Name: Deep Salunkhe, Rollab: 21102 A0014
smishing, and vishing
age Dam Course as
type of gresorine where attacker advent emails or messags, often
legitimate entities to trick
legitimate entities, to trick into revealing sensitive information like
a mentered statement or menter
1 m/2 cun o of man of the
s alles tyrotai
fraudulent text messages to toick
traudulent text message to brick
I into chickly on maliciow link.
ling personal information.
the installation at malicinus
alatas tod stambing leanage
six calls to deceme virtims into sentire information. Attackers may
sia calls to deceme victims into
sentire information. Attackers may
The state of the s
musted entitles
an the do coiminals plan copia
attacks and lider of 1

Assignment - 6 (OBT) Compare Phicking, Phishing This is a posing as password Smishing: A variat sending recipient involves vo revealing or other List different types of attacks on mobile dense anjone in detail. Malware: This includes wrutes, worms, trojons and. spy wons that an infect mobile devices and data Phishry Is miling: These attack your through foundulest messages



sidelanding: This refers to the prozective of installing apps from source other than official, app store, which can expose deviau to malwax. and unlnerabilities

Sim swapping: In this attackers trick mobile corres,

10to transferring a victims whom number

to a new SIM lard, allowing them to

intercept calls and message.

Molwase Attack.

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

O3] How do criminals plan cyber attacks? Flobosate each

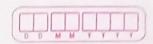
when planning and executing attacks:

(i) Target selection: They identify potential victims or organisation based on factors
like vulnerability, ralm of data and



- e Research and Reconnaissance: they gother information about their targets, including network information, security measures and employed behaviour
- 3 Exploit identification: They search for vylnerabilitis in
 the target system or networks
 that can be exploited to goin unauthorized access
- @ Attack rector Selection: They choose the most effective method of attack, such as phishy, malware, or social engineering
- B) Attack Execution: They launch the attack often using automated tools or scorph to maximize efficienty
- @ Data Exfiltration. If successfull, they steal sonsitive data or take contoad of the toogo's Stelle
- P Corex-up & Pers Wterm: They often pt to sonced. Here.

 tracks and mountain rough to
 the compromised system for future attacks



as Explain social engineering with the help of example

social engineery is a technique use, by attackers to manipulate individuals or organizations into severality sensitive information or performing action that benitis the attackers. It relies on human psychology and tout to deceive victims.

Example: Phishy Fmail

A common social enginery tactic is the phishy remail.

Attackers send email that appear to come from legitimate escapely, such as bunk or oblin retailor, using recipients to dick on malicious linic or open attachment. There messages often contain a sense of using or feer, prophy to act silver courtion. By clicking on the malicipus linic, victic, may be dedirected to take the a fake websit. When they are asked to onter their persons.