**Name : Shaik M. Bilaldeen**

**College : Annamacharya Institute of Technology and Sciences, Tirupati**

**Branch : E.C.E**

**ASSIGNMENT-3**

**Case Study Analysis:**

* ***Social Engineering*** is the type of manipulative attack that is used on the human beings in order to impersonate them and to theft their **PII (PERSONAL IDENTIFICATION INFORMATION)** in order to gain the access to the server which results in data breach and the breach security is so important to avoid these type of security threats.
* This type of security threats are happened when the organizations have vulnerabilities like
  + ***Lack of employee awareness training***: Employees with insufficient training and unaware about the required skills to detect and detect the threat leads to a massive threat
  + ***Inadequate authentication measures***: The organization or an individual must have to ensure multiple number of authentications in order to eliminate these type of threats at least anyone of these authentications.
  + ***Poor email security protocols*** : The poor email security protocols makes the whole organization to receive unwanted and threaten emails often, if anyone of the employee accidently clicked then everything goes wrong.
* The attack on the ***organization’s reputation, financial losses*** and ***customer trust*** these three are interconnected because an attack will be performed on a organization to demolish its reputation, the organization will see financial losses which was a cause of the decrease in the customer trust.
* The organizations are recommended to give proper training to their employees in order to detect and defend these types of threats ,they are required to get acquire the knowledge about the adopting multi-factor authentication and email filtering systems etc.

**Tactics and Statistics:**

* The threat actors uses various types of tactics and statistics in order to perform an attack on a victim the listed below are some of them
  + ***Authority exploitation :*** The threat actors uses the strategy that the mail is from the higher official who has the authority and impersonating in the name of authority attacks takes place and the employee will not able to disobey the orders from the higher official
  + ***Urgency or familiarity :*** The threat actors attacks the victim by creating the situation in which the victim feels like its very important/urgent and another situation which feels like very familiar and looks like legitimate to access the mail.
* The victim has to aware of these type of threats and must have the knowledge to detect and defend these type of threats and also have the communication skills in order to reach the persons who mailed those in order to get acknowledge
* The victim have to use some tools to mitigate the risk causing by these type of threats, by using strict verification protocols for sensitive information requests like “Firewall” and fostering a culture of security awareness within the organization we can mitigate the risks.

**Phishing Email Analysis:**

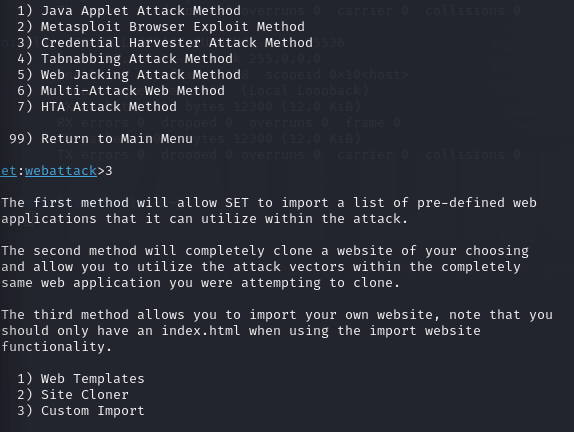
* The Phishing emails consist of red flags such as misspelled words, using formal language in the mail, addressing the victim without their name, requests for sensitive information which can leads to a mere threat but these all can be seen in the legitimate way.
* They tricks the human beings by using psychological factors like creating a curiosity, fear, intimidation, in order to don’t go in-depth analysis for the mail. They simply manipulates the human.
* The victim has to know about the strategy for detect and defend these type of security threat by keenly observing the email headers, misspelled words, requesting for sensitive information and taking preventive measures against phishing attacks

**Exploitation:**

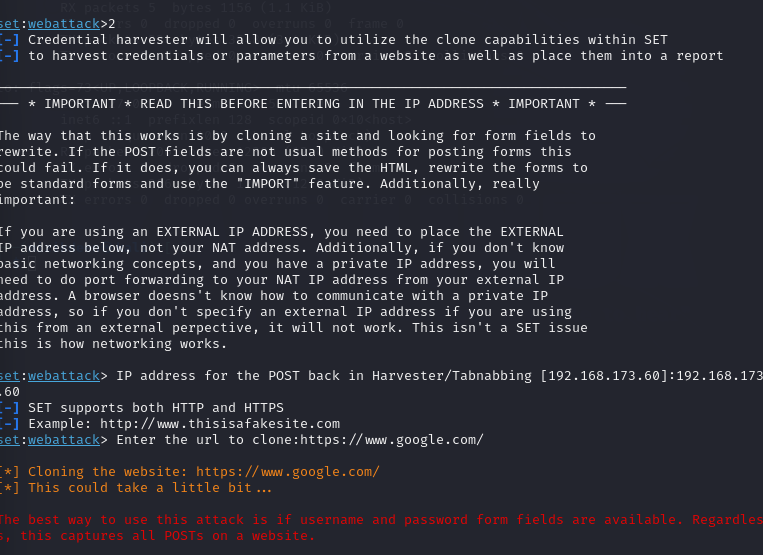
* The exploitation of the phishing can be done in two ways
  + By using commands
  + By using in-built tools in kali-linux
* Here I used in-built tool called ***SOCIAL ENGINEERING TOOL*** from the kali-linux in order to exploit the phishing.
* Under user, root type **“setoolkit”** to start the tool and it appears like as shown in the figure below.



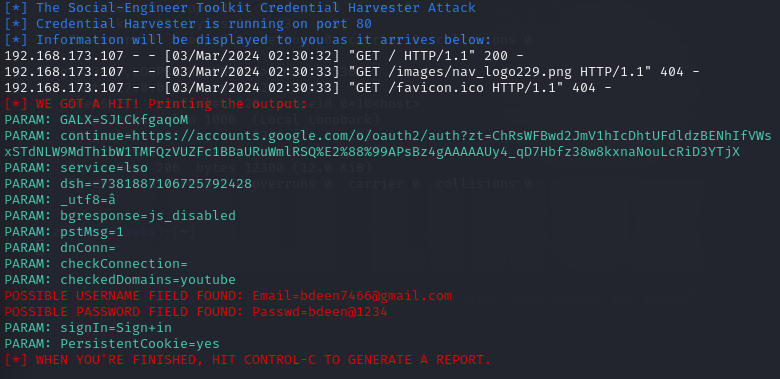
* Type “1” and press enter to perform ***“social engineering attacks”,*** then the interface appears as shown below



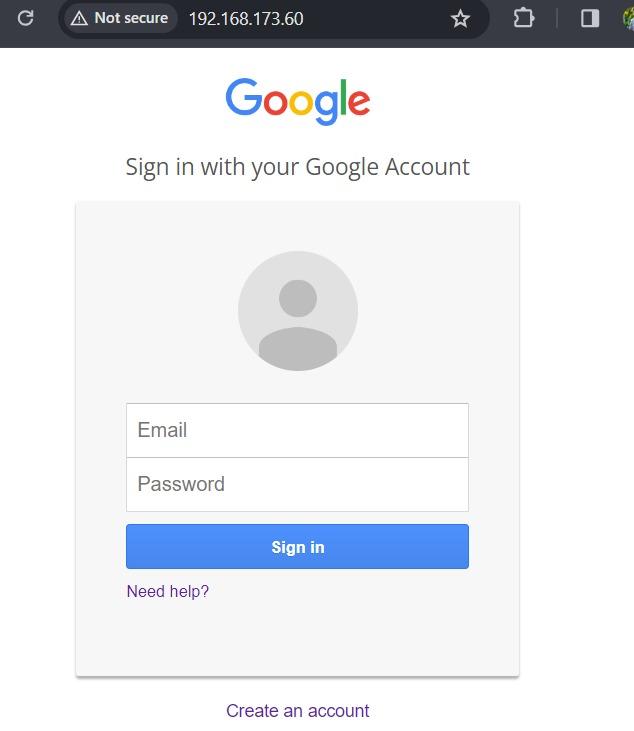
* Initially, we have to type 3 to perform ***“Credential Harvester Attack Method”***in order to gain the credentials of the victim in order to access them. After that it asks for the options to be selected from those we select option 2 in order to choose ***“Site Cloner”.***



* We have to give the ip address on which the victim browse for the phis and got attacked here I gave 192.168.173.60 as the ip address. Then, we have to give the url of the website that has to be copied and we have to wait for the cloned url to be launched and to accessed by the victim.



* We can able to see the victims log details and the ip address of the victim also the username and password credentials of the victim on surfing through the login page shown below.
* The exploitation can be seen as shown below



* In this way exploitation of phishing takes place.