CS6345-DIGITAL FORENSICS

ASSIGNMENT 3

STAGE-1

Ravi Sankar Gogineni-R11788968

Phishing attack on Hotmail email:

To send a phishing email to a Hotmail account,

first, we need to **create a URL** and

the second is to **send an email** to the target Hotmail email.

**Creating a URL**:

**Step-1:**

Installing Social Engineering toolkit:

We need to setup The Social Engineering Tool Kit. The command to install is as follows:

sudo apt install set

Text

Description automatically generated

**Step-2:**

Display of first menu:

After the installation of the toolkit, it displays a screen where we need to select the option from a menu. The menu options are as in the following screenshot.

Text

Description automatically generated

**Step-3:**

Selection of an option from the menu:

We select the option 2 from the menu displayed, which is Website Attack Vectors.

Text

Description automatically generated

**Step-4:**

After selecting option 2 from the menu above, it redirects to the menu below.

Text

Description automatically generated

**Step-5:**

Now from the menu above, to create a browser URL, we select the option 3 which is Credential Harvester Attack Method.

Text

Description automatically generated

**Step-6:**

After selecting option 3 from above, a menu is displayed. In the menu, we opt for option 1 which is Web Templates.

This method allows one to import their own website. It allows us to send the URL later.

Text

Description automatically generated

**Step-7:**

After selecting Option 1, the following IP address is displayed on the screen. The screenshot is as shown below:

Text

Description automatically generated

**Step-8:**

After that, we click on enter. Another popup menu is displayed as shown below:

Then it asks for an option to be selected.

The menu has the following options- Java Required, Google, Twitter.

We select option 2, which is Google.

Graphical user interface, text

Description automatically generated

**Step-9:**

After opting for the Google in the above menu and entering the IP address from step-7 (10.0.2.15), it redirects to another screen as shown in the below screenshot:

Graphical user interface, text, application

Description automatically generated

In the above screen, when someone try to enter their login credentials in the email and password slots, the information entered by the user will be displayed in the screen in step- 8. The screen where the login information(email and password) appears is shown below:

Graphical user interface, text

Description automatically generated

**Sending an email using the created URL:**

Phishing attack on the target Hotmail email:

Now, we need to send an email with URL to the Hotmail of provided assigned team. This can be done as follows:

**Step-1:**

Open the terminal same as in step-1 of the above process i.e., The Social Engineering Toolkit.

The below screen appears where a menu will be displayed:

Text

Description automatically generated

In the menu above, we select option 5 which is Mass Mailer Attack. This will display the menu as shown in the below screenshot. It prompts 2 menu options in which, we select the option that needs to be done. We select single email attack for a Hotmail email. So, we select option 1.

Graphical user interface

Description automatically generated

Step-2:

After selection option 1(E-mail attack single email address), we then enter the email address of the target Hotmail email of the assigned team.

Graphical user interface

Description automatically generated

We also need to select an option, in the same step as shown in the screenshot below. We select option-1 which is Use a Gmail Account for your email attack.

Graphical user interface

Description automatically generated

**Step-3:**

After entering the email that we use to send the phishing email. The following will be prompted by the command.

Text

Description automatically generated

* The FROM NAME the user will see:

This is the from address/name that the receiver of the URL email will see. The text we gave for this is :

**Google Support**

**Text

Description automatically generated**

* Email password:

We need to enter the email and password of the Hotmail email that we use for the phishing purpose.

Text

Description automatically generated

* Flag this message as high priority?

In this instance, we opted for high priority. So, we selected yes for the same purpose.

Text

Description automatically generated

* Do you want to attach a file:

Since, we didn’t want to attach any files with the email, we selected n for the same.

Text

Description automatically generated

* Do you want to attach an inline file:

Also, we don’t need any inline files. So, we select n for the purpose.

Text

Description automatically generated

* Email subject:

Now, it asks for the subject of the email we are about to send. We entered the following

**Your Google account has been hacked kindly change the password**

Text

Description automatically generated

* Send the message as html or plain? ‘h’ or ‘p’:

We want to send the email as a plain text. So, we select p and click enter.

Text

Description automatically generated

* Enter the body of the message:

The body of the message we entered is as follows:

**Hello Sudhattu,**

**Your account has been hacked due to a breach,**

**Kindly change the password using the link given below**

**http://10.0.2.15/**

we type END and click enter to end the typing if the message we entered.

Text

Description automatically generated

After we END the body of the message and click enter, we receive a text that says, SET has finished sending the emails.

Graphical user interface, text, application

Description automatically generated

After this step, we are done with the phishing email attack on the given Hotmail email.

The email we entered in the above process must receive an email stating that their google account has been hacked and prompted to click on the given URL.