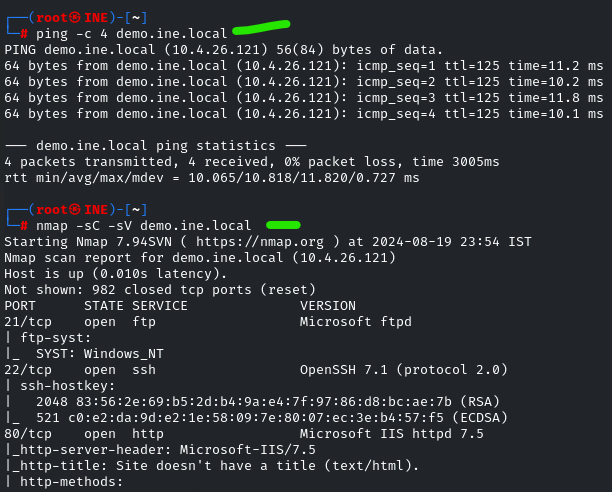
Starting, we need to ping the target to see if it’s active (the lab’s stability is very bad… so nothing will work if the service is down)

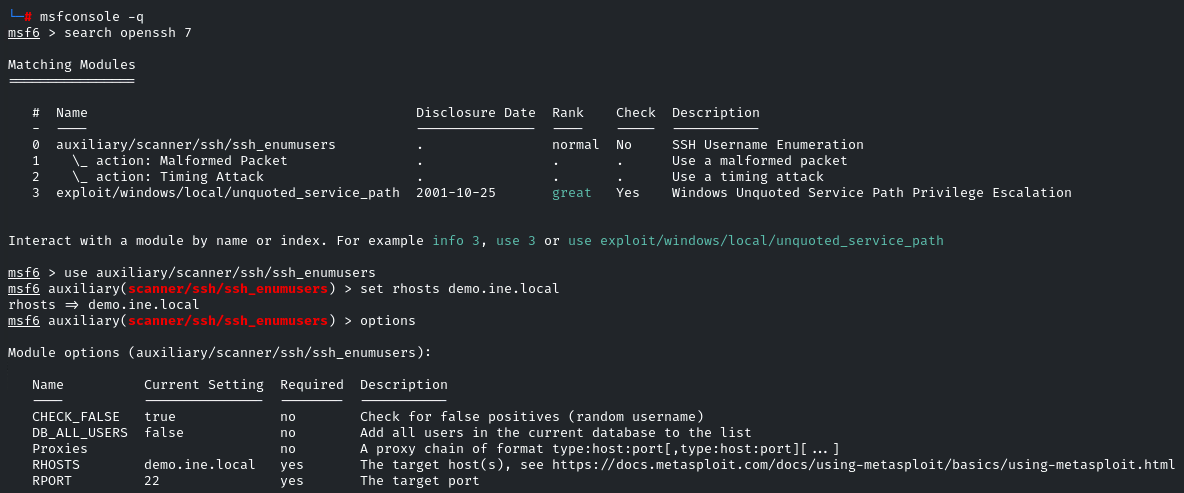
Basic service version scan follows…



Assume we are assigned the task of investigating ssh.

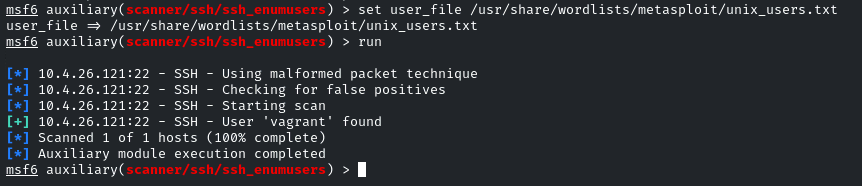
First, we need to run a scanner to see more data.

Command: use auxiliary/scanner/ssh/ssh\_enumusers



We’re hunting for usernames, so we need a name-list to plug in

The results below show “vagrant” as a hit. Darn shame the color coding on the left makes the [+] hard to see.

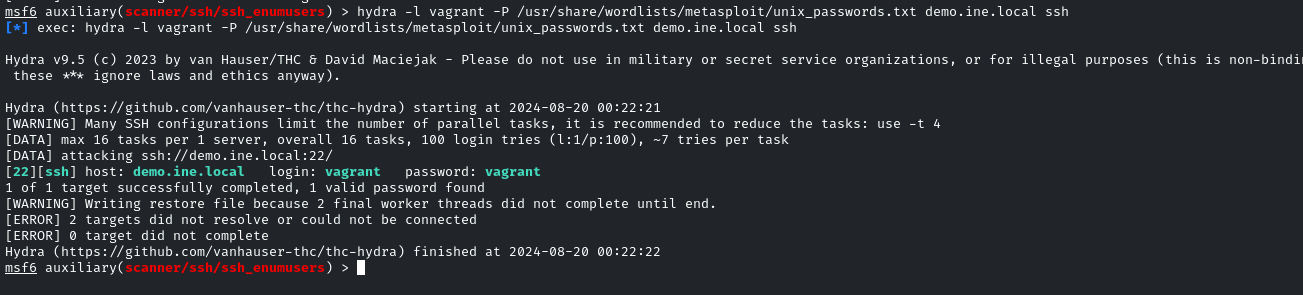


The scanner ssh\_enumusers helped us find a username, so we can simplify our hydra cracking process.

Command: hydra -l vagrant -P /usr/share/wordlists/metasploit/unix\_passwords.txt demo.ine.local ssh

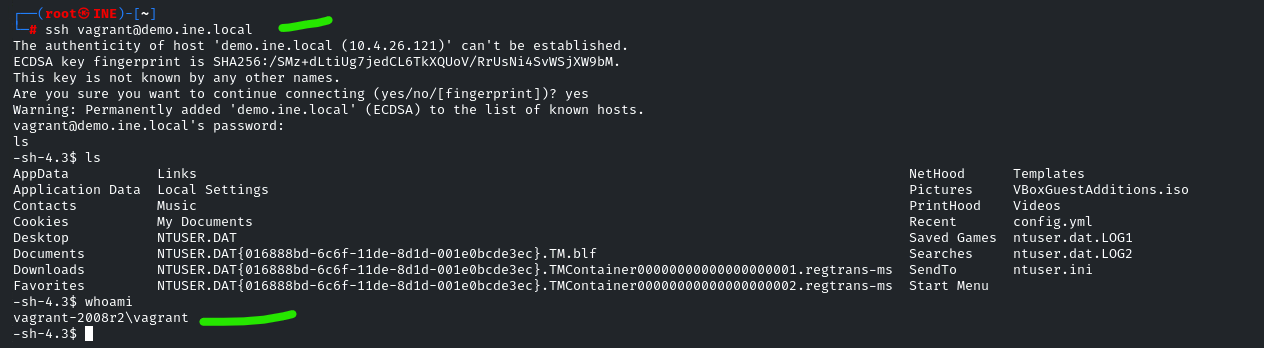
Note the small “L” to indicate a login name we want to statically set. A big “L” is for a list. Same with capital or lower case “P” for passwords in hydra.

Below, the output has login and pass both as vagrant



We can now login with the ssh service.

This is a no-tricks added interaction, like logging in normally, since we now know the username and password combo



The above command line’s second green indication marking shows the connected shell session on the target system, albeit not a very strong visual indicator for this exchange occurring.

Abstractions aren’t exactly visual in the world of comp-sci, after all…