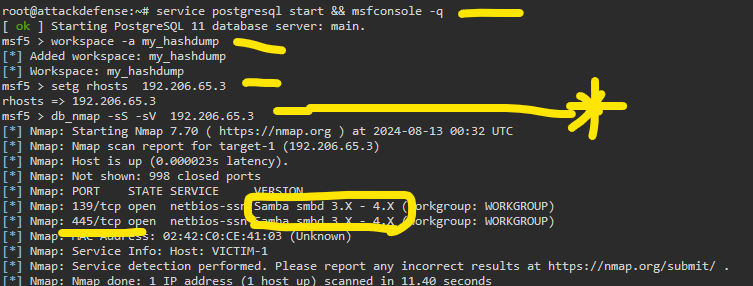
Start up an msfconsole session with postgresql,

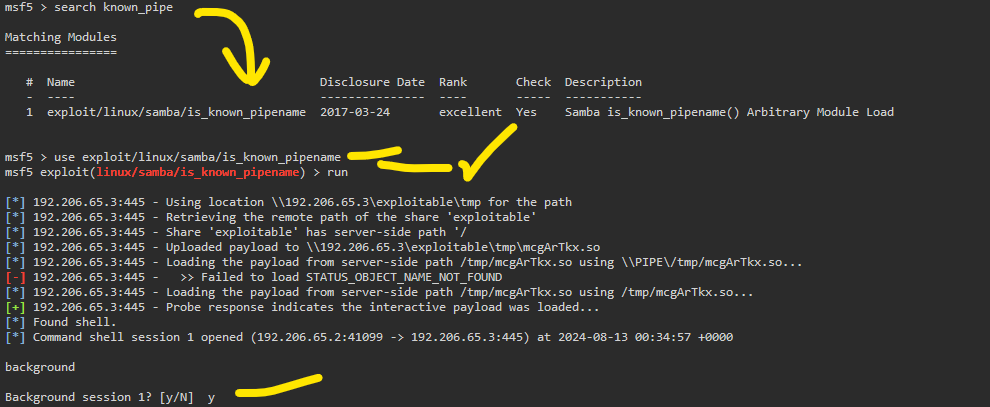
Normal setup with a workspace, my\_hashdump.

We set the global rhosts to our target ip address, then do an nmap scan within msfconsole via db\_nmap

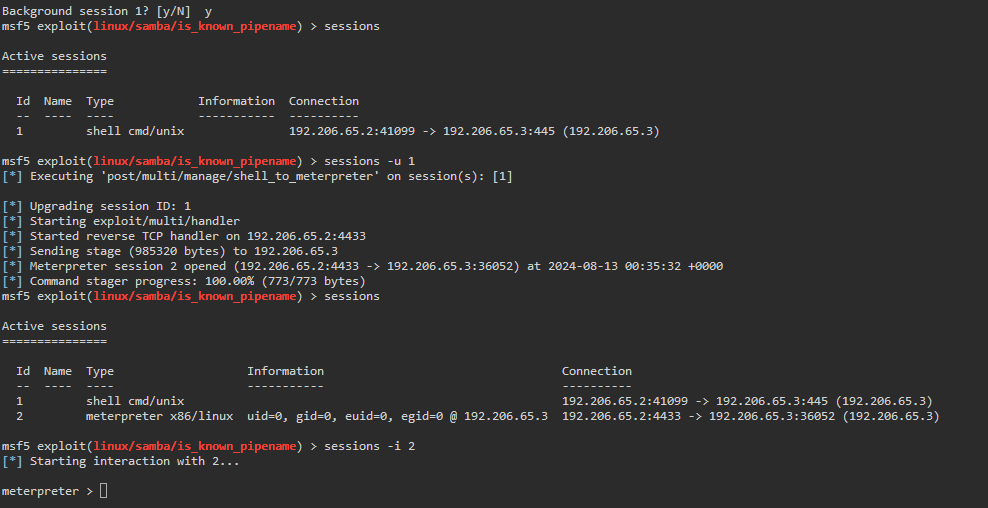
This is another repeat of the samba 445 exploit, drilling it in your head that you need “is\_known\_pipename” to pop this service.



Open a session through the is\_known\_pipename exploit that works on this samba version (3x – 4x)

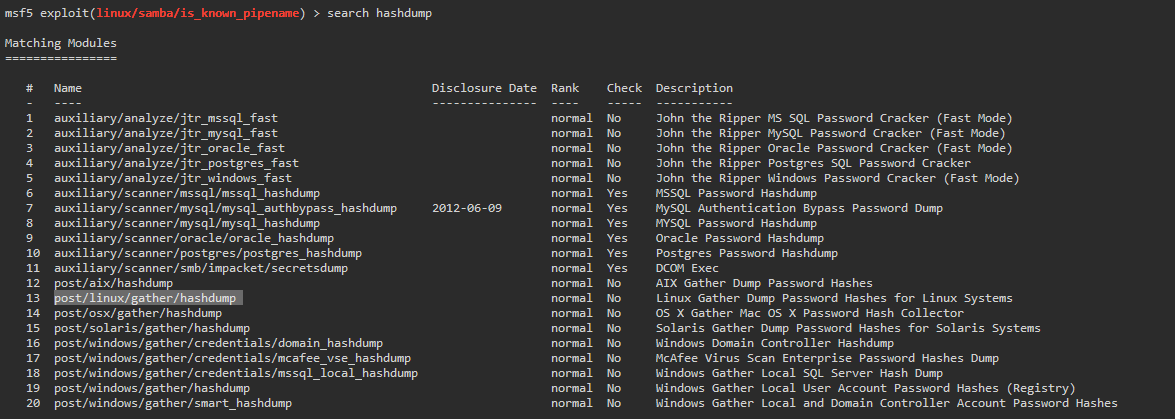


Put the session in the background, and upgrade it to spawn a meterpreter with command sessions -u 1.



With our way opened, we want to use some post-exploit modules to get data. Namely, hashdump

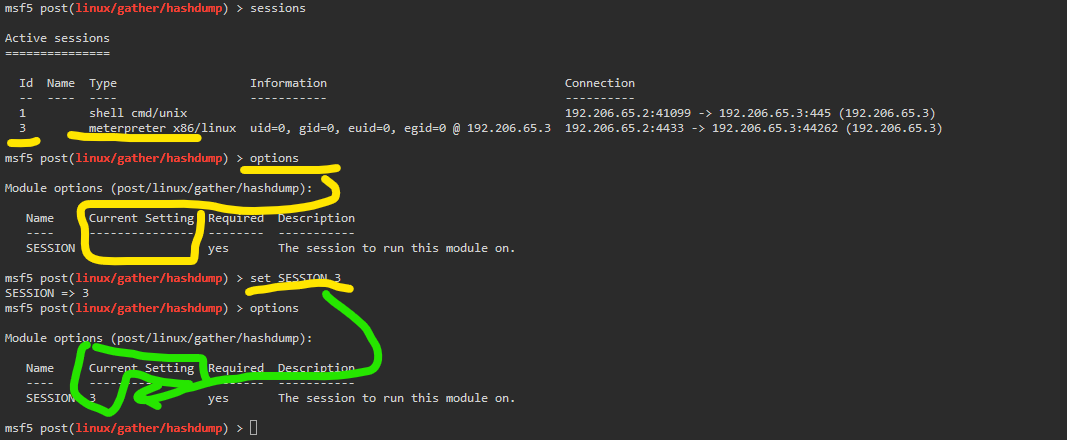
Command: use post/linux/gather/hashdump



We can check our sessions with command: sessions

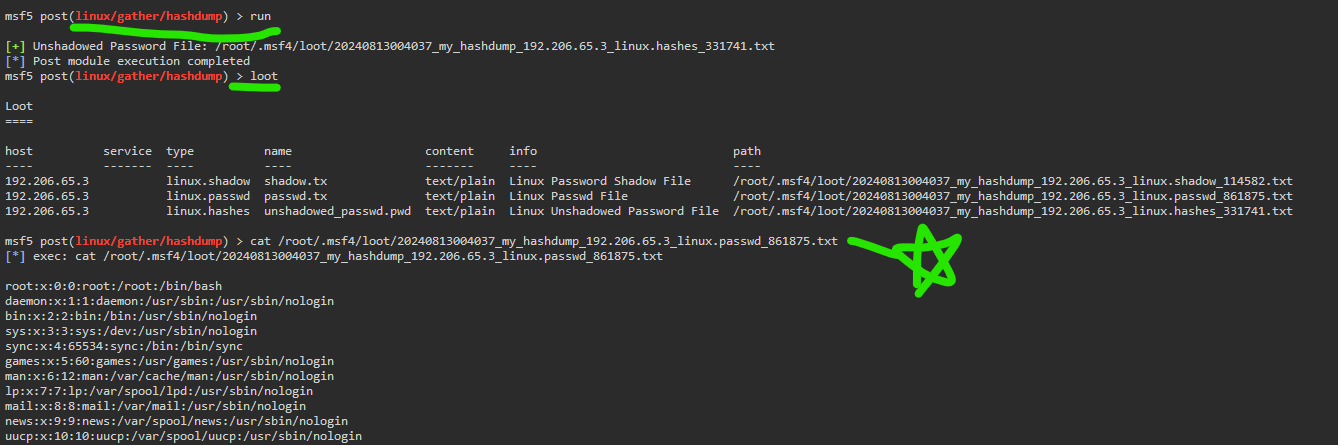
We want to set the option command: set SESSION #

To the number of the meterpreter session, in this case, being id #3.

Further, we confirm the option is set by typing in command: options

Run the hashdump, it’ll give you an output textfile or a few. We can check the outputs generated in msfconsole by the built-in command: loot.

We see where our post-exploit data results from running hashdump are when we check inside our digital loot-bag.



That’s the end of the demo