

## RESEARCH ON DICTIONARY ATTACK TO CRACK ONLINE PASSWORDS USING HYDRA

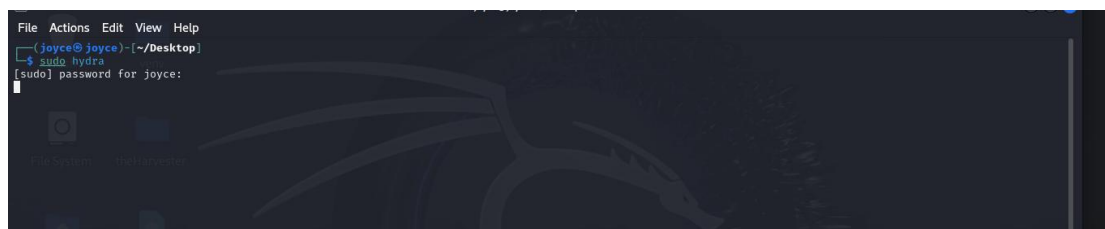
**Project Objective:** Learn how to conduct a dictionary attack to crack passwords using Hydra. This involves vulnerability assessment.

Hydra is a tool that is used to perform brute force attacks. It is an advanced password cracker, which can be used to crack passwords for online pages.

A dictionary attack is a type of password attack which uses a combination of words from a word list and attempted all of them in association with a username to login as a user.

**Project Tool:** Kali linux(Hydra,wordlists)

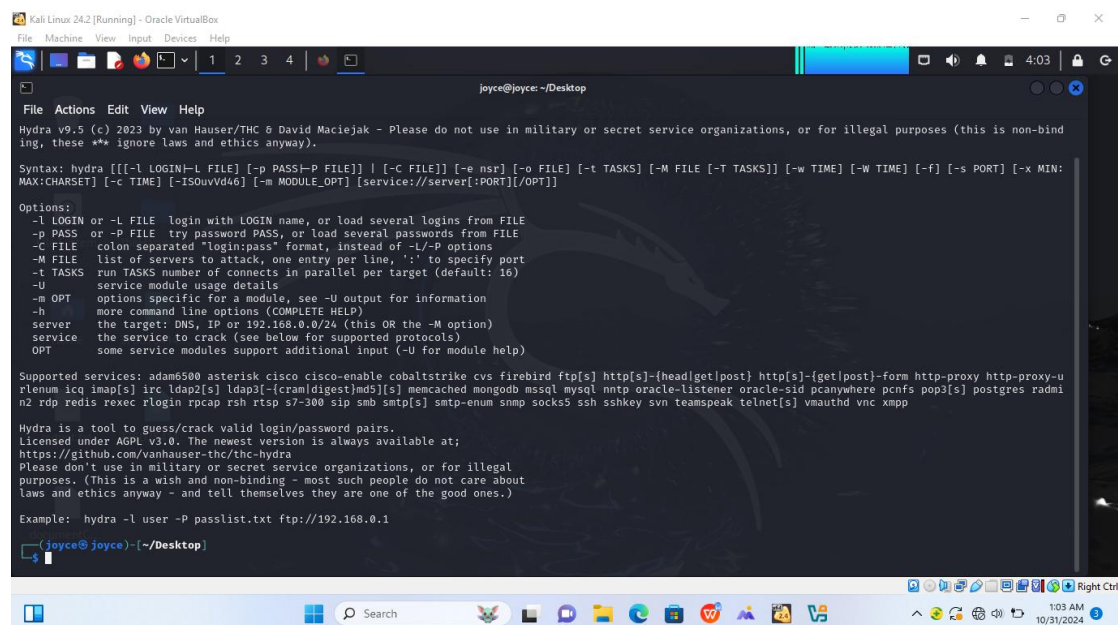
### Sudo hydra



```
File Actions Edit View Help
(joyce@joyce) ~/Desktop
$ sudo hydra
[sudo] password for joyce:
```

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

To use Hydra against an online target such as this site, it is required to capture the post-form parameters.



```
Kali Linux 24.2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
joyce@joyce: ~/Desktop
File Actions Edit View Help
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]]

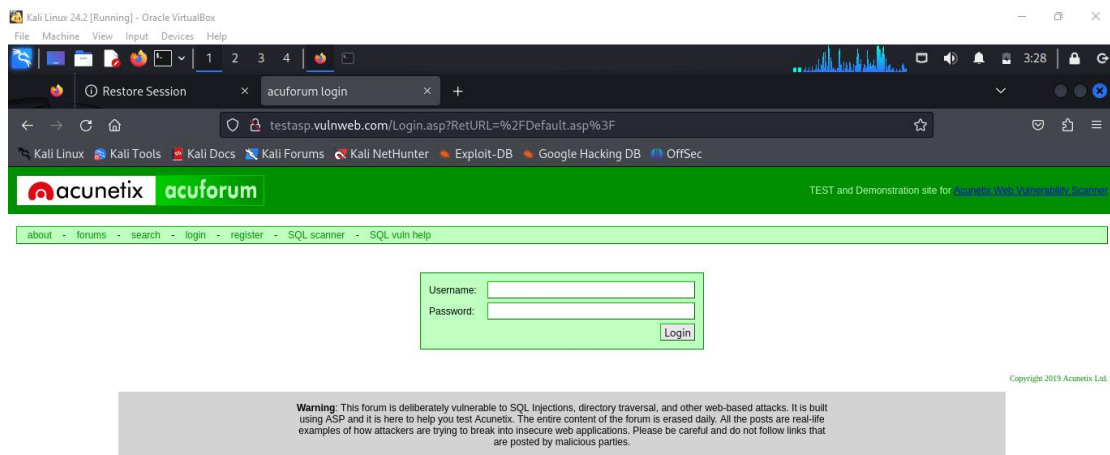
Options:
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-c FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line, ':' to specify port
-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: adam5000 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-[head|get|post] http[s]-[get|post]-form http-proxy http-proxy-u
rleenum 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 radmi
n2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmp

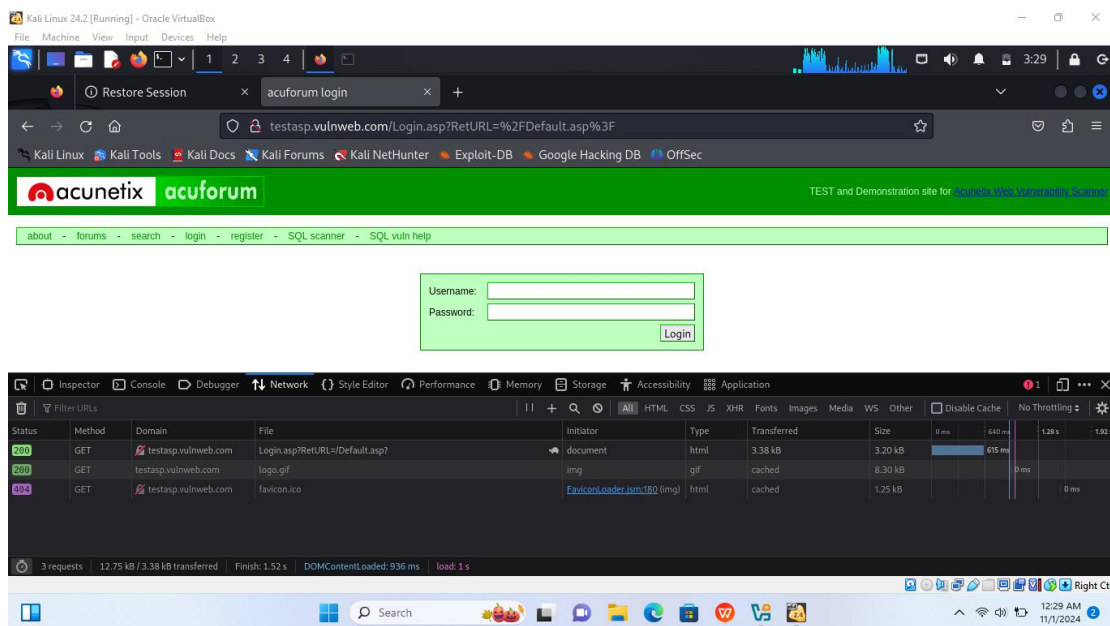
Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at:
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such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

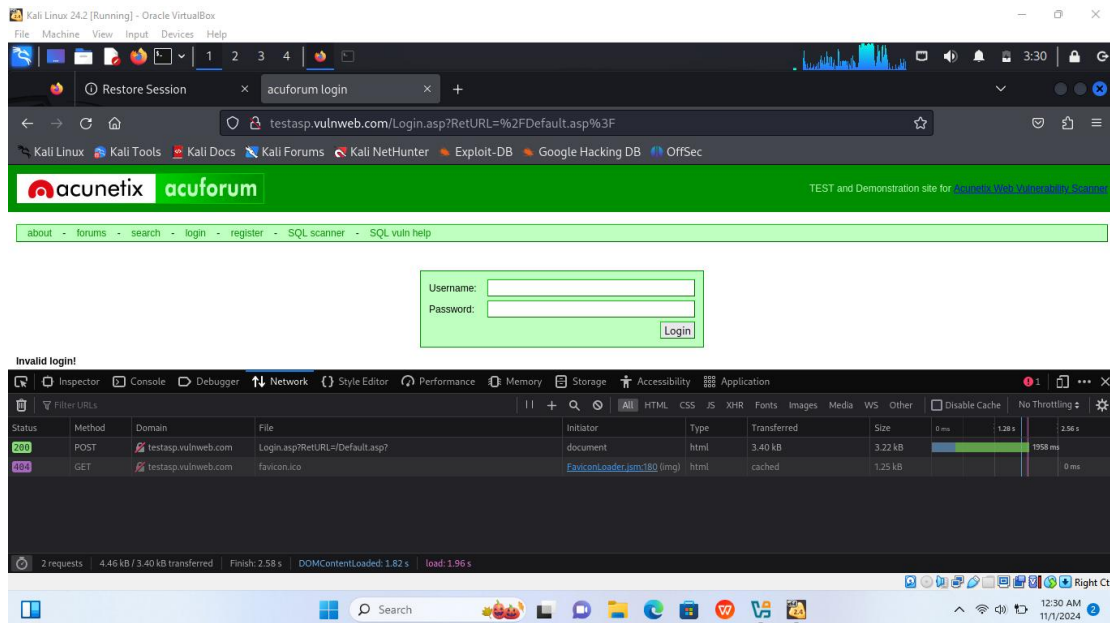
Example: hydra -l user -P passlist.txt ftp://192.168.0.1

(joyce@joyce) ~/Desktop
$
```

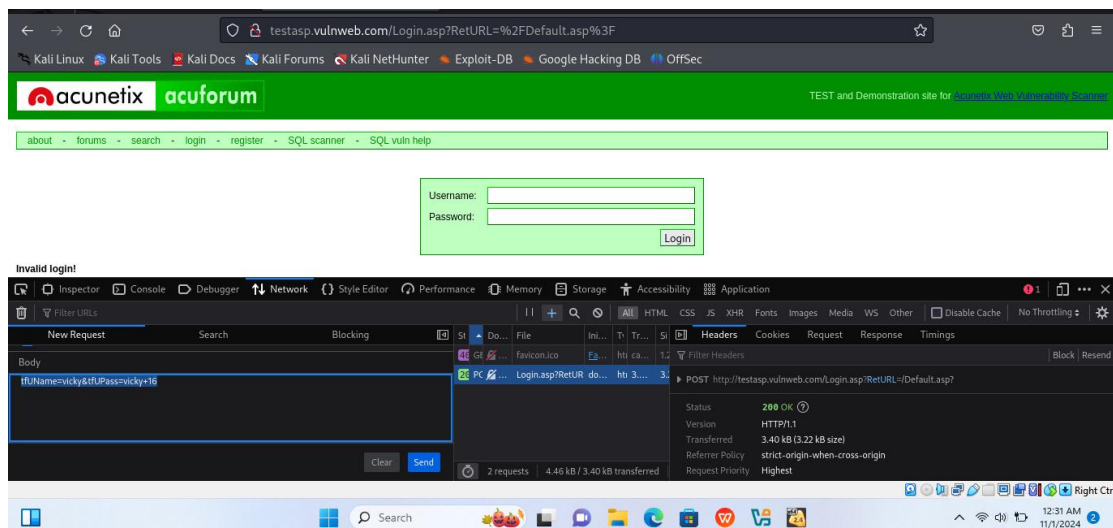


Hydra will use these parameters to send its various requests to the correct target.





The tab called “Network”, displays several (HTTP Method) GET requests. This machine is requesting data from the server.  
 Entering a random username and login. There is a new POST request in the Network Tab.  
 This request contains the parameters needed to brute force.



***tfUName=vicky&tfUPass=vicky+16 - This was the login details***

```
Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
joyce@joyce: /usr/share/wordlists

/usr/share/wordlists
amass -> /usr/share/amass/wordlists
dirb -> /usr/share/dirb/wordlists
dirbuster -> /usr/share/dirbuster/wordlists
dnsmmap.txt -> /usr/share/dnsmmap/wordlist_TLAs.txt
fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt
fern-wifi -> /usr/share/fern-wifi-cracker/extras/wordlists
john.lst -> /usr/share/john/password.lst
legion -> /usr/share/legion/wordlists
metasploit -> /usr/share/metasploit-framework/data/wordlists
nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst
rockyou.txt
rockyou.txt.gz
sqlmap.txt -> /usr/share/sqlmap/data/txt/wordlist.txt
wfuzz -> /usr/share/wfuzz/wordlist
wifite.txt -> /usr/share/dict/wordlist-probable.txt
joyce@joyce: /usr/share/wordlists

joyce@joyce: /usr/share/wordlists
$ locate wordlists
/var/lib/plocate/plocate.db: No such file or directory

joyce@joyce: /usr/share/wordlists
$ hydra -l admin -b
Could not find command-not-found database. Run 'sudo apt update' to populate it.
admin: command not found

joyce@joyce: /usr/share/wordlists
$ ls
amass dirb dirbuster dnsmmap.txt fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt rockyou.txt.gz sqlmap.txt wfuzz wifite.txt
joyce@joyce: /usr/share/wordlists
```

A word list is a collection of words or phrases, used for password cracking. In attempting to login as admin. A word list will be used to guess passwords to login as this account. Using rockyou.txt.gz

```
Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
joyce@joyce: /usr/share/wordlists

nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst
rockyou.txt
rockyou.txt.gz
sqlmap.txt -> /usr/share/sqlmap/data/txt/wordlist.txt
wfuzz -> /usr/share/wfuzz/wordlist
wifite.txt -> /usr/share/dict/wordlist-probable.txt
joyce@joyce: /usr/share/wordlists

joyce@joyce: /usr/share/wordlists
$ locate wordlists
/var/lib/plocate/plocate.db: No such file or directory

joyce@joyce: /usr/share/wordlists
$ hydra -l admin -P
Could not find command-not-found database. Run 'sudo apt update' to populate it.
admin: command not found

joyce@joyce: /usr/share/wordlists
$ ls
amass dirb dirbuster dnsmmap.txt fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt rockyou.txt.gz sqlmap.txt wfuzz wifite.txt
joyce@joyce: /usr/share/wordlists
$ hydra -l admin -b
Could not find command-not-found database. Run 'sudo apt update' to populate it.
admin: command not found

joyce@joyce: /usr/share/wordlists
$ hydra -I admin -P /usr/share/wordlists/rockyou.txt testapp.vulnweb.com http-post-form "/Login.asp? RetURL=/Default.asp::tfUName=vicky&tfUPass=vicky+16 pipe dquote>
joyce@joyce: /usr/share/wordlists
$ hydra -I admin -P /usr/share/wordlists/rockyou.txt testapp.vulnweb.com http-post-form "/Login.asp? RetURL=/Default.asp::tfUName=vicky&tfUPass=vicky+16 dquote>
```

This is a research and example on Hydra attempting on a dictionary attack for a POST request.