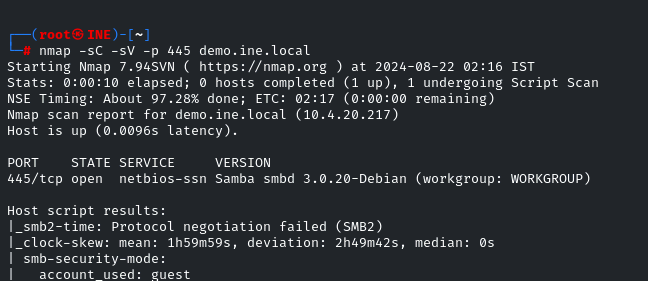
Start with an nmap scan of port 445 on the target demo.ine.local. Our goal is ultimately to find the info on hotfixes and versions of whatever server is running here so we can plan further attacks to evade intrusion detection systems.

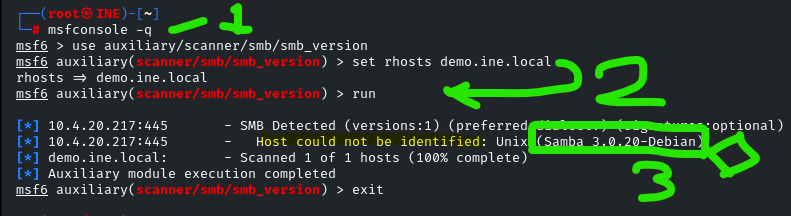
Our scan shows samba is running as a server.



We can get more info about samba with the smb\_version module in Metasploit.

Note 3) though it says “host could not be identified” we get the best guess, that it’s Samba 3.0.2debian.

We make note of this and go onward.



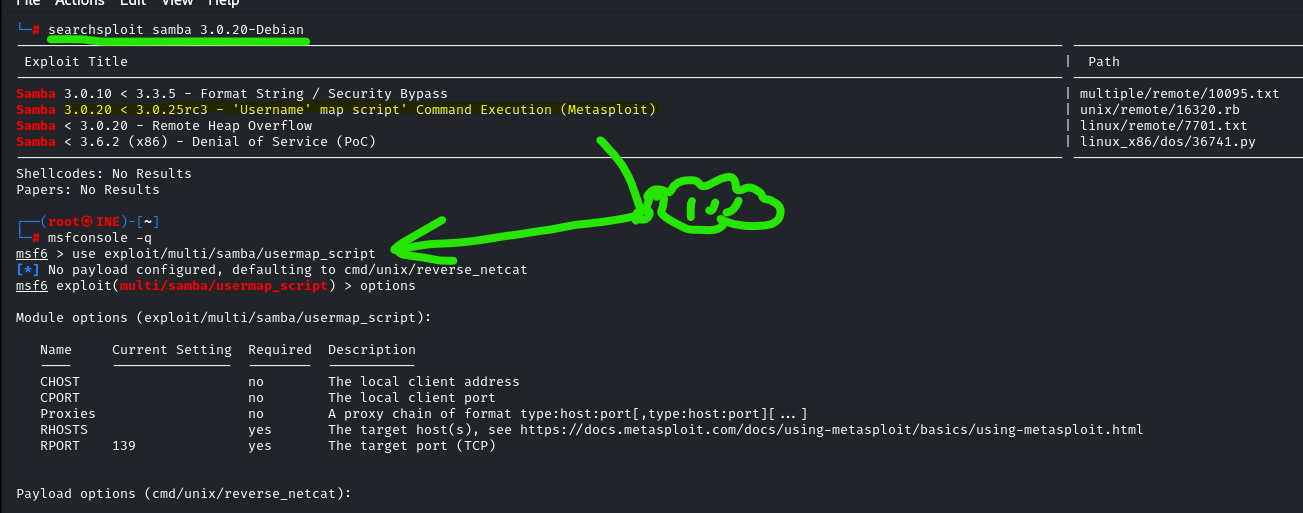
We take the version found and plug it into searchsploit.

We get the 4 results under “exploit title” where “samba” is in red on the left of the screencap.

The next part seems like a magic association, that the hilit one is correct for using in this scenario.

How on earth does the hilit item link to “usermap\_script” when it’s a bit of a leap to truncate the name into that…

I’ll explain. The hilit module, 3.0.20 …. Command execution (Metasploit) should first come to our attention because it’s ready-to-use in Metasploit. We’d need to research this online if we don’t know it.



Here’s the exploit DB page from online, actually looking at the module.

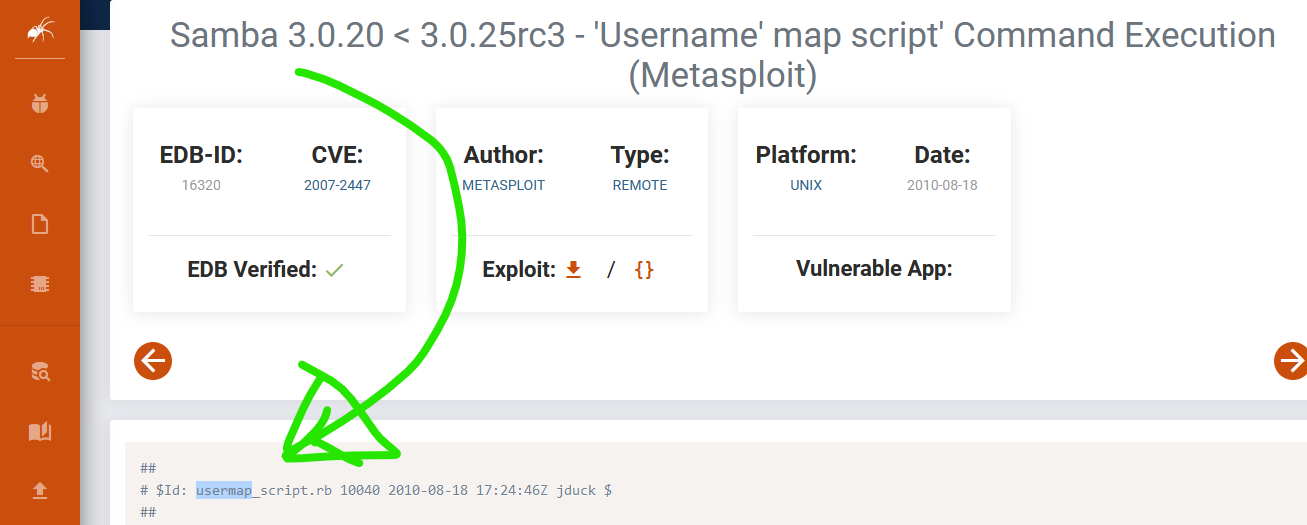
In the $id note, we can see this is associates with the program name usermap\_script.rb.

This is the id in Metasploit, making the association between the title and the module name. Sadly, this is a bit of obfuscation and just poor structuring where titles are not directly associated with module names within searchsploit or msfconsole in a clear way, but whatever, I guess.

You need this name and path : exploit/multi/samba/usermap\_script

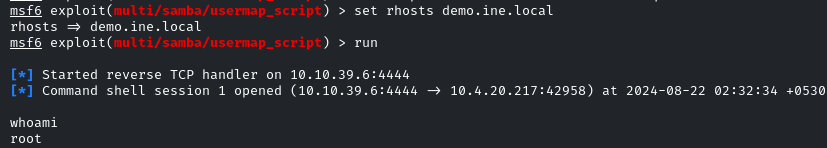
to even use the module, so this should be pretty important… again, just magic your way into memorizing everything and try harder, bro.

Also, the scanned version, 3.0.20 Debian, matches the version range indicated, so it’s valid to use, probably.



With our witchcraft module in Metasploit: use exploit/multi/samba/usermap\_script

Set the rhosts to the target and run that.



And we’re root, so we win.