DAY 9 hypothetical vulnerability on banking

Man-in-the-middle attack: Here, a fake website is created to get the attention of users to this website. Normally, the attacker is capable to trick the users by disguising their identity to make it appear that the message was coming from a trusted source. Once successful, instead of going to the designated website, users don't realize that they actually entered into the fraudster's website

Malicious hackers: It refers to those who breaks into computers without a proper authorization. They can include both insiders and outsiders. Hacking as an activity has become more prevalent after the advancement in connectivity among computers. This allowed hackers to access the computer victim's remotely. Hackers can break into computer systems or supporting equipments like switches or routers, and that could entirely damage the reliability of the network.

Guessing passwords: Using software to test all possible combinations to gain entry into a network.

Phishing attacks: With the massive quantity of personal information being kept by various institutions the protection of personal privacy became a big responsibility. Misuse personal details like social security numbers, driving license, bank accounts, etc. to conduct the fraudulent transactions.

Sniffers: It has also known as network monitors, this is software used to capture keystrokes from a particular PC. This software could capture login IDs and passwords.

Brute force: A technique to capture encrypted messages, then using a software to break the code and gain access to messages, user ID's, and passwords.

Worms: Destructive programs that replicate themselves without requiring another program to provide a safe environment for replication.

Logic Bombs: Designed to activate and perform a destructive action at a certain time. Internal attack

Fraud or theft: Computer software could misuse to conduct the frauds, which is normally committed by insiders who could be employees or persons having access to computer networks internally.

Back doors or trap doors: Typically a password, known only to the attacker, that allows access to the system easily without a problem with the security procedures.

Errors and omissions: The integrity of information systems and data could be threatened due to errors and omissions, which is usually occurring during the capture of data.