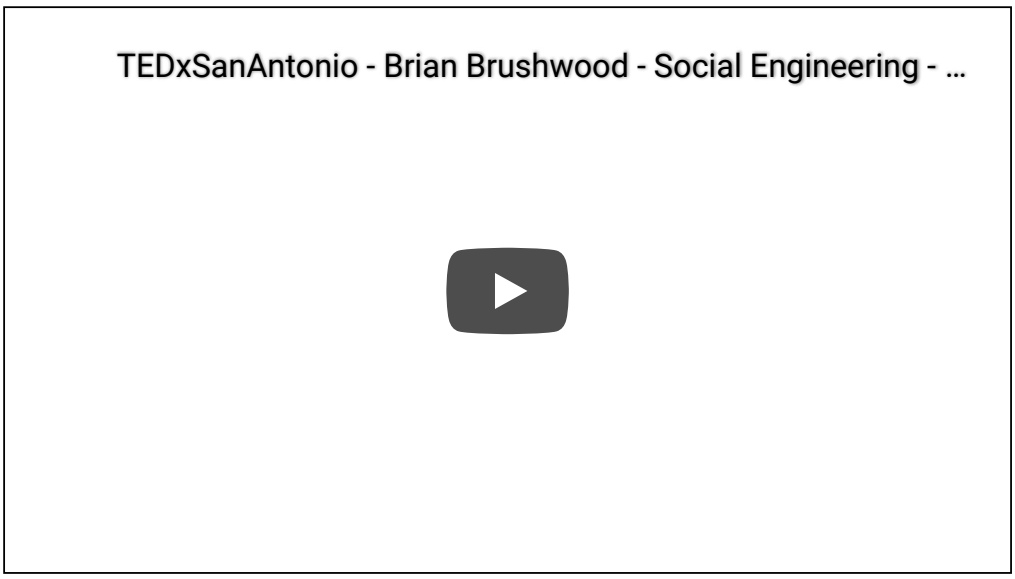
Social Engineering Toolkit (SET)

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.

Consider showing this video at the beginning of class:



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 attak may succeed.

MIDN are expected to cloned Facebook using the Social Engineering Tookit, 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!!

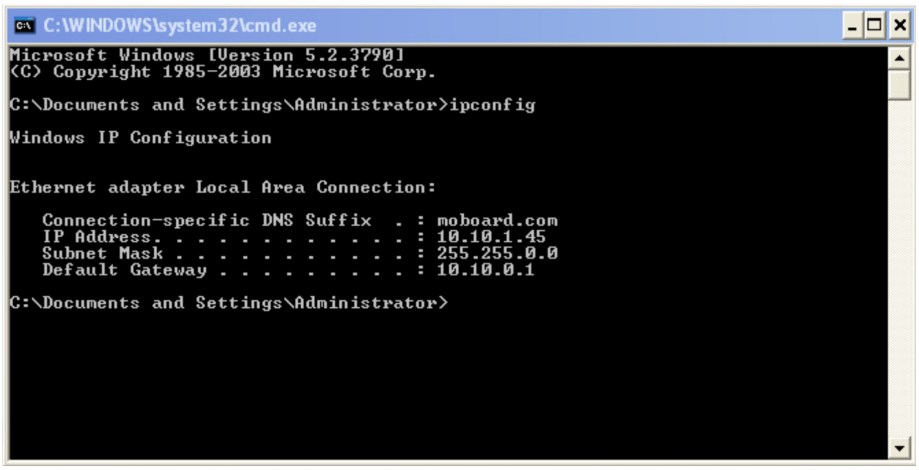
Instructor Note:

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.

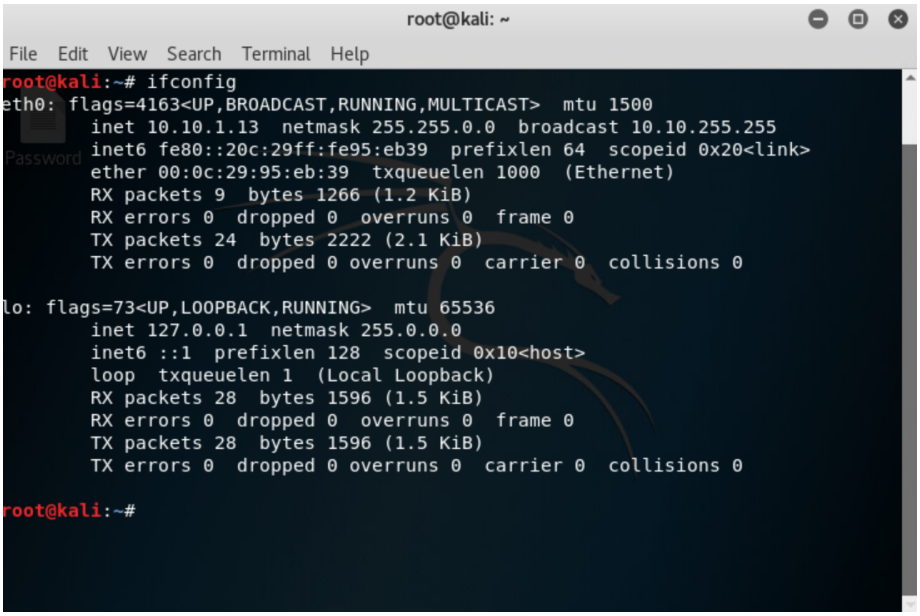
```
ipconfig
```



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 Metaploitable2-Linux virtual machines. Note that this is not a public IP, but we can access it within the subnet.

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

```
ifconfig
```



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 Metaploitable2-Linux virtual machines. Note that this is not a public IP, but we can access it within the subnet.

Social Engineering Toolkit (SET) Operation

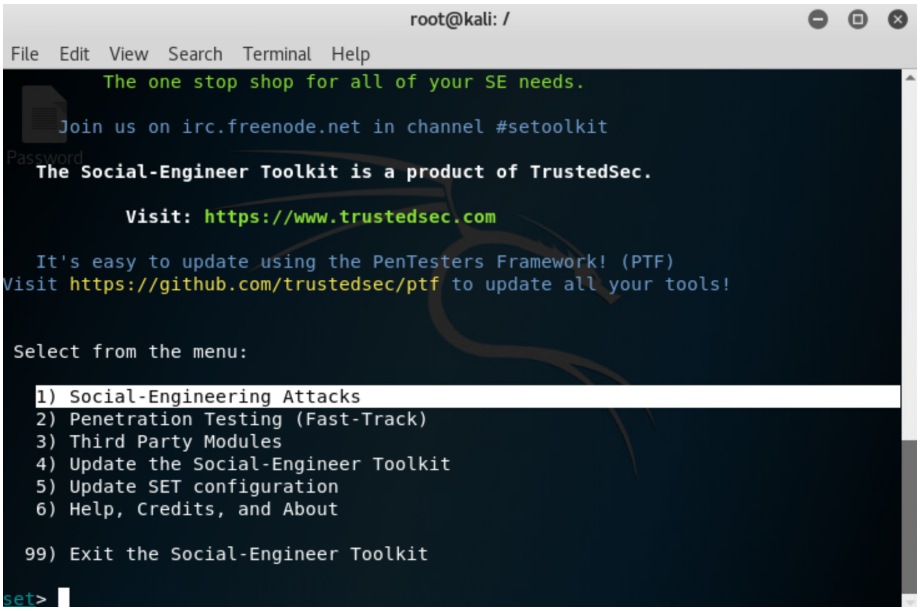
Start the Social Engineering Toolkit (SET)

```
setoolkit
```

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

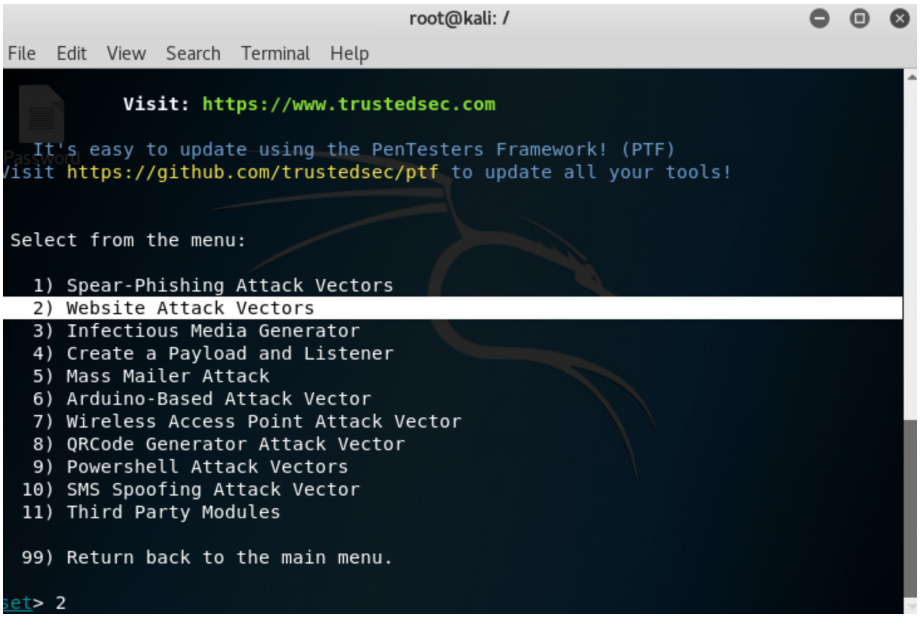
Select option:

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



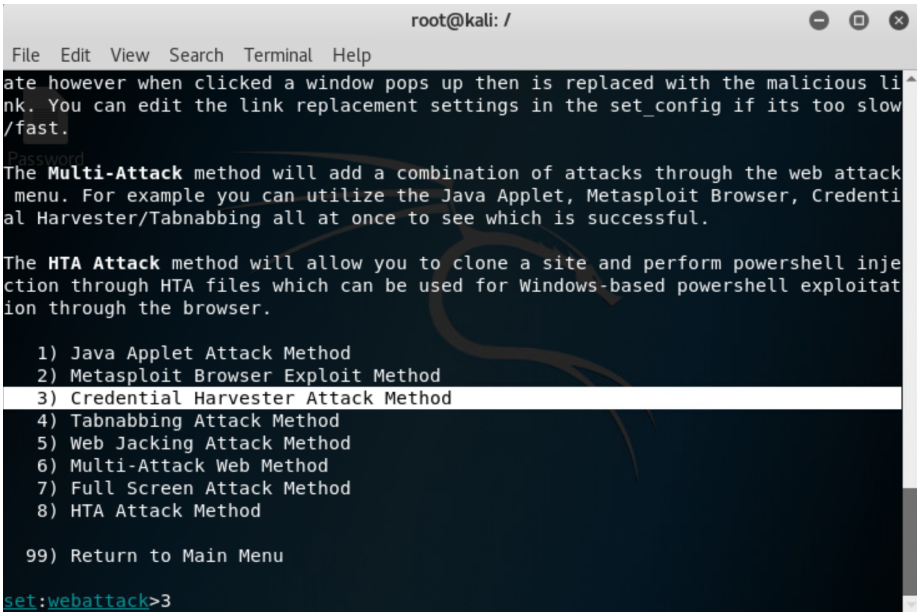
Select option:

```
2) Website Attack Vectors
```



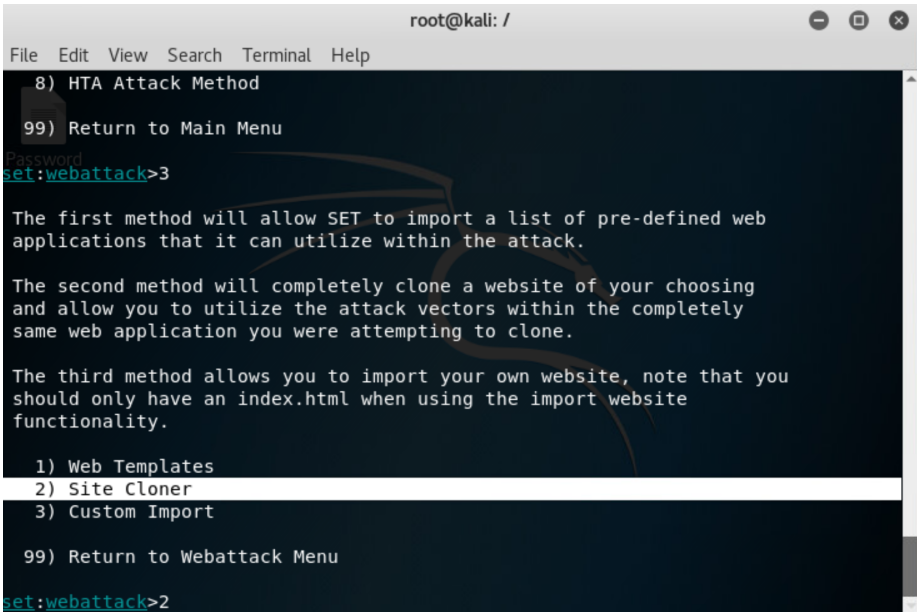
Select option:

```
3) Credential Harvest Attack Method
```



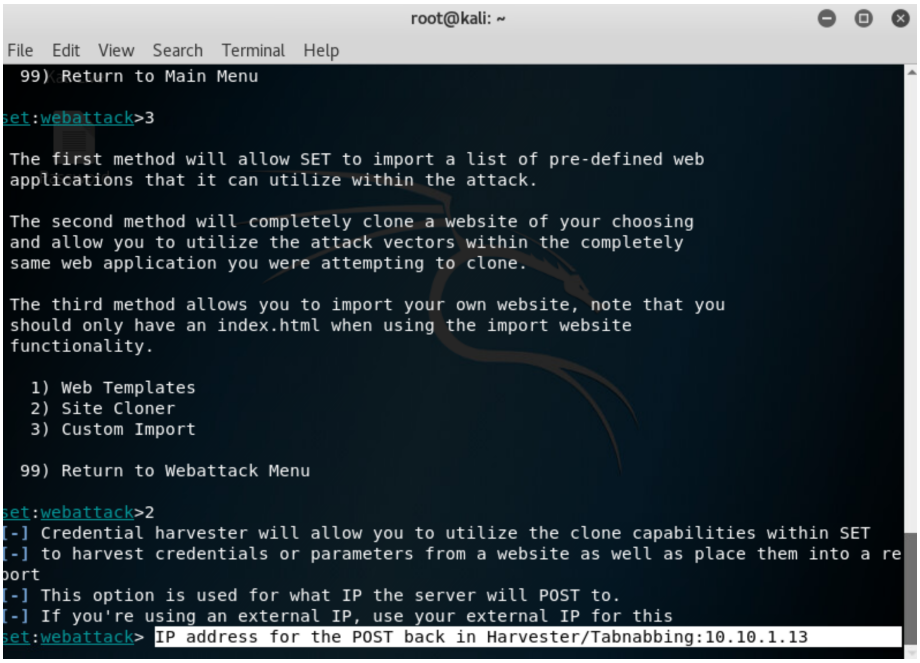
Select option:

```
2) Site Cloner
```



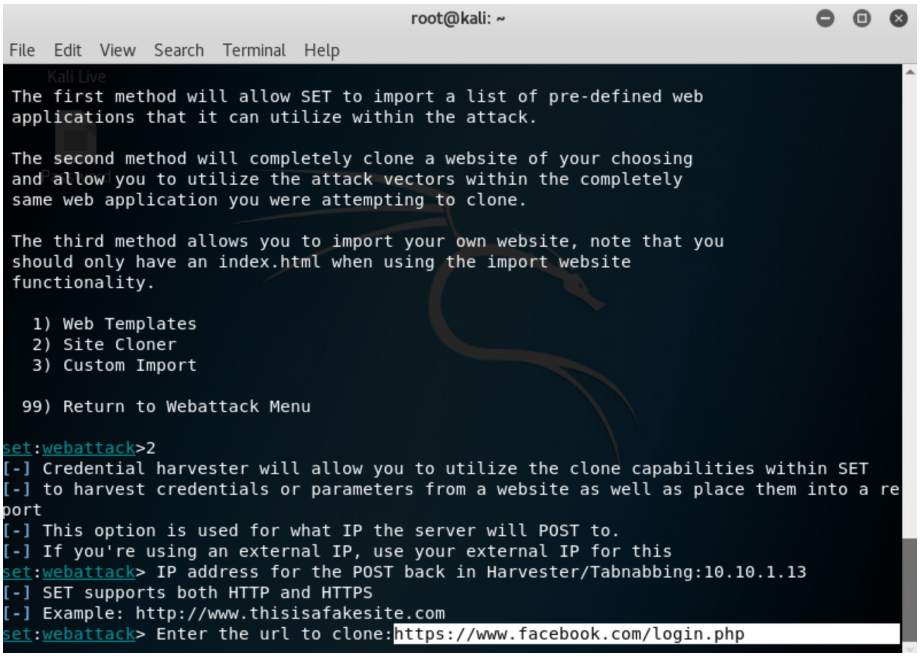
Enter the IP address for the Post back in Harvester/Tabnabbing

```
[Cyber Operator Host IP Address]
```

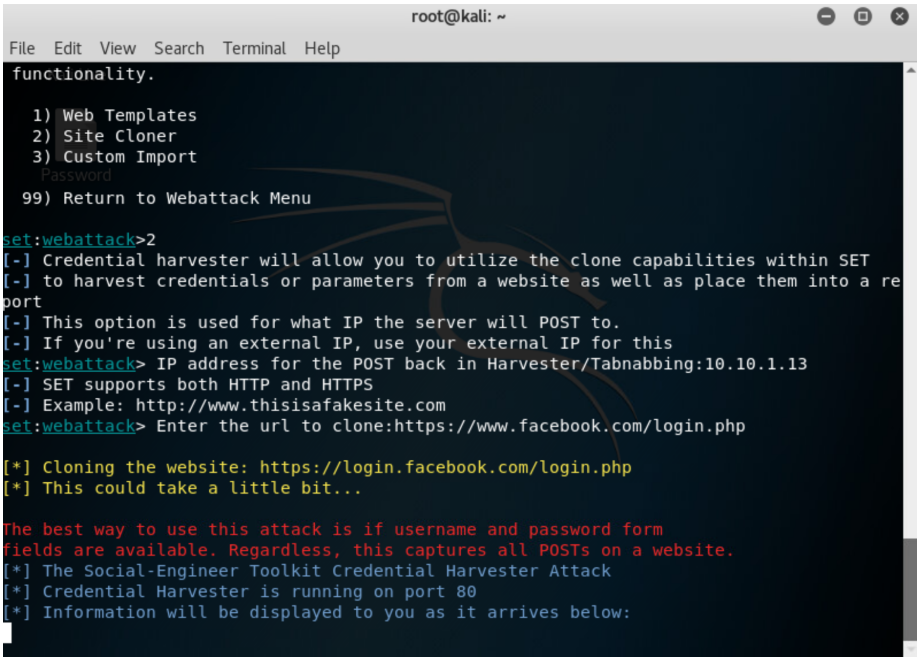


Enter the URL to clone:

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

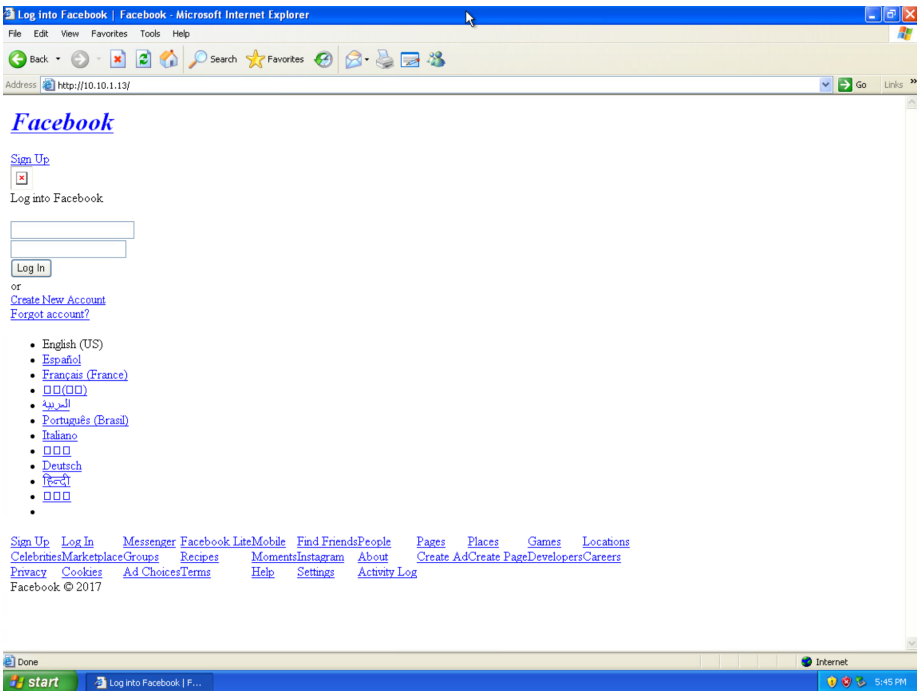


You have successfully cloned the website when you are told that the Credential Harvester is running on port 80.

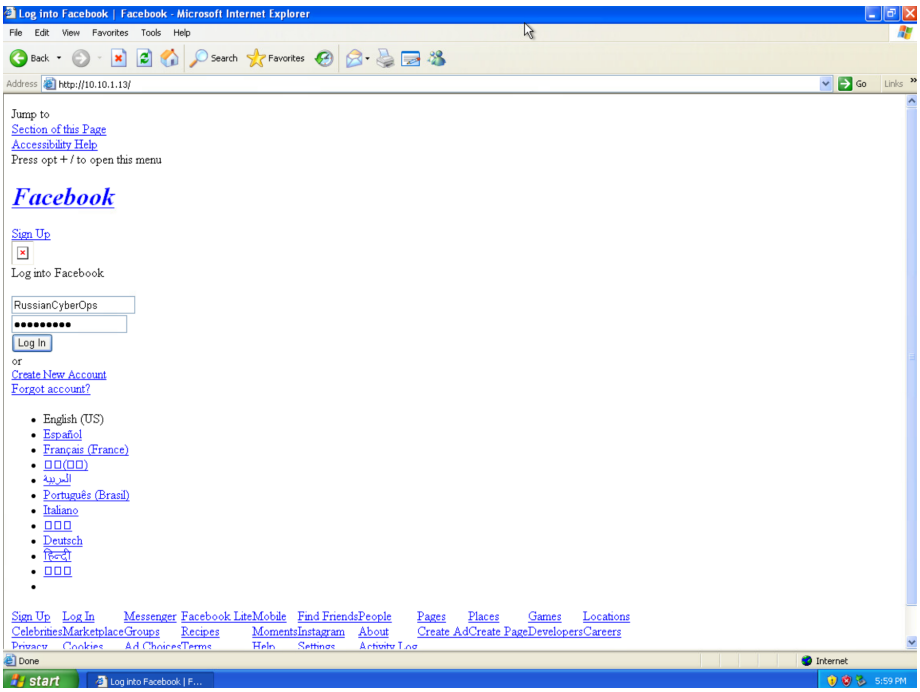


Visit the Target machine and open the web browser.

Enter the Cyber Operator IP Address into the address bar

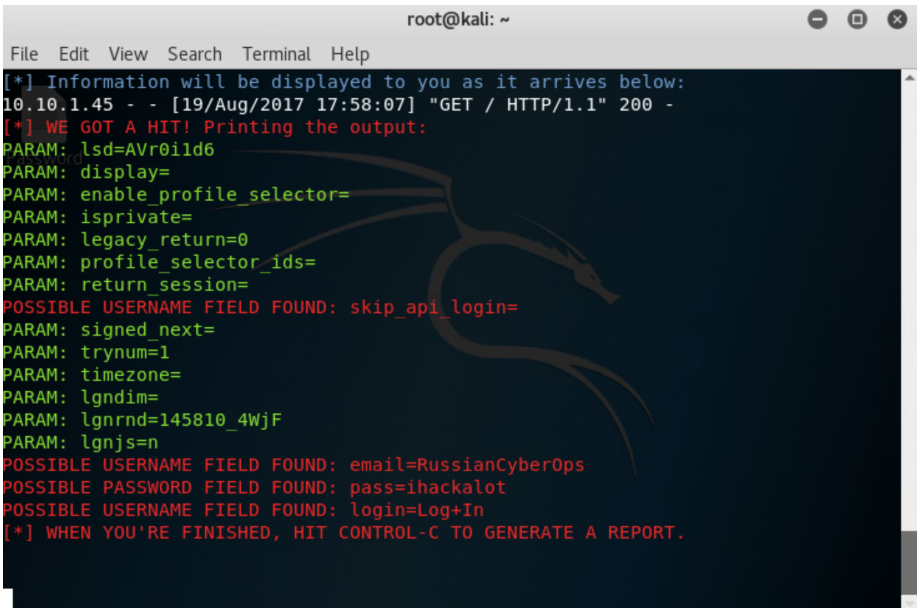


Enter the provided username and password (**see above**) and take a screenshot of the cloned Facebook web page.



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

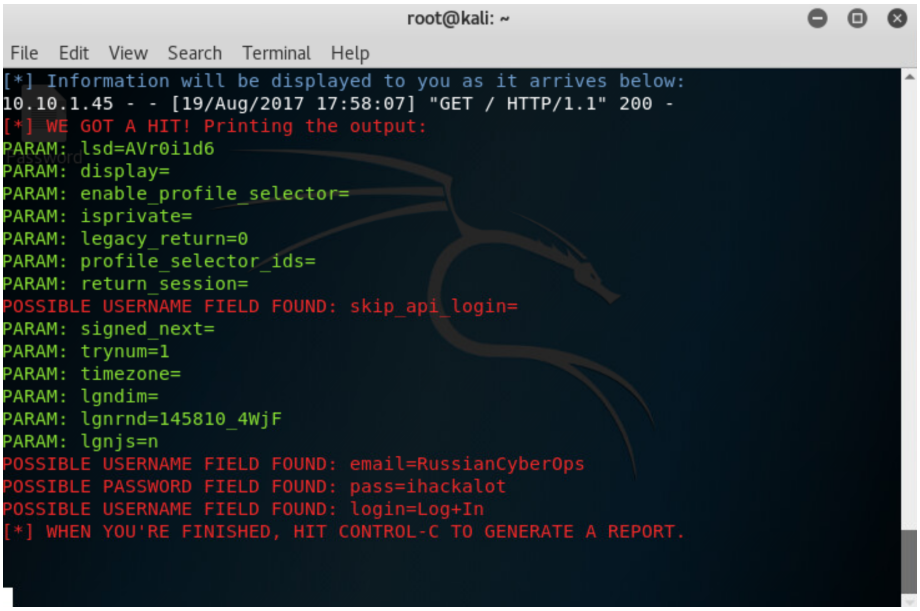
Take a screenshot of the Cyber Operator VM Harvest Credential results (displayed via the command line).



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.



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/