NAME: Abegain

SURNAME: Chauke

STUDENT NO: 230069509

Case Study

ZUUMER is a Video Conferencing company that allows anyone to have a meeting, workshop, interview, present class ONLINE in order to allow it's users to interact. ***ZUUMER*** has been downloaded more than one billion times throughout the world and has been widely used due to the lockdowns levels that are regulated throughout the world as a result of Covid-19 pandemic. Users should register for an account namely ***khomyunity*** account which allows a maximum of 80 users to interact with limited time of thirty minutes per session per day; or ***khomeshiyal*** account which allows companies or users to pay a monthly subscription fee with unlimited access to the platform. In the platform the host can record the session and participants consent to them being recorded once they join the meeting. There can be a maximum of four hosts in a session and hosts have administrative rights such as removing a participant, muting a participants, locking the session at a particular point, and many other administrative roles. The usage of platform is based on the acceptance of terms and conditions that are stipulated on the platform. Users can register themselves using their google, twitter, facebook, or Instagram accounts

Mr ***Khumalo,*** the Chief Information Officer have been receiving complaints from registered users about attacks or scammers that usually hack the sessions and require payment through ransomware in order to release the data from the sessions. Hackers usually look for open ports as well as personal information of the hosts which include names, surnames, telephone number, email addresses, companies where they work, location, and so on. Mr Khumalo has employed ***Puleng*** in order to look for vulnerabilities within the system so that they can improve it.

Section A (32 marks)

NOTE that ALL answers to these questions should be based on the SCENARIO!!! Answer ALL QUESTIONS!!!!!

1. What type of a hacker is Mr Khumalo narrating in the scenario and why? Provide enough reasons. (5)

   -It's a Black Hat hacker, because they break into meetings without permission. They use ransomware to lock people's data and ask for money. This shows they are doing it for selfish and illegal reasons, which makes them dangerous.

2. What type of a hacker is Puleng and why? (5)

   - Puleng is a white hat hacker because she was hired by Mr. Khumalo to help find problems in the system. She is using her hacking skills in a legal and helpful way. Her goal is to protect the system and make it safer for users.

3. In the scenario, it is mentioned that

   "Hackers usually look for open ports as well as personal information of the hosts which include names, surnames, telephone number, email addresses, companies where they work, location, and so on."

   Briefly discuss the hacking methodology/methodologies that is used by an attacker mentioned in question 2 above to infiltrate the system. HINT: *Out of all the methodologies that you have learned in the subject – there are ONLY two that are relevant to this case study – think carefully. It is up to you if you want to discuss two methodologies or one methodology – as long as you provide appropriate explanation.*

   (6)

   - Phishing - is when a hacker tricks someone into giving away personal or sensitive information by pretending to be someone they trust. In this case, the hacker may send fake emails or messages that look real to the hosts, asking them to click a link or provide login details, phone numbers, or company information. Once the hacker gets this information, they can access the session or system and use it to install ransomware or steal data.

- Malware - is harmful software that hackers use to damage or control a system. In this case, the hacker uses malware like ransomware to lock users' data and then demands payment to unlock it. The malware could be installed when a host clicks a fake link or opens an infected file, giving the hacker control over the session and stored information.

4. Session hijacking is the process of an unauthorised user gaining access to a connection between two clients or a client and server. Briefly discuss session hijacking techniques that Mr Khumalo and his team should be aware of. (12)

   - Session fixation – The attacker tricks a user into logging in with a known session ID. Once the user logs in, the hacker uses that same session ID to take control of the session.
   - Session sniffing – The hacker captures session data (like cookies or tokens) from the network using tools. This is possible if the connection is not encrypted.
   - Cross-site scripting – The attacker injects malicious scripts into the system. When a user clicks the script, it sends session details to the attacker.
   - Man-in-the-middle – The hacker secretly sits between the user and server, listening and possibly changing the information sent back and forth.

5. Would you say that the attacker in the scenario is a passive, active or hybrid attacker? Provide reasons for your answer. (4)

   - It is active attacker, because they are directly interfering with the system by hacking into sessions and demanding ransom to release data. They exploit weaknesses like open ports and target personal information to carry out their attack. This shows they are actively taking action to disrupt and control the platform, rather than just observing it.