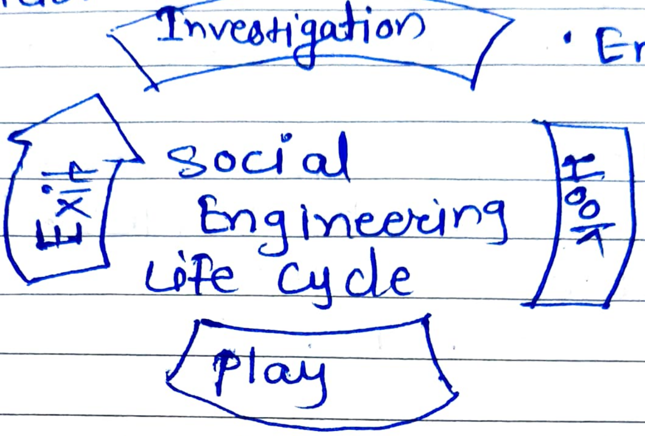
Preparing ground For attack
- Identifying the victims(s).
- Gathering background info.
- Selecting attack method(s).

Closing interaction, ideally without arousing suspicion:
- Removing all traces of malware
- Covering tracks
- Bringing charade to

Deceiving victim(s) to gain foothold :
- Engaging target
- Spinning story
- Taking control of interaction



Obtaining Info. over period of time:
- Expanding foothold
- Executing attack
- Disrupting business / and siphoning data

Social Engineering attack lifecycle

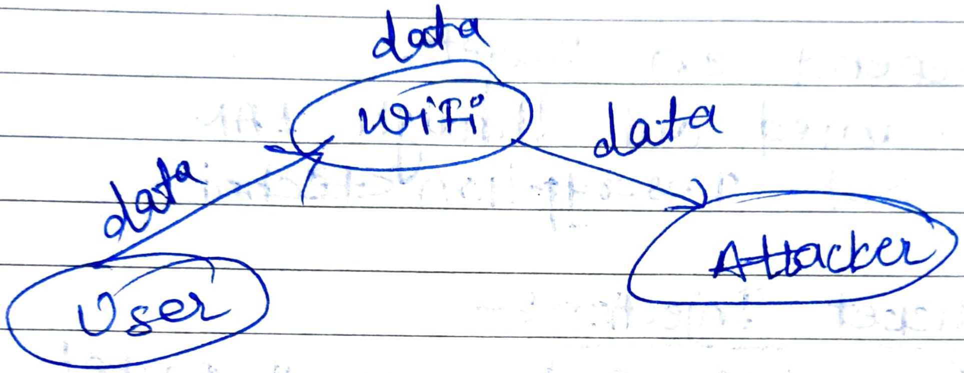
MAN-In-The-Middle-Attack :-

- Attacker secretly relays and possibly alters the communication betn 2 parties who believe they are directly communicating with each other.

Types:

1. Rogue Access Point
2. ARP Spoofing
3. mDNS Spoofing
4. DNS Spoofing

① Rogue Access Point



② ARP Spoofing

- MAC address change with other's MAC address

192.168.1.1 xx : xx : xx : 01 (Router)
IP Add. mac ID

192.168.1.1 xx : xx : xx : 02 (Attacker)

③

- ping google.com
172.217.160.142 IP Address of google

spoofed IP address → 192.168.1.10

document.cookie

CDN
content
Deleivery
Network

Microsoft
Baseline
Security
Analyzer

Page No.
Date.: / /

Techniques:-

1. Sniffing
2. Packet Injection
3. Session Hijacking
4. SSL Stripping

(1) Sniffing

- Depend on target.
- Carried out through LAN
- SSL Descryption ~~Techni~~

(2) Packet Injection:-

- Inspecting each & every packet

Defense:-

1. Strong WEP/WAP Encryption on Access Points
2. Virtual Private Network
3. Force HTTPS
4. Public Key Pair Based Authentication