Name: Deep Salunkhe.
Roll No: 21102A0014

Assignment - 6 (OBT)

D D M M Y Y Y Y

Q1] Compare Phishing, smishing, and vishing

⇒ Phishing: This is a type of cybercrime where attacker send fraudulent emails or messags, often posing as legitimate entities, to trick recipients into revealing sensitive information like password.

Smishing: A variation of phishing, smishing involves sending fraudulent text messags to trick recipients into clicking on malicious link. or providing personal information.

Vishing: Similar to phishing and smishing, vishing involves voice calls to deceive victims into revealing sensitive information. Attackers may pose as bank representative, government officials, or other trusted entities.

Q2] List different types of attacks on mobile device. Explain anyone in detail.

⇒ Malware: This includes viruses, worms, trojans and. spywares that can infect mobile devices and data.

Phishing/smishing: These attack user through fraudulent messags and calls sideloading : This refers to the practice of installing apps from source other than official app store, which can expose devices to malware and vulnerabilities

sim swapping : In this attackers trick mobile carries, into transfering a victims phone number to a new SIM card, allowing them to intercept calls and messags.

Malware Attack.

A common malware attack on mobile devices involves the installation of malicious app. These apps may appear legitimate but contain hidden code that can steal personal data, track user activity or even take control of the device. Once installed the malware can silently collect sensitive information and send it to the attackers

Q3] How do criminals plan cyber attacks? Elaborate each step briefly.

⇒ Cyber criminal typically follow a structured approach when planning and executing attacks:

① Target selection: They identify potential victims or organisation based on factors like vulnerability, value of data and ease of attack.

(2) Research and Reconnaissance : They gather information about their targets, including network infrastructure, security measures and employee behaviour

(3) Exploit identification: They search for vulnerabilities in the target system or networks that can be exploited to gain unauthorized access

(4) Attack vector Selection: They choose the most effective method of attack, such as phishing, malware, or social engineering

(5) Attack Execution: They launch the attack often using automated tools or scripts to maximize efficiency

(6) Data. Exfiltration: If successful, they steal sensitive data or take control of the target's system.

(7) Cover-up & Persistence: They attempt to conceal their tracks and maintain access to the compromised system for future attacks

aa] Explain social engineering vith the help of example

⇒ social enginering is a technique used by attackers to manipulate individuals or organizations into revealing sensitive information or performing action that benifits the attackers. It relies on human psychology and trust to deceive victims.

Example: Phishing Email.

A common social enginering tactic is the phishing email. Attackers send email that appear to come from legitimate sources, such as bank or online retailer, urging recipients to click on malicious link or open attachment. These messages often contain a sense of urgency or fear, prompting to act without caution. By clicking on the malicious link, victim may be redirected to take to a fake website, where they are asked to enter their personal information.