the account of POTUS.

3) Scenario:

- Making a self-destruct message system that deletes messages 5 seconds after they have been used.

Assumptions:

- Only agents belonging to a certain team can access system and in order to log in to the system they must perform a retinal scan which only when successful will allow them to gain access to the system.
- Attacker knows that such a state-of-the-art system exists which will delete the message when opened after 5 seconds and attacker knows that he has a limited time to access the message and make use of it for his attack once the message is opened.
- Attacker has a sophisticated system which allows he/she to confuse the system to identify an intruder as an agent, screen record the messages without the agent knowing. Attacker also has a set of dedicated teams to break into the system which may be funded by terrorist organizations, different nations etc.

Assets:

- A sophisticated hardware exists which is able to scan the retina and give access to the system, if fallen into the wrong hands it can have very dangerous repercussions.
- Database consists of all the information about the agents which is encrypted, it also contains the retinal scans of various agents which allows them to gain access to the system.
- A machine learning model which was used to train the system to build a accurate system which only identifies the retinal scan of the agent and all other unknown scans must be restricted.

Threats

- Social Engineering attacks to allow the attacker to gain the device which has this system implemented in it, this could be done by posing as a superior or a friend.
- Data poisoning attacks to allow the attacker to introduce innocent data into the machine learning model which has the wrong label. This will trick the system into letting attacker gain access to the system.

- Robbery could also pose as an attack in which the robber will steal the device from the agent and may sell it to people with malicious intentions.

Countermeasures:

- Make use of ciphertext which can be deciphered only the communicating parties which provides extra security even when the messages are being monitored by a malicious party.
- Make use of anti-screen recording software which will alert the user when someone is trying to record their screen, thus allowing the agent to know that anything henceforth from this point in the communication is compromised.
- We can keep an accurate count of the learning samples which are made used by the machine learning models so when an attacker will try to initiate data poisoning attacks by inserting innocent looking data with malicious label.

4) Scenario:
    - Netflix Recommendation System which recommends new shows and movies to watch based on user's prior watching history.

Assumptions:

- The users generated data like what the user clicked, what genre the user is watching the most, does the user complete the shows, movie they started watching. All this data is used to train the recommendation system to predict what should be presented to the user as his next watching options.
- The above data is very sensitive and if fallen into the wrong hands could be used to manipulate the users, so only members of the team responsible for applying machine learning on this data must be allowed access to this data, anyone else should not be allowed to access the data.
- The attacker knows there exists data records that can link a certain user and what they watch, so targeting these records could allow the attacker to promote the target items by maximizing the items that are recommended to the user such that there is a high ratio of target items included in the top k recommendations to the user.
- The attacker can only access a part of the training data, the attacker can control only a few users. The attacker does not know the details of the system like architecture, parameters to the model.

Threats:

- Data poisoning attacks such that attacker can recruit a bunch of controlled users to visit the target and select proxy items. This will inject fake data into the system, thus manipulating the system to recommend target data decided by the attacker.
- Phishing attacks to manipulate innocent users into thinking them that they are accessing the correct website where in real life they are actually on a fake website which looks similar to actual website and making them into giving their username and passwords. The attacker can then use these usernames and password to inject fake data and trick the recommendation system.

Countermeasures:

- Proper Authentication must be employed to check if the user does not have multiple accounts having the same email address because this would be a sign that this user maybe using all the accounts to manipulate the recommendation system.
- Two factor Authentication to protect the user account even when they fall prey to phishing attacks so the attacker cannot gain access to the account of innocent users and trick the recommendation system because the recommendation system would think all this clicks are generated by a genuine user and must be incorporated into the training of the system.