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

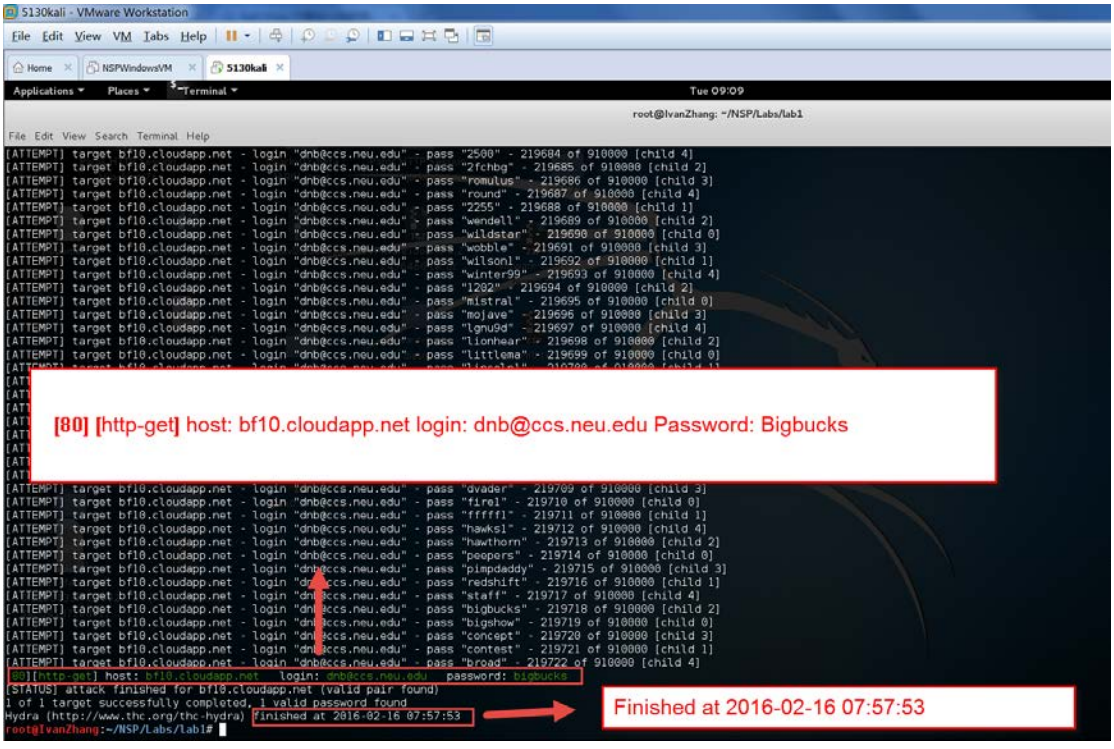
Answer:

1. Hydra result

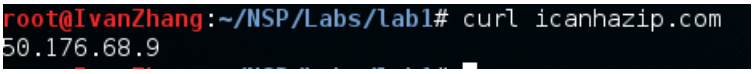
In this case, we use theharvest email collection tool to collect email addresses related to domain ccs.neu.edu. Actually, because the limitation of theharvest and google, I only got 40 email address but I run the commercial version of metego to get the rest of email addresses. Then I downloaded the pre-prepared 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



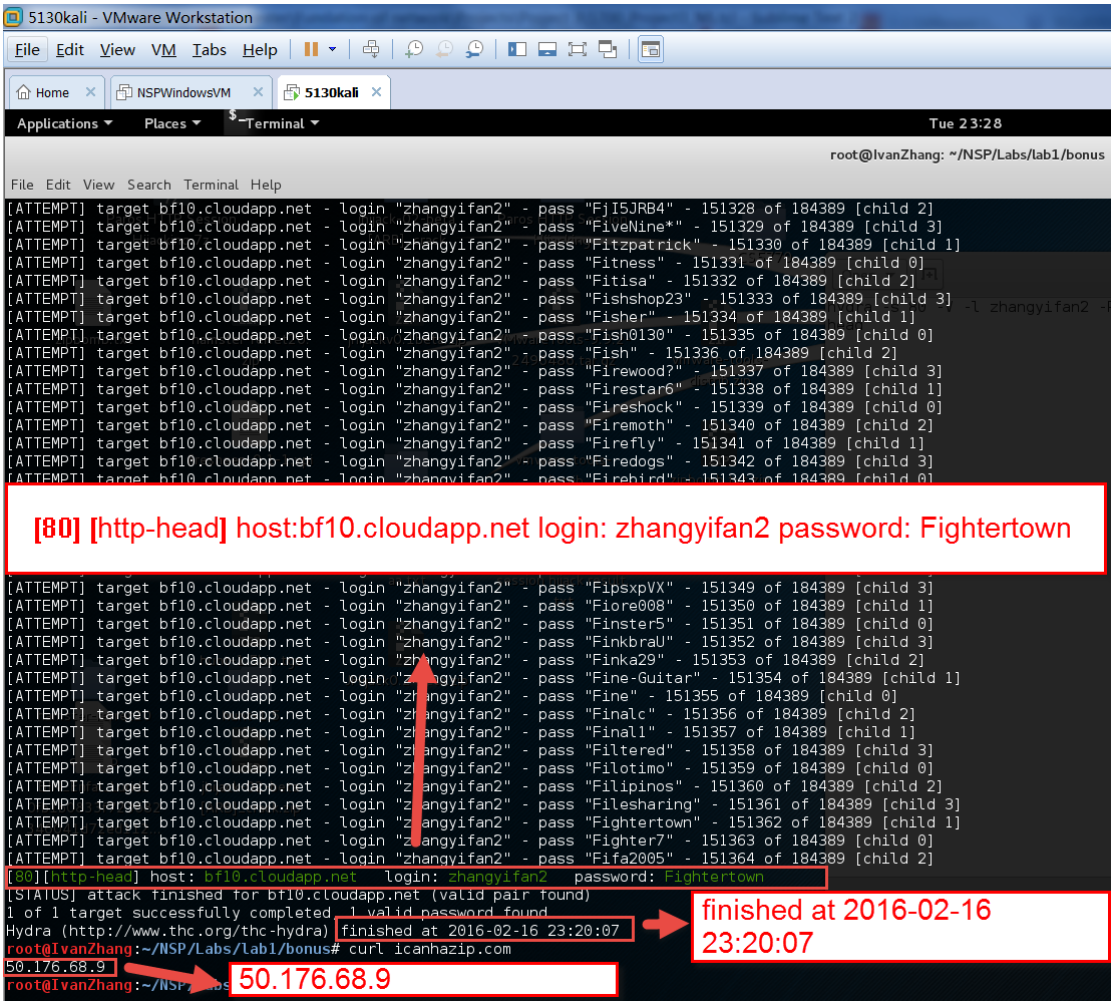
2. Current public IP address



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



2. After the login