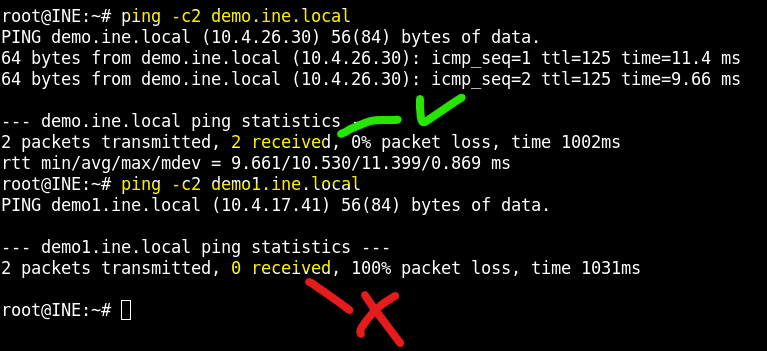
Start with the target demo.ine.local

We want to grab a flag that’s somewhere on the administrator’s account on this target.

First, let’s ping it to see if it’s up.  
note that demo.ine.local is reachable, but demo1.ine.local is not.

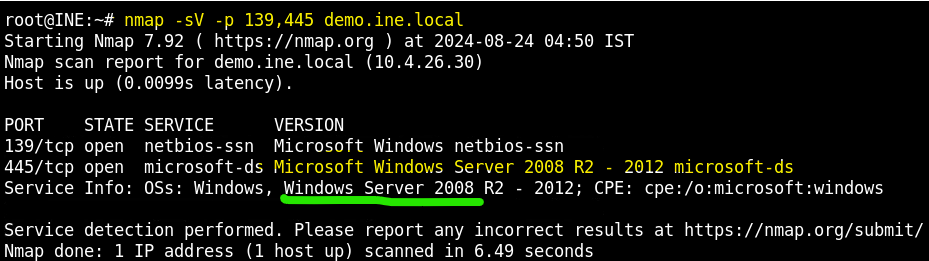
(this is just to show what the negative output looks like, see the red “x” where we get 0 packets received)

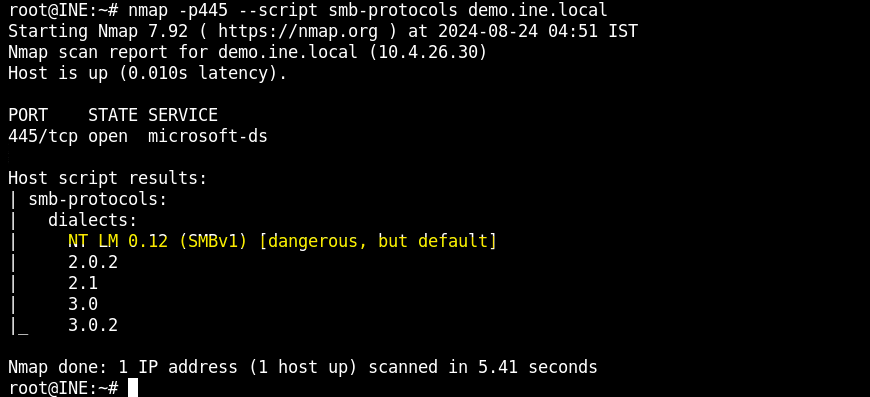


Scenario update: our team is delegating different tasks to infiltrate this target. Your target is SMB. (this is similar to another lab I’ve done before, but this is a unique instance overall, just happens to overlap with a lot of the same process.)

SMB can be on 139 or 445, so we scan both of those.

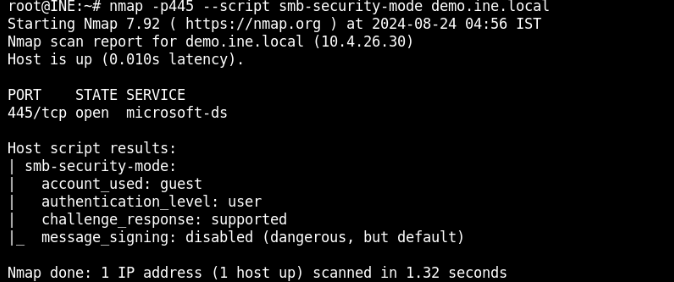
We’re not actually interested in netbios, so 445 looks like the correct smb port, given the OS information of running a windows “Server”



FOR REFERENCE, see what smb protocols are active with the screenshot script scan

That smbv1 is a dangerous default that’s a good finding for exploits. But no time to get bogged down in specifics. We want more info. Let’s see if we can get in with the default guest account.

A guest account is automatically available for SMB on windows. The following scan sees if we can login and get info from that account.



Similarly, we can try logging in anonymously by just connecting to the smbclient indicating a space for the login, and targeting the ip address of our desired machine.

This is also called a null session, as we give no value for the login or the password, just hitting enter to continue.

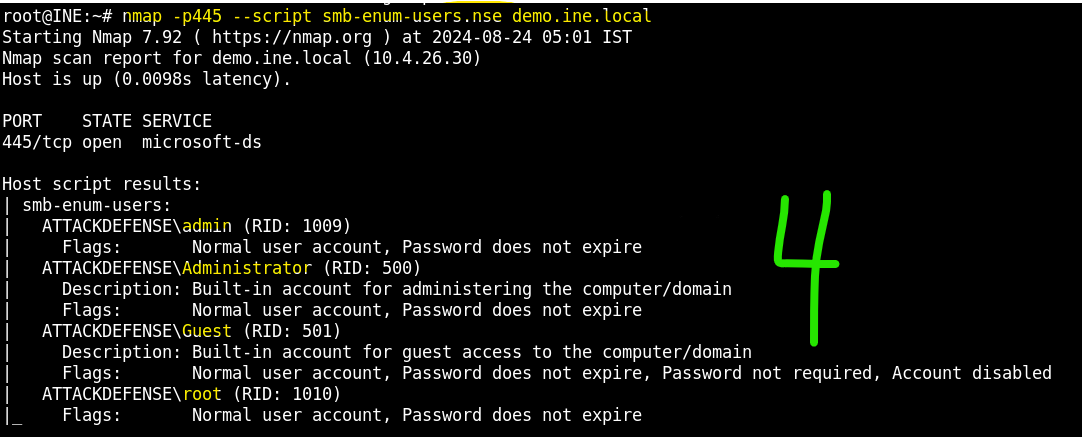
Note the hilit part showing anonymous login successful



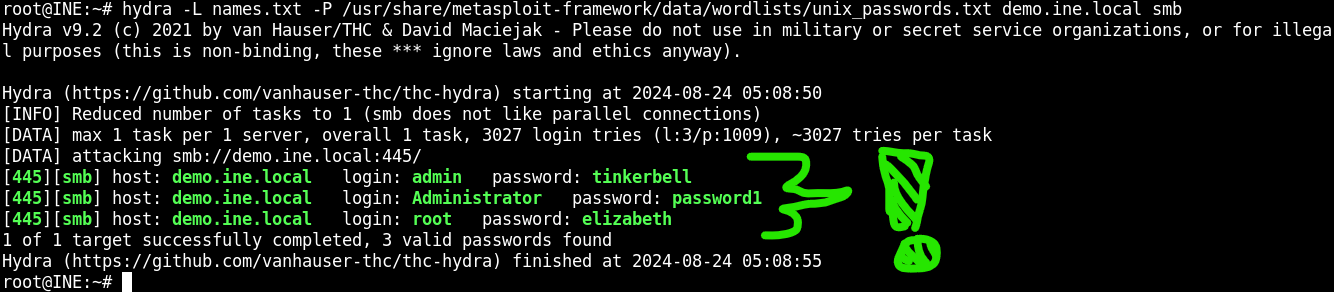
Finally, and this is more practical, we want to enumerate the users available with the screenshot script

Command: nmap -p445 –script smb-enum-users.nse ip.address

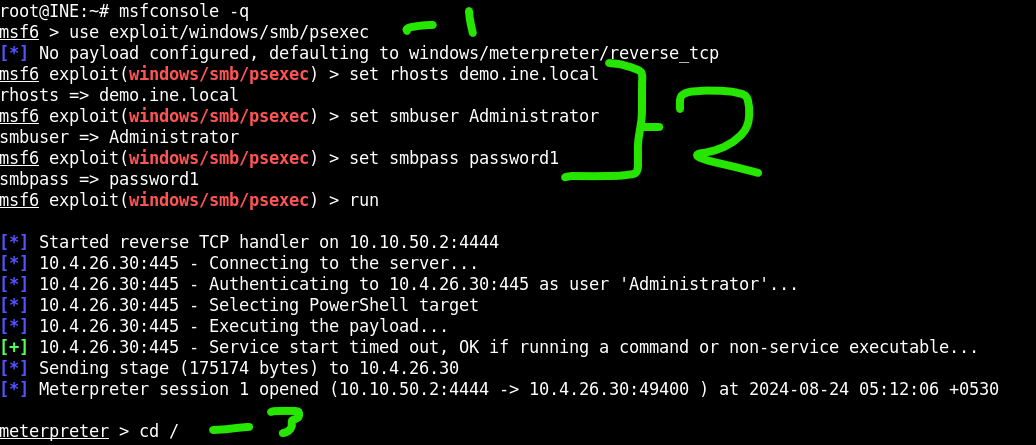
We see 4 accounts returned. Our main target is the Administrator, to get the flag on their account.



We make a short text file, names.txt, containing these 4 names. Then we brute force with hydra to get the passwords for smb login.



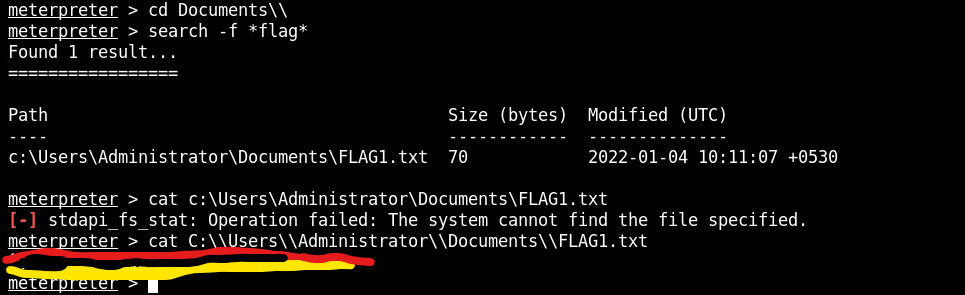
We can now use the username and pass of administrator in the psexec module to exploit smb and get into the target machine.

1. Start up msfconsole
2. Set the parameters for smbuser (administrator’s username), smbpass (their password), and rhosts to the target ip address
3. We get a meterpreter session, and cd into the main directory. From here we can navigate files

…

After getting to the Administrator’s documents, we got a lot to sort through, so let’s search for any files containing the name “flag”

Command : search -f \*flag\*



Be sure to escape the slash characters so you can use the right absolute path to the target file and cat out the contents.