Red Team Attack!

nmap 192.168.1.1/24

Graphical user interface, website

Description automatically generated

ip found 192.168.1.105

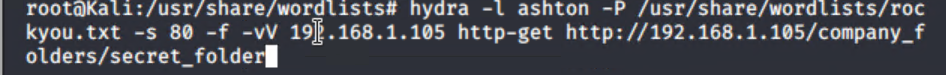
open ports 22 and 80

Text

Description automatically generated

dirb 192.168.1.105 /usr/share/wordlists/dirb/common.txt

found secret folder. Based off the meet\_our\_team folder I decided to attack ashton’s user



This is my attack command

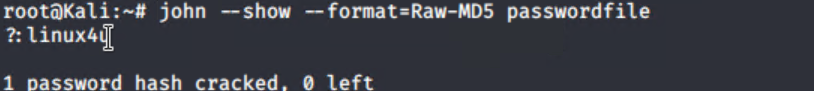
Text

Description automatically generated

This is the password that I found!

Graphical user interface, text

Description automatically generated



Used john to crack the hash and got ryan’s password of linux4u

Text

Description automatically generated

Went to webdav and entered Ryan’s credentials. Now we can open a webdav folder.



Then made a payload.php file through msfvenom and dropped it into the webdav file folder.

After the payload was in the proper place, I started msfconsole on my terminal. I set the payload and set the LHOST and was able to open meterpreter on their system.

Graphical user interface, text

Description automatically generated

Once there I went to the root directory and used the ls command and found the file for the flag.

A computer screen capture

Description automatically generated with medium confidence



Here is the flag!

We then downloaded the flag to our system.



This completes the Red Team attack on a vulnerable system.

Analysis