## **----------------------------------------------------------------------------Social Engineering-------------------------------------------------------------------------**

## 

## **# Basic**

## **\*\*Social engineering is an act of stealing information from humans. Its a mind manipulation technique.\*\***

## **- No interaction with target system or network**

## **- Non-technical attack**

## **- Convincing the target to reveal information**

## **- One of the major vulnerability which leads to this type of attack is \*\*Trust\*\*.**

## **- User trust in another user and does not secure their credentials from them.**

## **- Employees are uneducated at organizations, so this is a major vulnerability.**

## **- Lack of security policies and privacy are also vulnerable.**

## 

## **# Phases in Social Engineering**

## **\*\*Research\*\***

## **- Collection of information from the target organization**

## **- Collected by dumpster diving, scanning, search on the internet, ...**

## **\*\*Select target\*\***

## **- Select the target among other employees**

## **- A frustrated target is more preferred**

## **\*\*Relationship\*\***

## **- Create relationship with the target**

## **- Earn the trust**

## **\*\*Exploit\*\***

## **- Collecting sensitive information such as usernames, password, etc...**

## 

## **# Types of Social Engineering - SE Attacks**

## **\*\*Human-based Social Engineering - SE\*\***

## **One-to-one interaction with the target. Earn the trust to gather sensitive information from the target.**

## **\*\*\*Eavesdropping and Shoulder Surfing\*\*\***

## **- Eavesdropping is a technique in which attacker is revealed information by listening to the conversation.**

## **- Reading or accessing any source of information without being notified.**

## **- Shoulder Surfing is a method of gathering information by standing behind the target.**

## **\*\*\*Dumpster Diving\*\*\* --->**

## **- Looking for treasure in trash.**

## **\*\*\*Piggybacking and Tailgating\*\*\***

## **- Piggyback is a technique in which attacker waits for an authorized person to gain entry in a restricted area.**

## **- Tailgating is a technique in which attacker gains access to the restricted area by following the authorized person.**

## 

## **\*\*Computer-based Social Engineering\*\***

## **\*\*\*Phishing\*\*\***

## **attacker make fake page like facebook ,instagram and etc. and when any people go to the link and try to log in**

## **they will redirected to the original page of website and we get the log in details like username ,email and password.**

## **\*\*\*Spear Phishing\*\*\* --->**

## **Similar as phishing but in this we can target our friends and relatives through the call, msg and email and coveince**

## **them to open link and log in with the like when they try to log in we get the log in credentials. (phishing with already known**

## **people like friends ,relatives)**

## 

## **\*\*Mobile-based Social Engineering\*\***

## **\*\*\*Publishing Malicious Apps\*\*\***

## **These applications are normally a similar copy of a popular application.**

## **\*\*\*Repackaging Legitimate Apps\*\*\***

## **Repack a legitimate app with a malware.**

## 

## **\*\*Insider Attack\*\* --->**

## **Social Engineering is not all about a third person gathering information, it may be an insider with privileges.**

## 

## **\*\*Impersonation on Social Network Sites\*\***

## **\*\*\*Social Engineering Through Impersonation on Social Network Sites\*\*\***

## **- Attacker gathers personal information of a target from different sources mostly from social network sites such as full name, date of birth,**

## **email address, residential address, etc.**

## **- After gathering the information, the attacker create an account that is exactly the same. Then introduced to friends, group joined by**

## **the target to get updates or convince the target's friends to reveal information.**

## 

## **\*\*Identity Theft\*\***

## **- Stealing the identification information of someone**

## **- Popularly used for frauds**

## **- Prove the fake identity to take advantage of it**

## 

## **# Countermeasures**

## **\*\*Secure sensitive data\*\***

## **Store Data at rest in a secure manner (Use Encryption ). Don't share Sensitive info/Documents with everyone.**

## **\*\*Physical security\*\***

## **Who has access to Physical records (Data), who has access to sensitive areas (Server room, Admin block, Data Centres), and how you ensure that Physical security.**

## **\*\*Least privileges\*\***

## **Assign least Privileges to Employees/User.(Low Permissions)**

## **\*\*Strong policies\*\***

## **Password Policies, Access Policies, Device Controls, etc.**

## **\*\*Training\*\***

## **Train your Employees for popular and new S.E Attacks.**

## 

## 

## **# Tools**

## 

## **SET (Social Engineering Toolkit) -->**

## 

## **- https://github.com/trustedsec/social-engineer-toolkit**

## **- ./setoolkit**

## **- now select 1. Social-engeering attack**

## **- now select 2. web attack vectors**

## **- select 3. Credentials harverster attack method**

## **- select 2. site cloner**

## **- now type url (facebook.com, instagram.com)**

## **- now type your ip in browser and you get the page now try to login and we got the credentials in our tool**

## 

## **BlackPhish -->**

## **- git clone https://github.com/iinc0gnit0/BlackPhish**

## **- cd BlackPhish**

## **- ./install.sh**

## **- sudo python3 blackphish.py**

## **- select platform which you want to use (Instagram, Facebook, google, netflix and etc.)**

## **- select localhost.run**

## **- give website which you want redirected (like www.google.com, www.facebook.com and netflix.com)**

## **- now you see username and password**

## 

## **Zphisher -->**

## 

## **Localhost: -->**

## **- link = https://github.com/htr-tech/zphisher**

## **- start tool = ./zphisher.sh**

## **- select your method i will select 6 then select 1 for localhost for same network || select 3 after 6 for if your target is in other network**

## **- now you get local ip with port you get the phishing page at this ip**

## **- now try to login**

## **- now you see login credentials in tool**

## 

## **Outter from network**

## **- start tool = ./zphisher.sh**

## **- select your method i will select 1 then we select 3 for fake security login page then select 3 for cloudfared**

## **- now we got 2 links and select any one and send it to your target and when our target try to login we got the credentials in our tool**

## 

## 

## 

## **horizontal line**