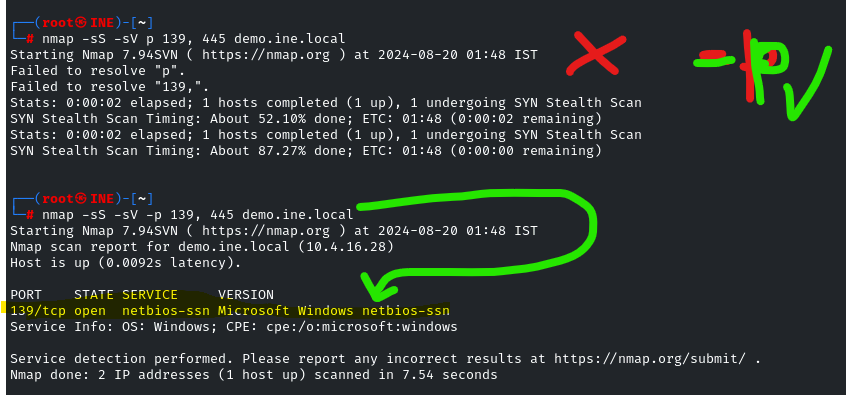
Scenario: you’re tasked with scanning SMB vulnerabilities on the target demo.ine.local.

You’re trying to get the hashdump of the Administrator account on this device.

SMB is usually on two normal ports, 139 or 445, so let’s indicate both in our scan…

Um, not using “p” alone, but with “-p” to indicate ports. Easy mistake in the top section…

Anyway, we ding it’s running on port 139.

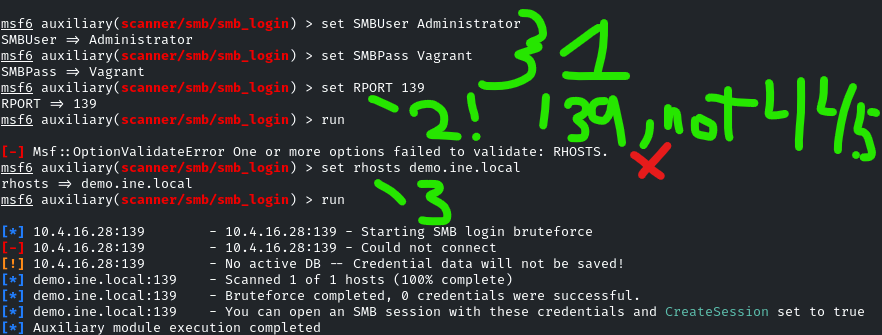


We could run a hydra crack with something like : hydra -L wordlist1 -P wordlist2 demo.ine.local ssh.

We’ve done like three labs in a row reiterating that, so I’m just skipping to new content. So, assume we cracked the credentials and known the username is Administrator and the password is Vagrant.

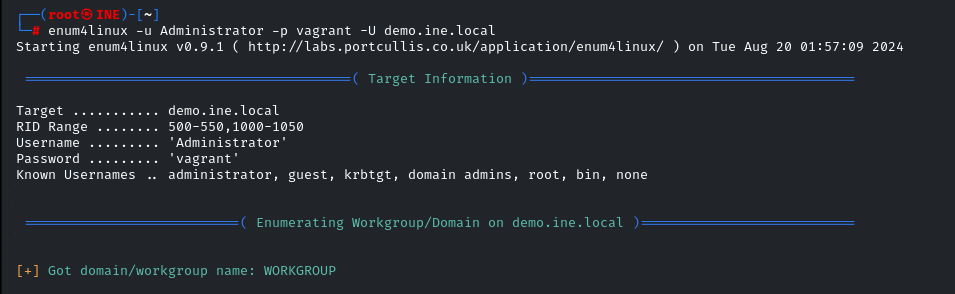
We can use the auxiliary module smb\_login to set up a session.

Note that, before, we confirmed that smb is running on 139, so we need to change this from the default 445 in the module. Um, and set rhosts too. I was stupid and earned an “x” by forgetting to set the rhosts before trying to run.

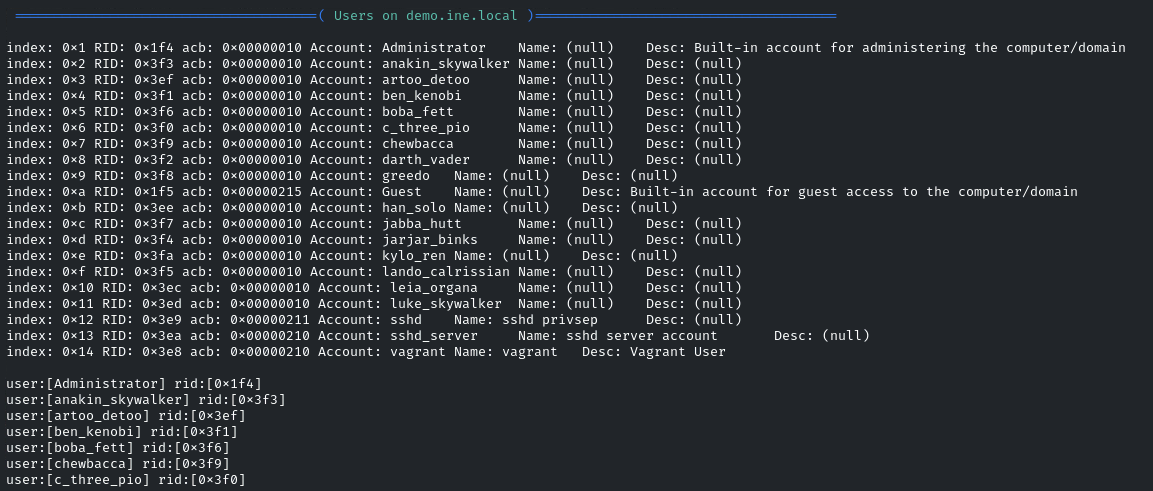


Alright, so we’ve confirmed we can login with those credentials. Now, here’s what we’re actually focused on: enum4linux.

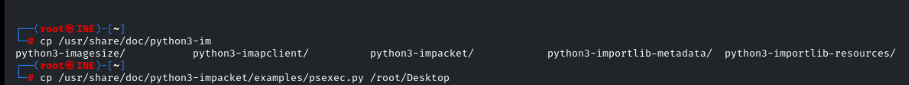
Command: enum4linux -u Administrator -p vagrant -U demo.ine.local



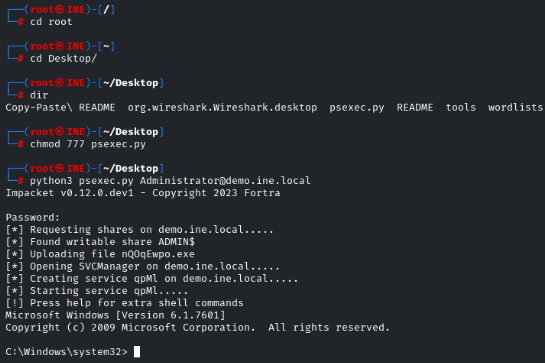
The output shows a bunch of user info… this data is modeled after a bunch of movie characters, it seems.



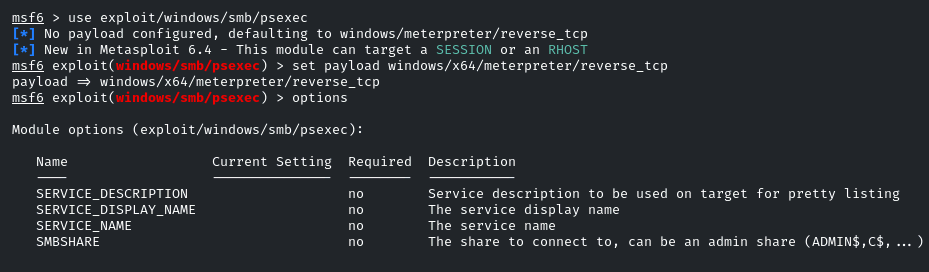
Use the screenshot path to copy psexec to a working directory. We’re messing with it to get extra maneuverability on the target system.



Give all privs to the file so it can be executed and activate it. On a targeted service. Here, we have demo.ine.local vulnerable to this. How do we know it will work? This is just an association you have to memorize: smb active? = try psexec.py

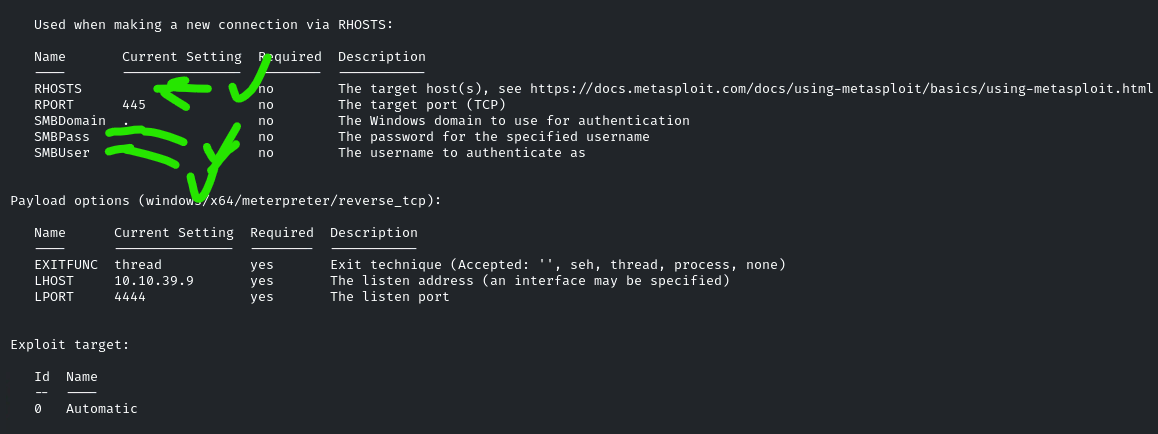


Set the correct payload depending on the 32 or 64 bit infrastructure of the target

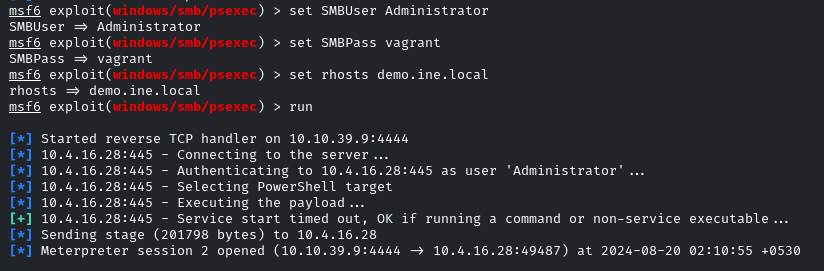


Check the info to make sure you got everything you need to run psexec.

We need a target ip, username, and pass, which we got already.



Setting the info and running it



Running psexec gives a meterpreter session.

From there we can get a hashdump, which is considered out objective here.

