…

Reminder for startup:

Start up msf console and the postgresql database to keep track of data

Command 1: Service postgresql start && msfconsole -q

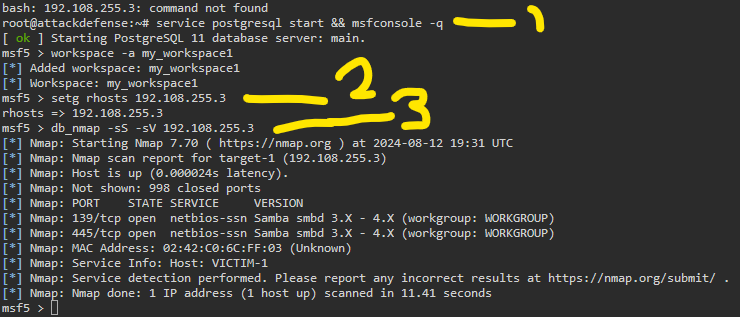
Then make a new workspace and give it a name, here my\_workspace1

Command 1.5: workspace -a my\_workspace1

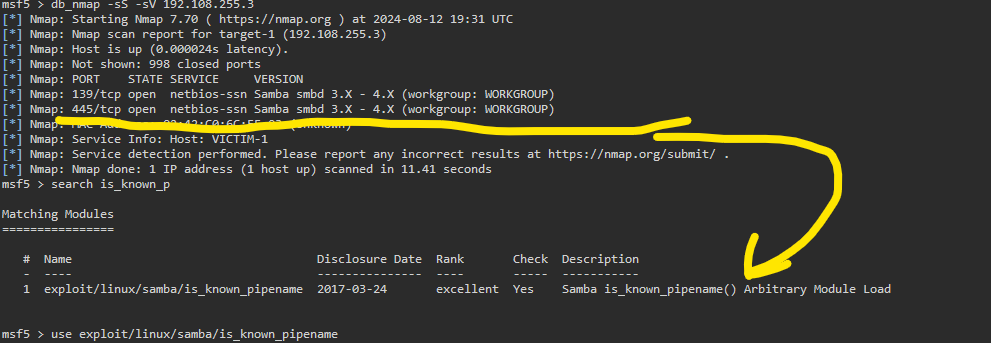
2) set the global rhosts

3) do a db\_nmap scan within msfconsole

Command: db\_nmap -sS -sV ip.address

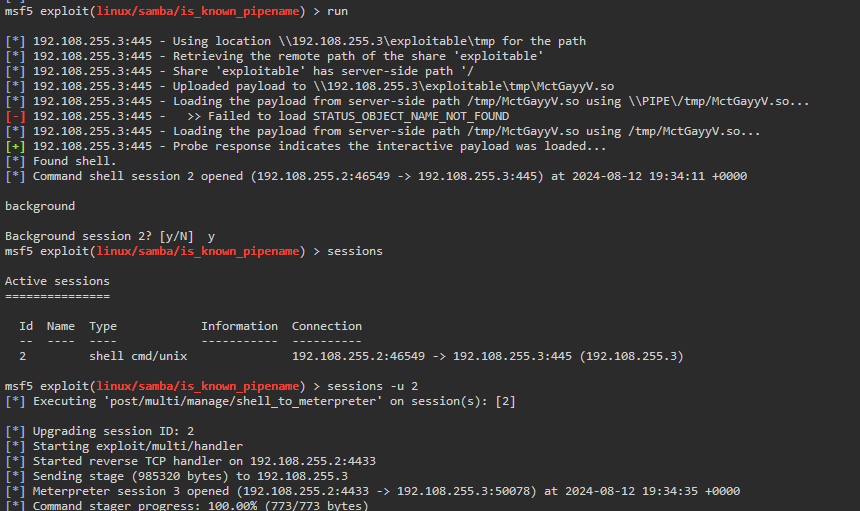


Samba is open on port 445, http, but magic your way into knowin this is vuln. To is\_known\_pipename.



We already set our rhosts so we can run it and get a session, as shown by session #2 below.

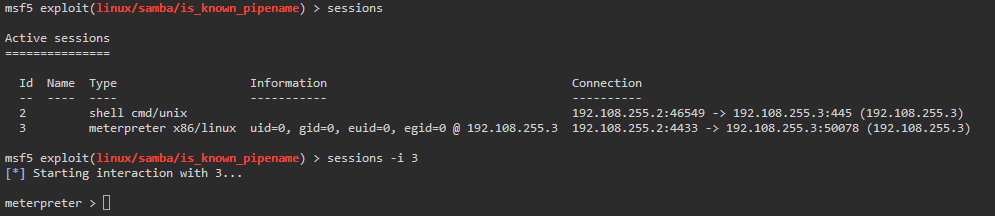
I ran this once before, but cleared it and got a neater console layout for the screenshot, which is why it isn’t #1.



Above, we use the command: sessions -u 2

This upgrades the session and opens another session which we see below.

Note how #3 is meterpreter x86



Basic enumeration shows we have root.

We can dump contents of /etc/passwd ,which is our goal.

