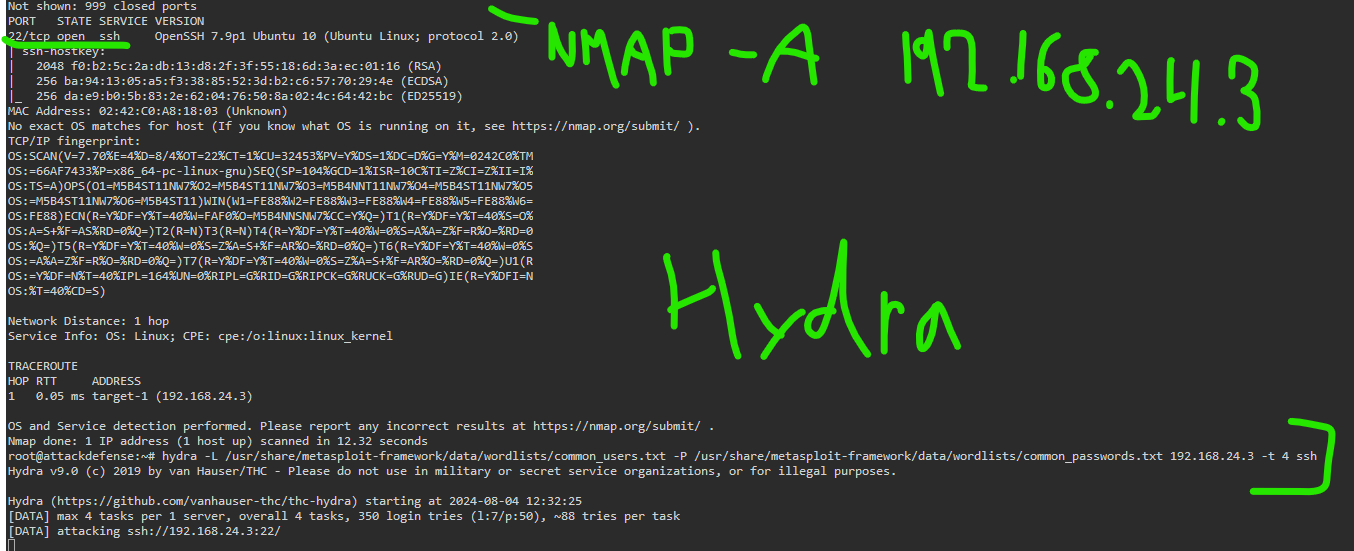
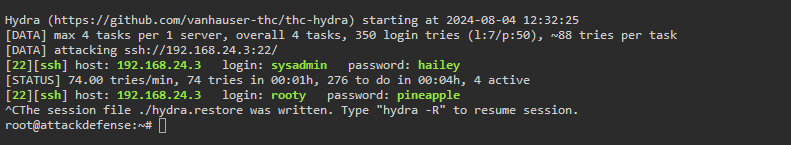
Scenario: attack the target machine. Start with nmap -A.

We find port 22 open over tcp. It appears to be running an open ssh service.



We run a hydra brute force (above), and then stop the session after finding sysadmin and rooty. These are enough for our investigation right now.



Login to the ssh session with the found credentials.

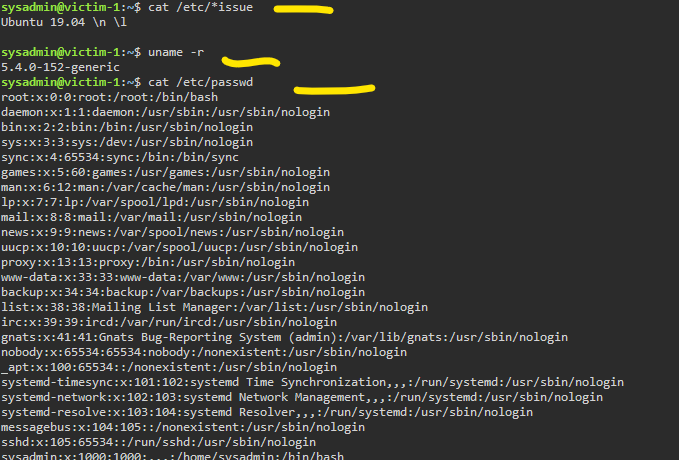
Looks like we’re in ssh now…

Cat out the /etc/\*issue file just to see what version is running, if tis doesn’t work, try “release” instead of issue to get similar info.

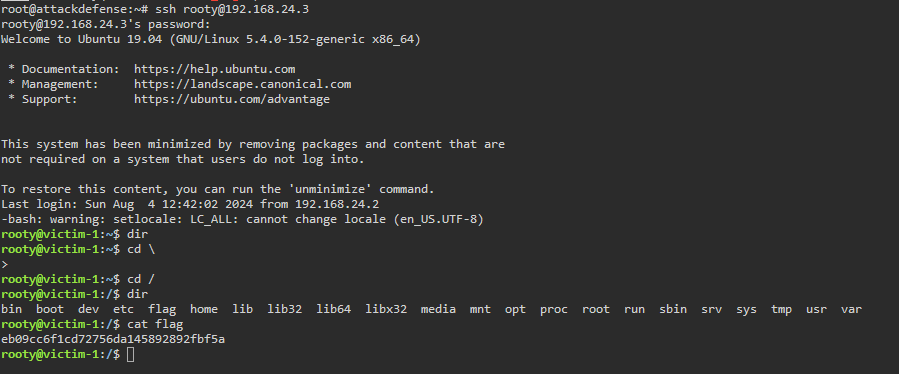


See uname -r for info on the service running.

More useful, we can see the info in the /etc/passwd file



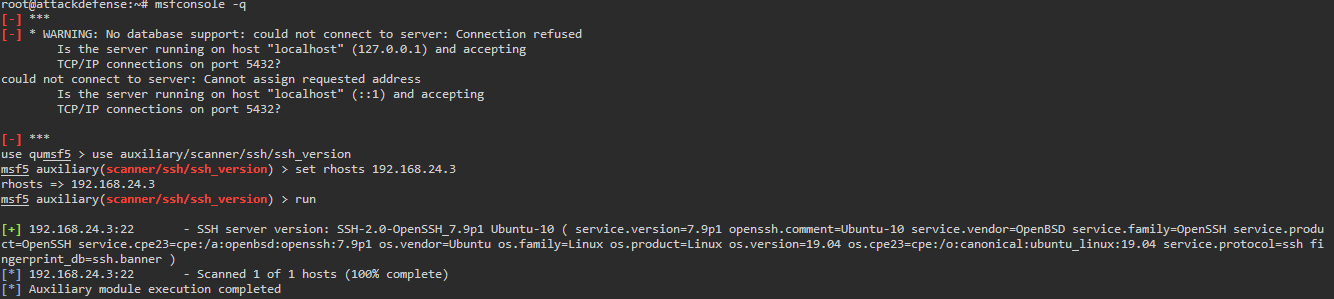
We can access the root directory with the rooty user, and find the flag in the home directory, as shown below



That’s nice and all, but let’s move over to msfconsole and run a scanner to see the ssh version going on here.

This is kind of a bonus, to not rely on hydra and know how msfconsole allows for similar functionality.

This reveals to us openssh\_7.9p1, which can add to further enumeration.

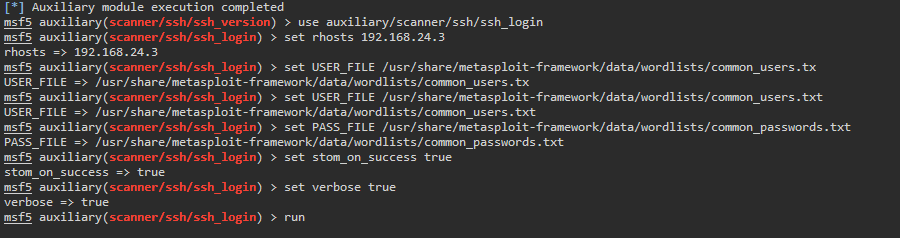


With the version figured out, let’s scan for credentials that’ll get us in.

This is basically the same functionality as using hydra to crack credentials, but we can do it with an aux scanner in Metasploit too.

Set up the files for the username and password.

I messed up and wanted to do “stop on success” in the settings too, but did a typo.



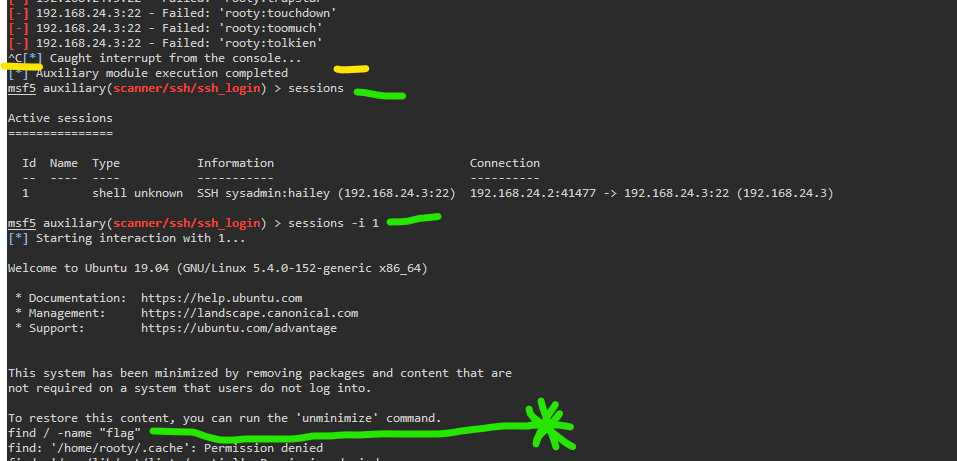
Since I did the typo, I uset ctrl + c to stop the scanner after getting enough credentials

Start a session with the credentials

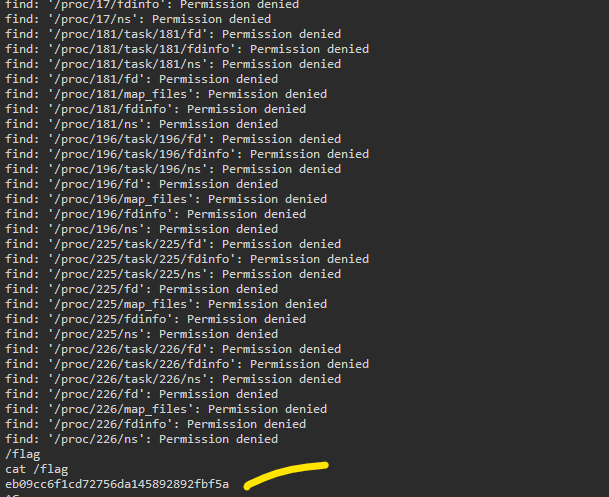
Open up sessions, (shows we are in as sysadmin with the password of haliey)

Command to interact with session 1

Now, let’s hunt for a file with the name of flag.



The results of the ‘find’ command



We get a flag file and a flag code.

That’s the game, ladies and gents.