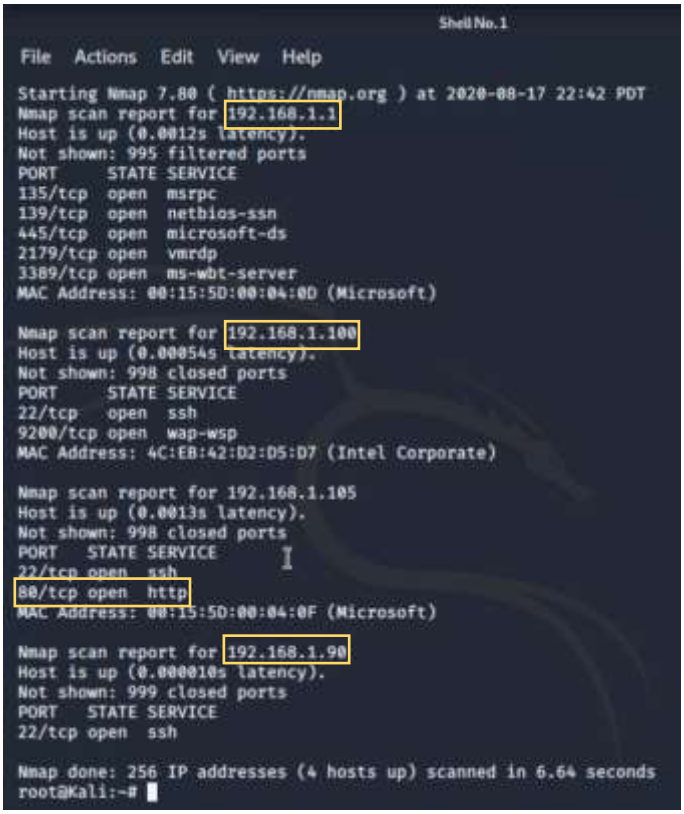
Penetration Testing

Lyfted Health Corp.

September 1, 2020

Nmap Scan



The first thing we need to do is to gather as much evidence as we can to make it easier for us to solve the puzzle. Using an Nmap (Network Mapping) scan would be the best way of identifying which devices are running, finding hosts, and finding open ports.

Here we have our scan and what is running on the network. We can see that there are four different sections that represent the devices.

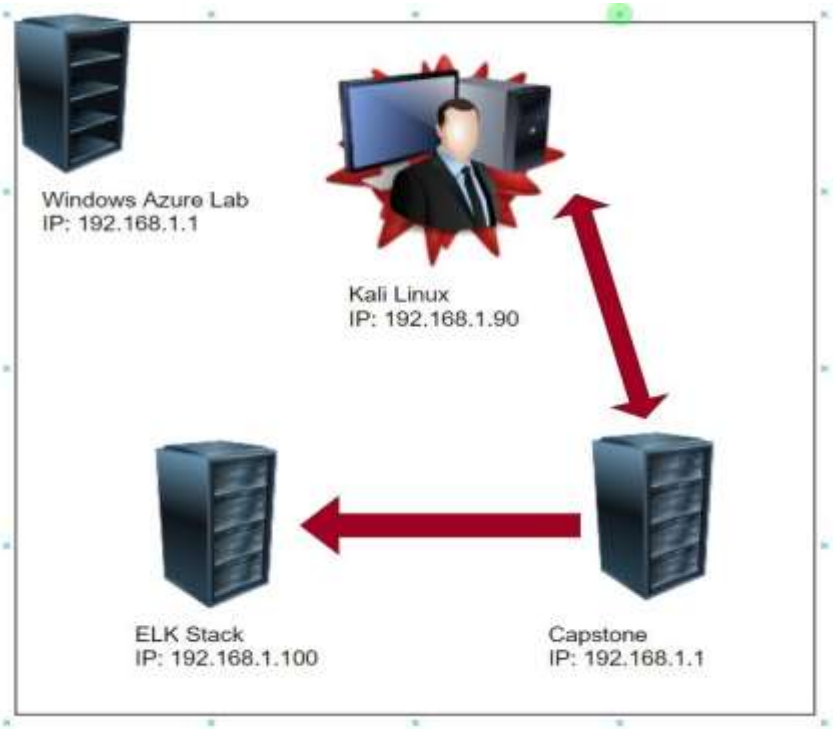
IP Address

Azure IP: 192.168.1.1

Capstone IP: 192.168.1.105

ELK IP: 192.168.1.100

Kali IP: 192.168.1.90



Network Diagram

Windows Azure Lab: This is the environment provided for us by Windows

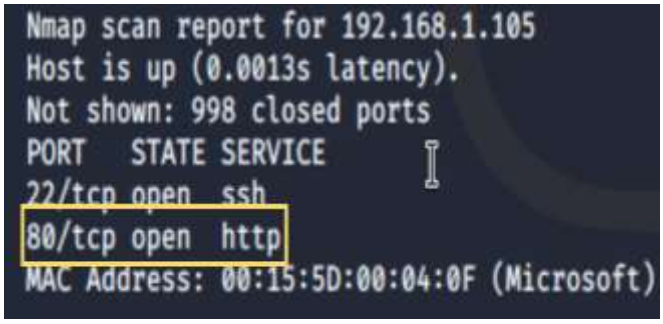
Kali Linux: This will be our local macheine

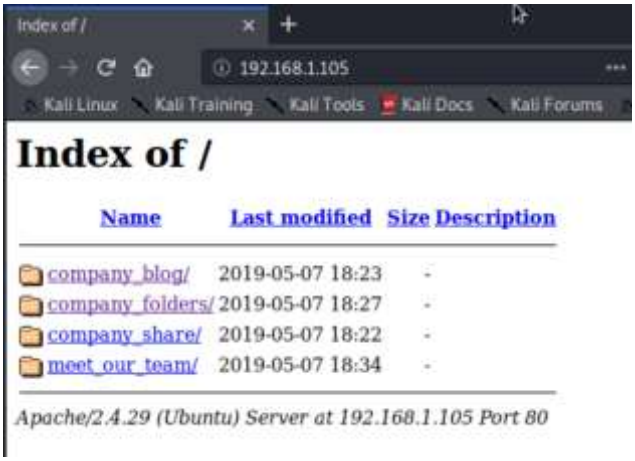
Capstone: This will be our main machiene to attack. We must be able to connect to Capstone in order to talk to ELK Stack.

ELK Stack: This will be our main database server. It is a one-way communication with capstone.

Checking Ports for Entrance

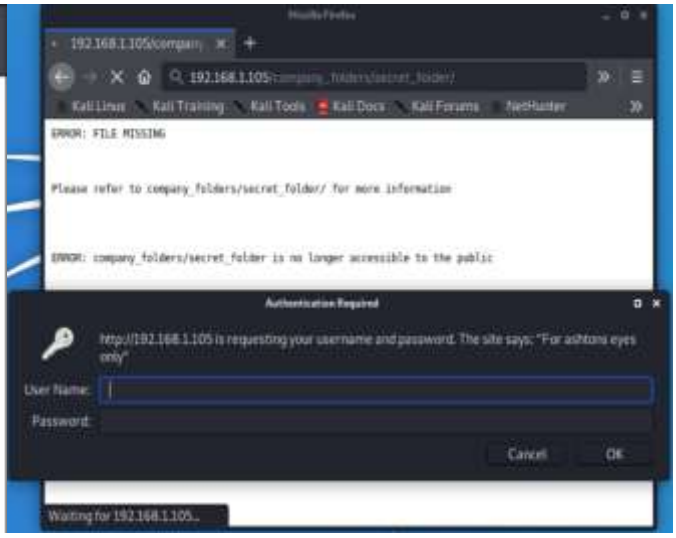
Here is an example of exploiting an interpoint. By using the Nmap scan and evaluating 192.168.1.105 (Capstone) we can see that port 80 is open with an http service. We can take advantage of this open http port by typing in the ip address into the web browser. After typing in 192.168.1.105 firefox browser this screen opens up on the GUI. There are just folders to look through but the process of looking for things that might be able to take advantage would apply to





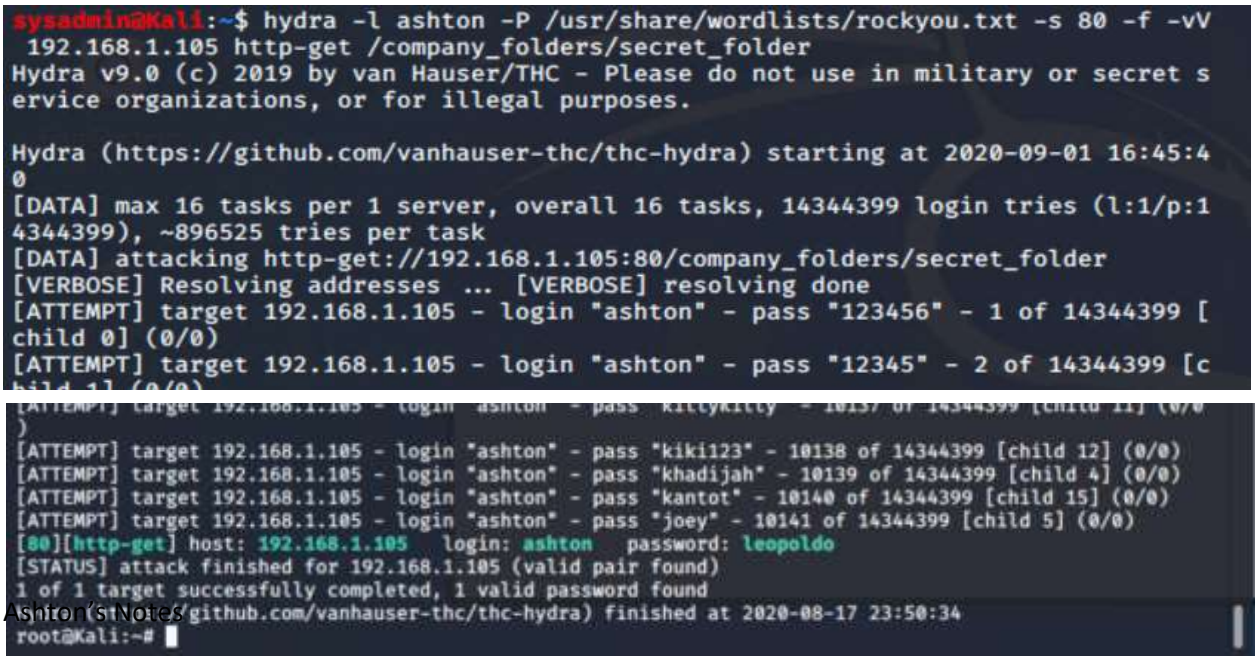
Sniffing Around

After going through the folders on the GUI I decided to take the path of /computer_folders/company_culture/file1.txt. Following my attempt to open the file is where there is a message saying that the folder has been moved to the path of /company_folders/secret_folder. I then changed my web browser url path to /company_folders/secret_folder and then received a box that requires certain credentials. This authentication requirement box gave us a lot of information. We are given the name “ashton” and the fact that it is for his eyes only means he has higher privileges.



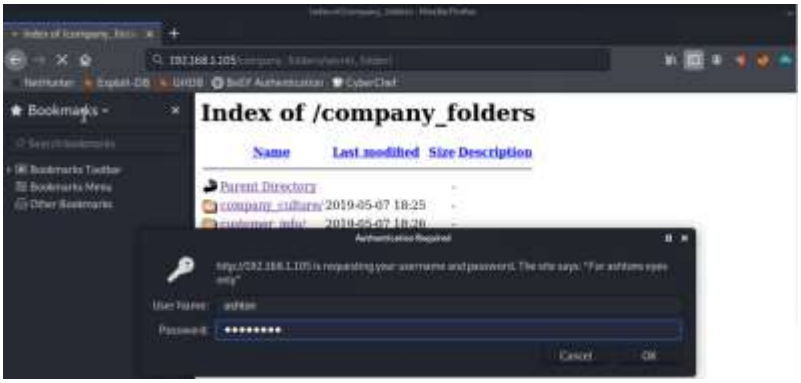
Attack Initiated

Now that we have a user “ashton” we could use hydra to brute force attack and get his password through the terminal. We are going to be using Hydra, a tool to guess/crack valid login/password pairs. The command that we used was *hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder*. The options I put in -l is login, -P is password using the wordlist, -s is port -f is stop when match is found, and vV is for verbose to format.



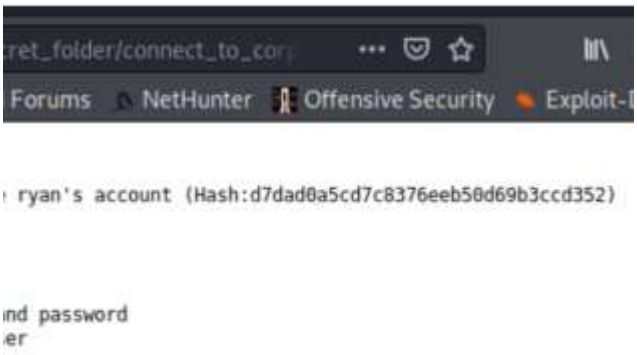
Ashton’s Notes

After logging under Ashton’s account we see that Ashton makes a critical error here in giving us a username, as well as a hash leading to its password. He then tells us what he plans on doing and then lays out step by step to expose his private and privileged information.

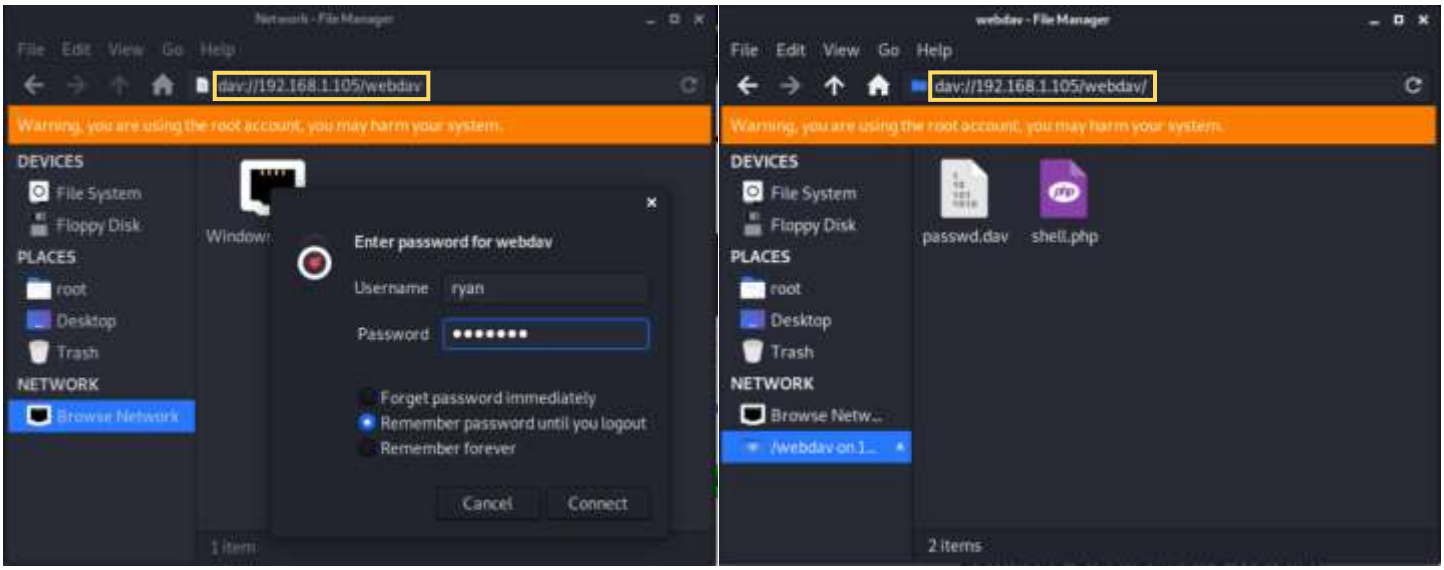


Ryan's Password

We are now going to take the information about the user ryan and his hash (d7dad0a5cd7cb376eeb50d69b3ccd352). I use google to find the website CrackStation to see if it could help me with this hash. We put in the hash and the click Crack Hash to get us our results "linux4u."



In Ashton's notes he did mention changing to webdav (Web Distributed Authoring and Versioning) to share files with Ryan. Webdav is an extension of the http protocol that allows users to work remotely. For this we will need a different network. The instructions were to change a network to use webdav and type "dav://192.168.1.105/webdav." This is where we ender ryan's username and password (which we just cracked). After hitting enter we get our shell!



Conclusion

Lyfted Health Corp. has done a decent job as far as security. The main and easiest way was through the http ports and gain too much information based off of the information gathering. They accidently gave us Ashton as a user and then later Ryan with his password. Ashton should not have that information in the “secret_foler.” It gave the attacker a name, hash, intentions on what to do, step by step instructions.

Possible Solutions would be

- Password Lock after 5 fails
- Whitelist IP addresses
- More awareness and responsibility for data
- Update their antivirus often

Lyfted Health Corp.

September 1, 2020

.