Lab 2 - Social Engineering Attacks

Disclaimer

This lab is for educational purposes only. We are not responsible for how you use these tools in any way, shape or form. These tools are very powerful and can cause a lot of damage to systems. Who carries out unauthorized social engineering attacks may be prosecuted.

Social Engineering Attacks

Social engineering is the term used by cybersecurity professionals for describing a wide range of exploitative behaviours. Such attacks use psychological manipulation and confidence tricks to create security risks, including compromising systems and the exfiltration of data. Attacks in social engineering occur in one or more steps, some of which we will present in the exercises below. First, we must check that your system is prepared for the task.

Preparation

Your PC

This lab will be presented in a tutorial format. Students are free to observe only or follow along as they choose. If you intend to follow along then please start by ensuring that your PC has virtualisation enabled. This should still be the case from the previous Lab and the coursework, but if you need to revisit something then please consult the video tutorial provided. This is "Virtualisation & Command line basics" on the course wiki:

https://secure.ecs.soton.ac.uk/noteswiki/w/COMP6224-2223

Software

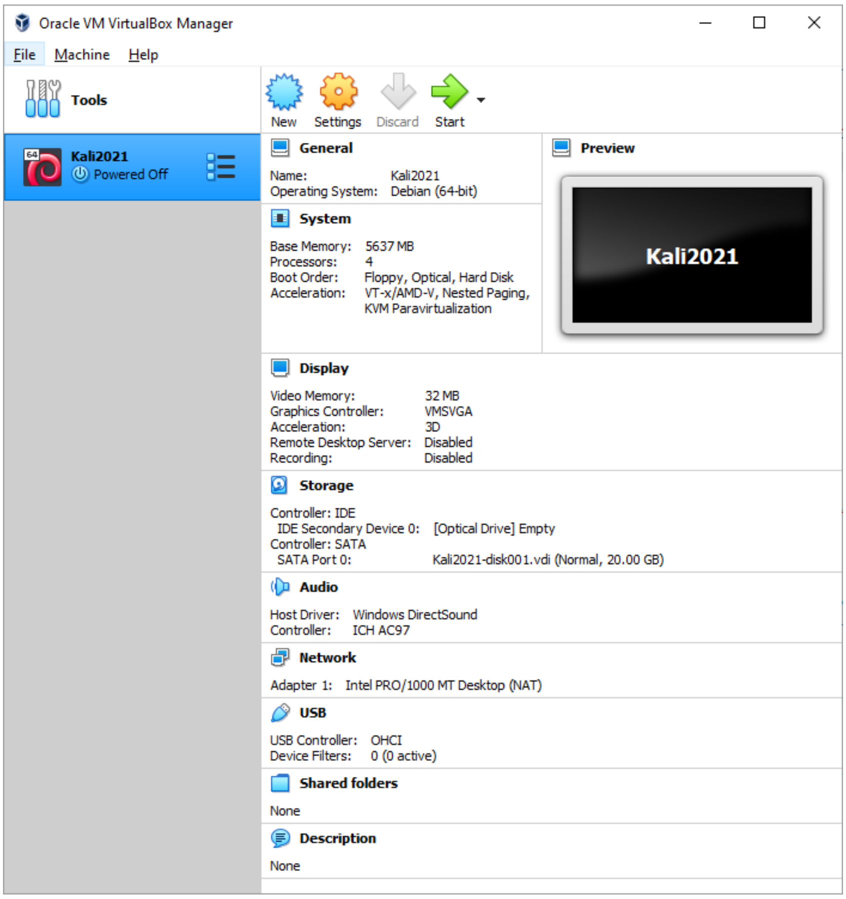
You can download the software, called VirtualBox, from here: virtualbox.org. Please download the correct version for your operating system and install it.

Setting up the Environment

For the following series of exercise, we will use a Kali Linux Virtual Machine (VM) which you can download here: https://software.soton.ac.uk/software/128 Please download "Kali-2021" and use this VM only, but **do not update it** even if prompted to do so! Make a note of where you saved the OVA file on your machine.

Import the VM in VirtualBox

Open VirtualBox, click on "file" and then on "import appliance". The virtual machine should now be ready to go as shown below:



General

Name: Kali2021
Operating System: Debian (64-bit)

System

Base Memory: 5637 MB
Processors: 4
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display

Video Memory: 32 MB
Graphics Controller: VMSVGA
Acceleration: 3D
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Kali2021-disk001.vdi (Normal, 20.00 GB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders

None

Description

None

Run the VM and Login

To run the VM just double click on its name, then wait a second or two and log in when prompted. **The username is root, while the password is foundations**.

Tips:

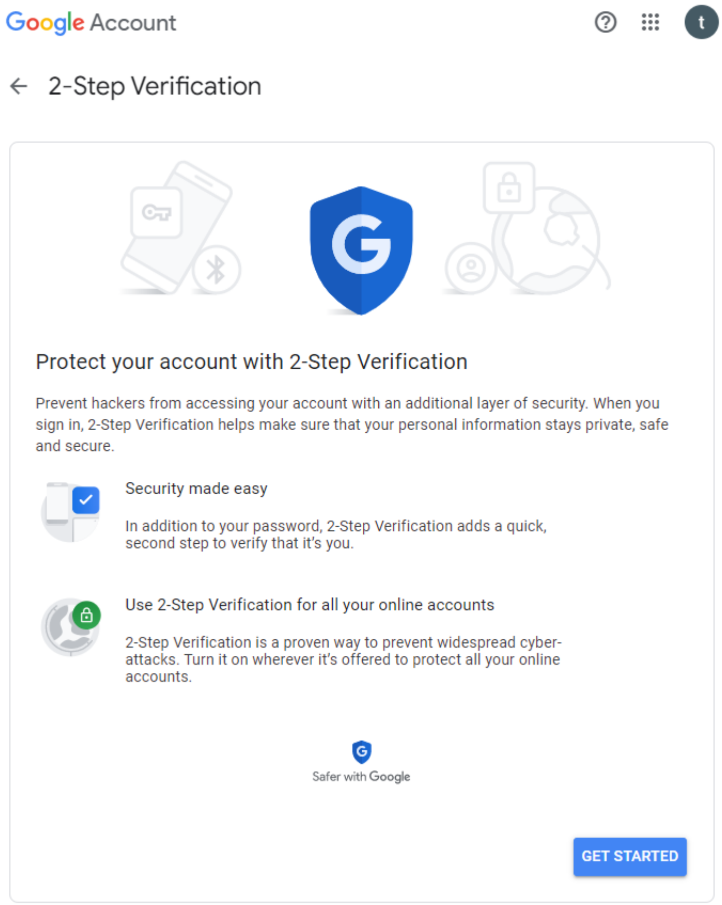
- If your mouse appears stuck inside the screen containing the virtual machine, simply hit the right Ctrl button to undo this.
- If you have the window containing the VM as the active window on your system and you hit the PRTSC button then the screenshot will be saved to the Pictures folder on the VM. If not, then the screenshot will be on your host system (Windows or Mac) and treated accordingly.
- Do not update the VM.
- If you copy and paste a command into the command line and it does not work,

try typing it out by hand.

- If you are unsure about a command, you can always use the "help" and "man" commands to find out more. Please refer to Tutorial 4 for more on this.

Gmail

To complete this lab, you will need to send a phishing email for which we will need a Gmail account specifically. We recommend creating a new Gmail account just for this task even if you already have one. You also need to activate 2nd-Step Verification on this account to setup an app password. Please login to your new Gmail account and then go to https://myaccount.google.com/signinoptions/two-step-verification/enroll-welcome in a new tab. Then follow the instructions to activate 2-Step Verification:



Protect your account with 2-Step Verification

Prevent hackers from accessing your account with an additional layer of security. When you sign in, 2-Step Verification helps make sure that your personal information stays private, safe and secure.

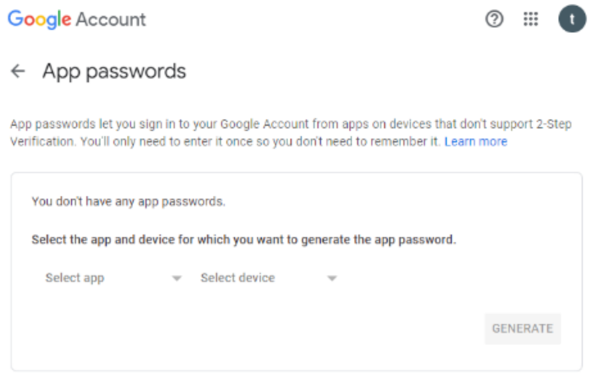
Security made easy

In addition to your password, 2-Step Verification adds a quick, second step to verify that it's you.

Use 2-Step Verification for all your online accounts

2-Step Verification is a proven way to prevent widespread cyber-attacks. Turn it on wherever it's offered to protect all your online accounts.

After you activated 2SV, please go to https://myaccount.google.com/apppasswords in a new tab and generate an app password:



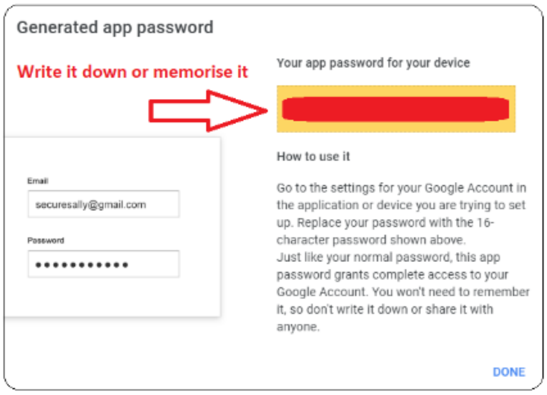
Google Account

← App passwords

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. Learn more

You don't have any app passwords.

Select the app and device for which you want to generate the app password.



Generated app password

Write it down or memorise it

Your app password for your device

[redacted]

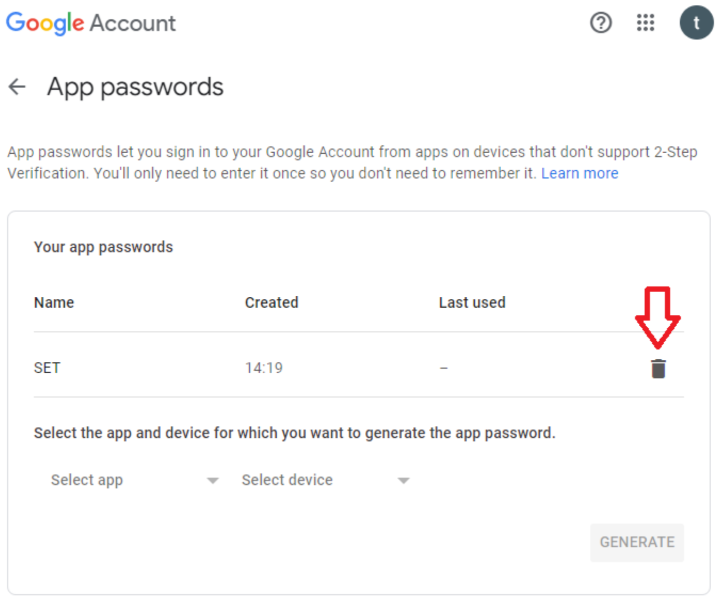
How to use it

Go to the settings for your Google Account in the application or device you are trying to set up. Replace your password with the 16-character password shown above.
Just like your normal password, this app password grants complete access to your Google Account. You won't need to remember it, so don't write it down or share it with anyone.

Email: securesally@gmail.com

Password: ●●●●●●●●●●●●

You need to write the app password down or memorise it for the rest of the lab. You can generate more app passwords as you wish but you may want to remove the app password(s) at the end of the lab:



Google Account

← App passwords

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. Learn more

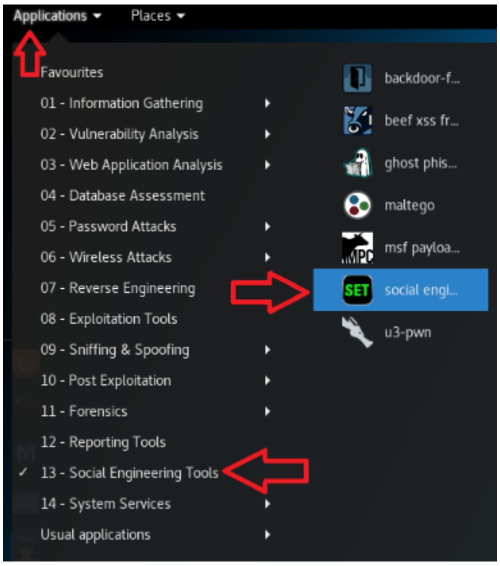
Your app passwords

Name	Created	Last used
SET	14:19	–

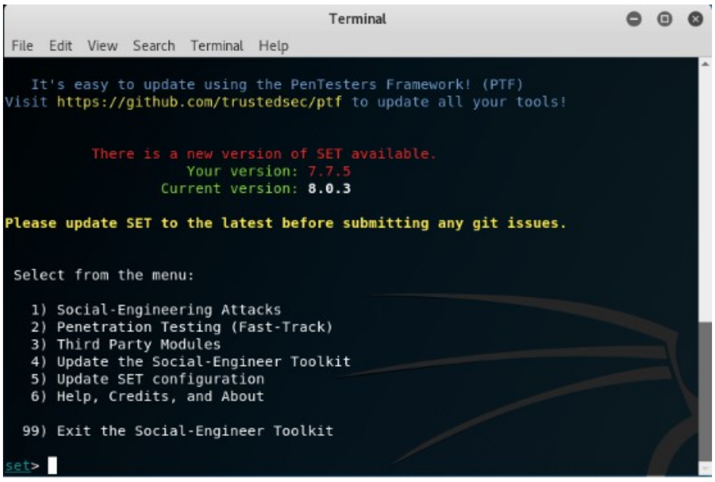
Select the app and device for which you want to generate the app password.

Social Engineering Toolkit (SET)

In this lab, you will learn how to setup a fake Twitter's login page and subsequently, how to use this fake webpage to steal a target's credentials by way of a phishing attack. The webpage setup and distribution of emails are both automated, but the structure of the email you send out is not. Although you need to understand the logic of this process, your primary input will be thinking about what makes an email believable and what tricks users into clicking on fake emails. We will use the **Social Engineering Toolkit (SET)**, which is already installed on Kali Linux, to conduct the exercises in this lab. SET is menu-driven and aimed at exploiting the human element of security. You can run SET by choosing it from the Applications Menu in Kali Linux as illustrated below.



Once you click on the SET toolkit, it may ask you to accept terms and conditions. Thereafter it will open with the options shown in the following screenshot:



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


          There is a new version of SET available.
                    Your version: 7.7.5
                 Current version: 8.0.3

Please update SET to the latest before submitting any git issues.


 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>
```

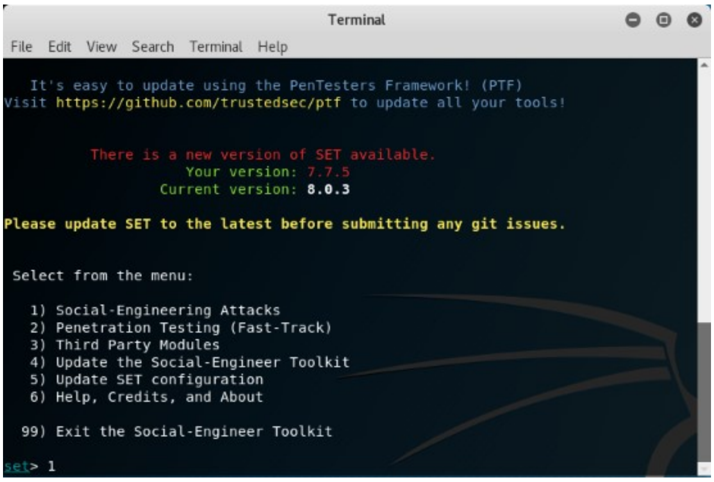
Exercise 1: Fake Twitter's Login Page

In this step, we will setup a fake Twitter's login page and test the fake webpage.

Site Templates from SET

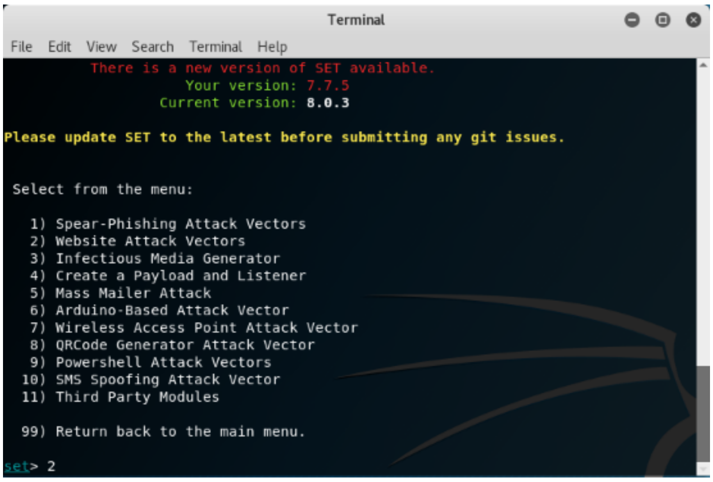
Please perform the following steps:

Select **1) Social-Engineering Attacks** to receive a listing of possible attacks that can be performed.



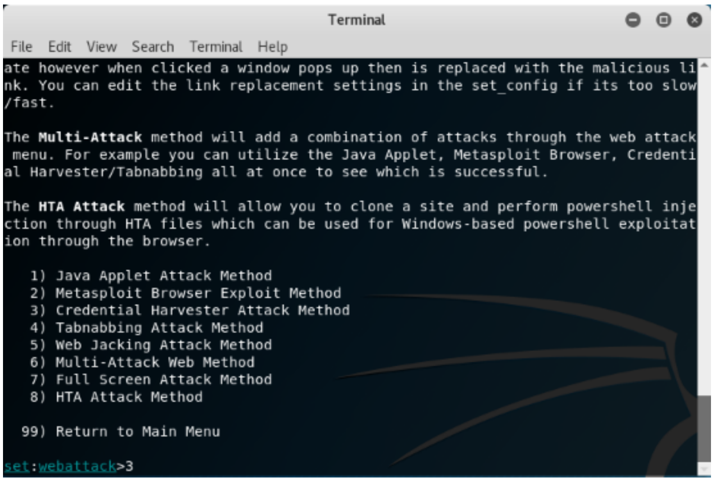
```
   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


          There is a new version of SET available.
                     Your version: 7.7.5
                  Current version: 8.0.3

Please update SET to the latest before submitting any git issues.


 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
```

Now select **2) Website Attack Vectors**.

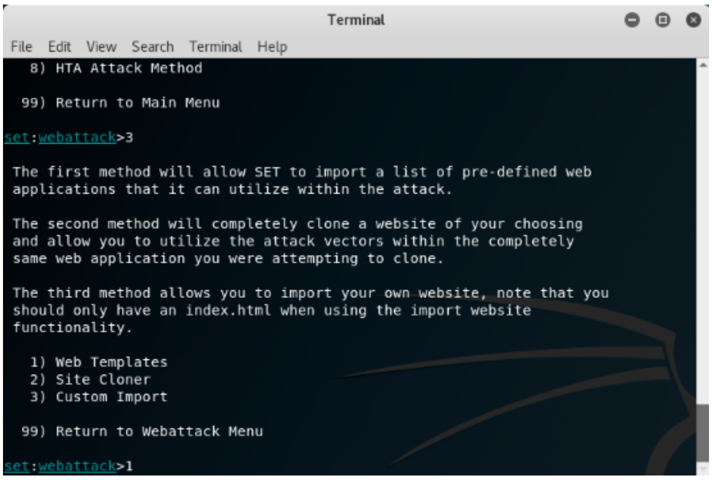


```
          There is a new version of SET available.
                     Your version: 7.7.5
                  Current version: 8.0.3

Please update SET to the latest before submitting any git issues.


 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) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 2
```

We will take a look at the third option, **3) Credential Harvester Attack Method**.



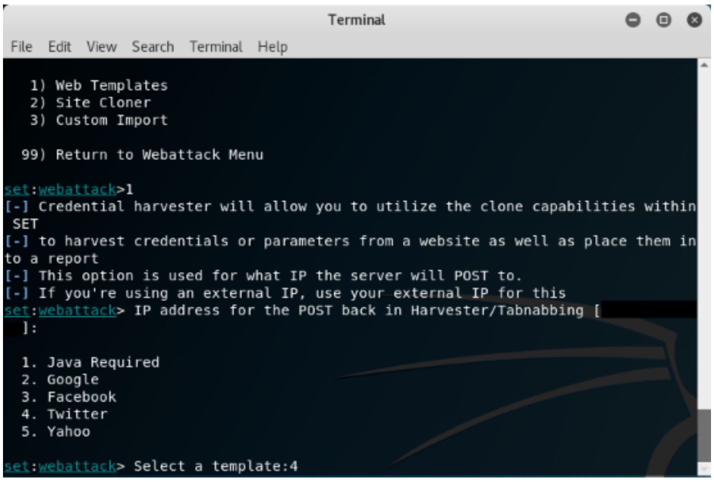
```
ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.

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, Credenti
al Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell inje
ction through HTA files which can be used for Windows-based powershell exploitat
ion 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) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```



```
  8) 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>1
```

We will select option **1) Website Templates**. This method will use a template of a fake webpage and allow you to harvest the credentials of anybody logging in to the fake webpage. You will get a prompt stating: IP address for the POST back in Harvester/Tabnabbing 10.0.2.15. This simply means that the IP address for the fake login page will be 10.0.2.15 (Please note that this IP address is an example only, use whatever your system displays, which may for instance be 192.168.0.1). When you see this prompt, just hit enter.

Now we will select **4. Twitter** to setup a fake Twitter's login page.

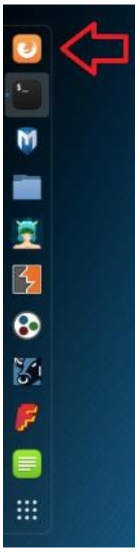


```
  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu

set:webattack>1
[-] 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 in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [[redacted]
  ]:

 1. Java Required
 2. Google
 3. Facebook
 4. Twitter
 5. Yahoo

set:webattack> Select a template:4
```

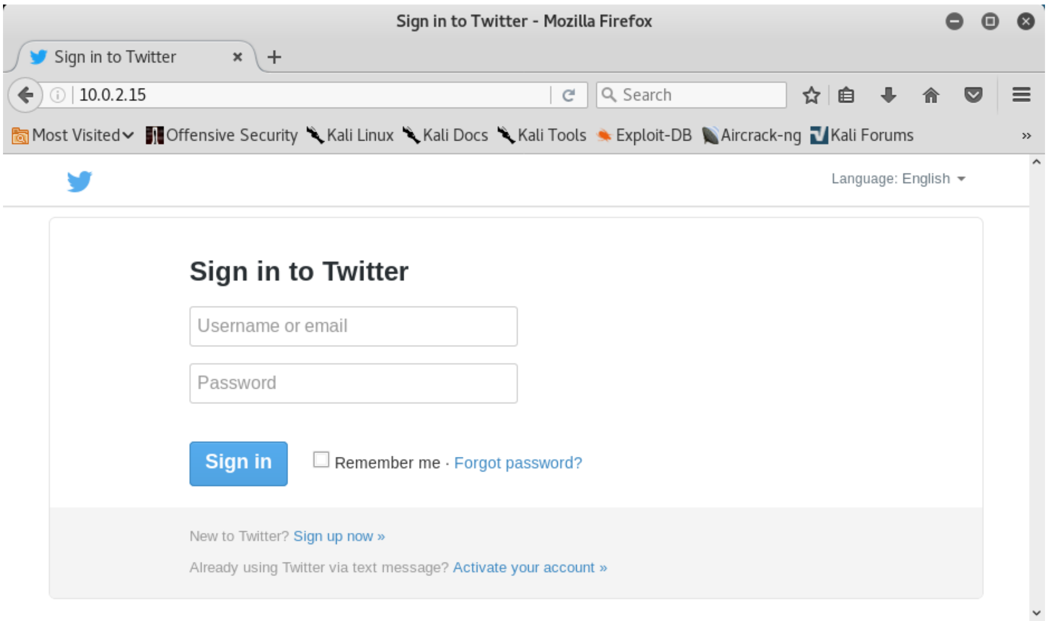
Hint: for the task below, when you harvest the credentials on the Kali machine you will see a lot of data on the screen. Simply scroll through it till you **find the username and password** you put in on the target machine.

Task

Open a browser and access the fake login page. (Hint: access the fake webpage by entering the IP address provided into the address bar.)



Now enter some fake login details on the fake webpage and look at what happens on the SET. Please **do not use your real username and password** for Twitter. . . Make something up. Can you find the login details you used?



Sign in to Twitter - Mozilla Firefox

Sign in to Twitter

10.0.2.15

Sign in to Twitter

Username or email

Password

Sign in

□ Remember me · Forgot password?

New to Twitter? Sign up now »

Already using Twitter via text message? Activate your account »

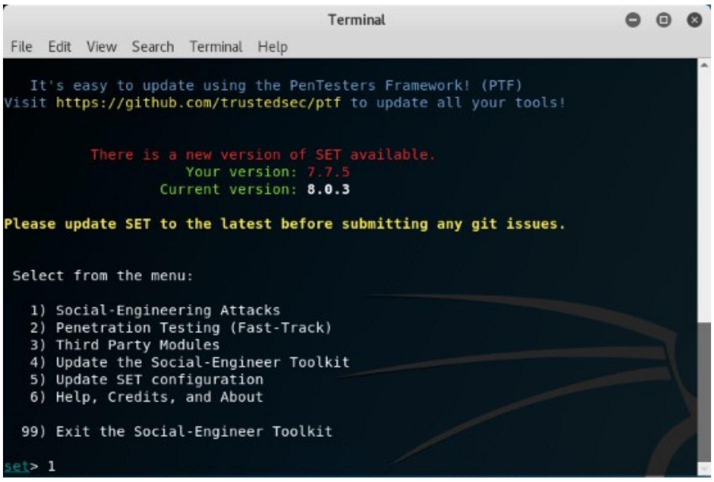
Exercise 2: Sending Phishing Email

In this exercise, we will conduct a phishing attack to steal Twitter login credentials. We will use the fake Twitter webpage created in the previous exercise. A phishing email of your own design will be used to get the user to visit our fake Twitter webpage. As a result, you will need access to an email account to send these mails from, which will have to be a Gmail account for SET. Setting up a Gmail account is covered under section "Gmail" above.

You will also need another target email address to send the email to. This must be an account you have access to (please **do not email this out to third-parties**).

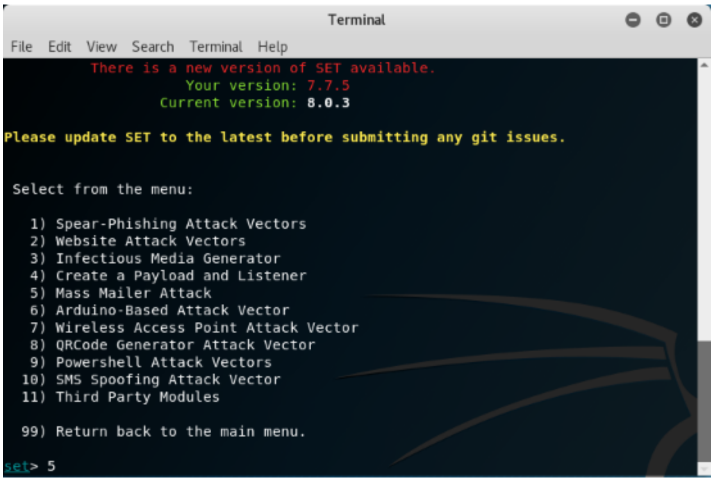
(Hint: follow the steps from exercise one and keep that terminal window open with SET running, then open another SET and follow the steps below.)

Select **1) Social-Engineering Attacks** to receive a listing of possible attacks that can be performed.



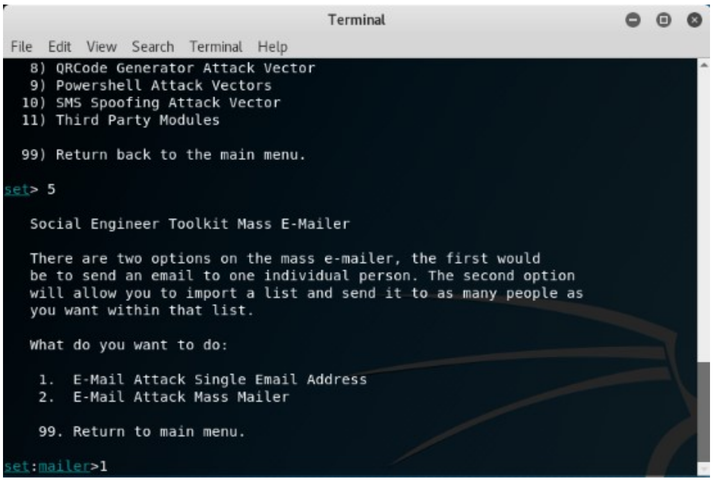
```
  It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


         There is a new version of SET available.
                    Your version: 7.7.5
                 Current version: 8.0.3

Please update SET to the latest before submitting any git issues.


 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
```

Select **5) Mass Mailer Attack**.



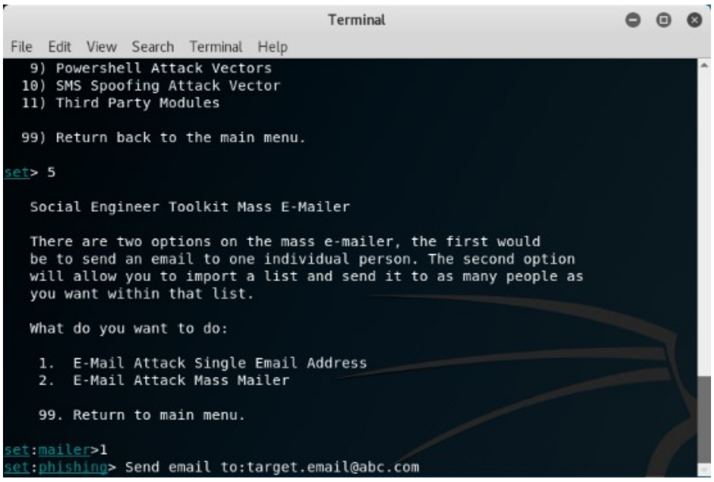
```
         There is a new version of SET available.
                    Your version: 7.7.5
                 Current version: 8.0.3

Please update SET to the latest before submitting any git issues.


 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) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 5
```

Select option **1) E-mail Attack Single Email Address**.



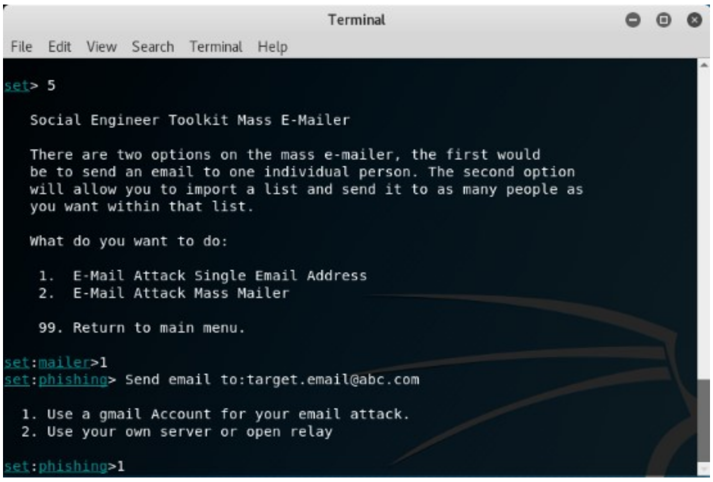
```
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) SMS Spoofing Attack Vector
 11) Third Party Modules

 99) Return back to the main menu.

set> 5

  Social Engineer Toolkit Mass E-Mailer

  There are two options on the mass e-mailer, the first would
  be to send an email to one individual person. The second option
  will allow you to import a list and send it to as many people as
  you want within that list.

  What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:mailer>1
```

Put a target email address to send your phishing email to. This must be an account you have access to (please **do not email this out to third-parties**).



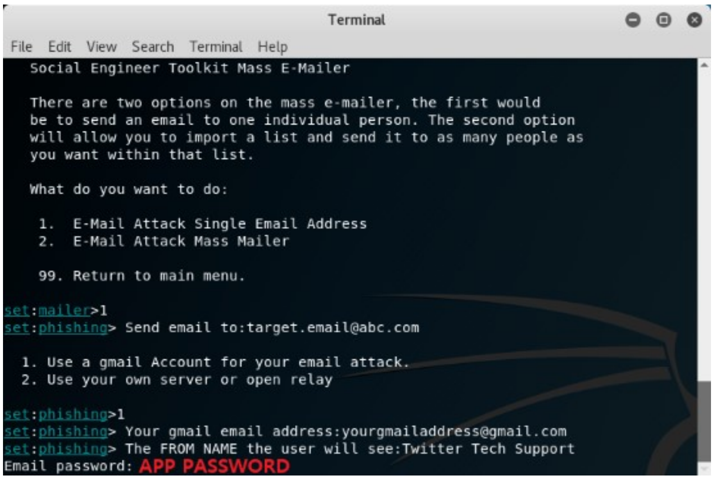
```
  9) Powershell Attack Vectors
 10) SMS Spoofing Attack Vector
 11) Third Party Modules

 99) Return back to the main menu.

set> 5

  Social Engineer Toolkit Mass E-Mailer

  There are two options on the mass e-mailer, the first would
  be to send an email to one individual person. The second option
  will allow you to import a list and send it to as many people as
  you want within that list.

  What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:mailer>1
set:phishing> Send email to:target.email@abc.com
```

Select **1. Use a gmail Account for your email attack**.



```
set> 5

  Social Engineer Toolkit Mass E-Mailer

  There are two options on the mass e-mailer, the first would
  be to send an email to one individual person. The second option
  will allow you to import a list and send it to as many people as
  you want within that list.

  What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:mailer>1
set:phishing> Send email to:target.email@abc.com

 1. Use a gmail Account for your email attack.
 2. Use your own server or open relay

set:phishing>1
```

Put your gmail address and construct your phishing email. When you put "Email password", **use the app password**. Also remember to include a link to the fake webpage.



```
   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

    1.  E-Mail Attack Single Email Address
    2.  E-Mail Attack Mass Mailer

    99. Return to main menu.

set:mailer>1
set:phishing> Send email to:target.email@abc.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:yourgmailaddress@gmail.com
set:phishing> The FROM NAME the user will see:Twitter Tech Support
Email password: APP PASSWORD
```

Once your phishing email is delivered to the target, open it and see what it looks like. Is this a believable email? Can you think of ways to improve this email both in terms of appearance and contents.

Bonus: What can we learn from inspecting the email once received by the target?

Bonus: How would you go about constructing a better-looking email using this approach? Do you think a service such as bitly would help?

You may want to remove the app password(s) now.