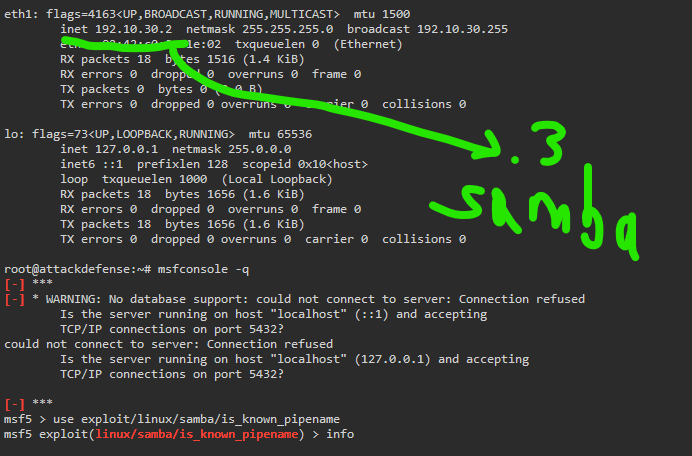
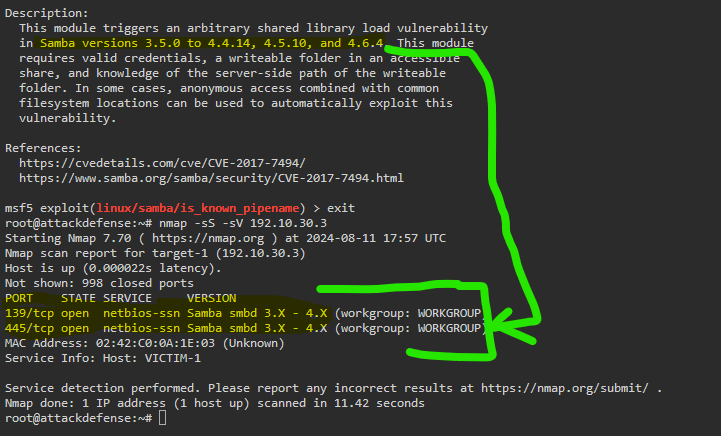
We are trying to upgrade a shell session to a meterpreter session

Assume we already did a service version scan and the targeted ip below is running samba

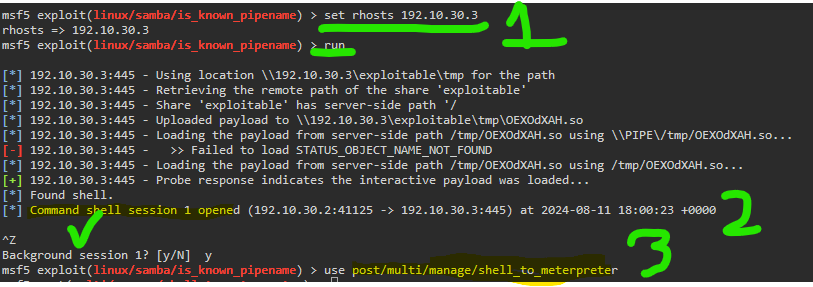


We can use used an exploit for a vulnerable samba server and already have a shell session from using exploit/linux/samba/is\_known\_pipename

We know it’s vulnerable because the versions described in the description of the exploit module match the fingerprinting we’ve done of the target system, having samba 3.x on it

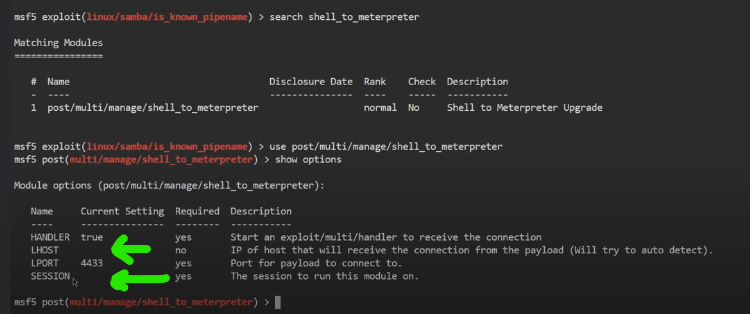


The below exploit will only have a shell on the target.

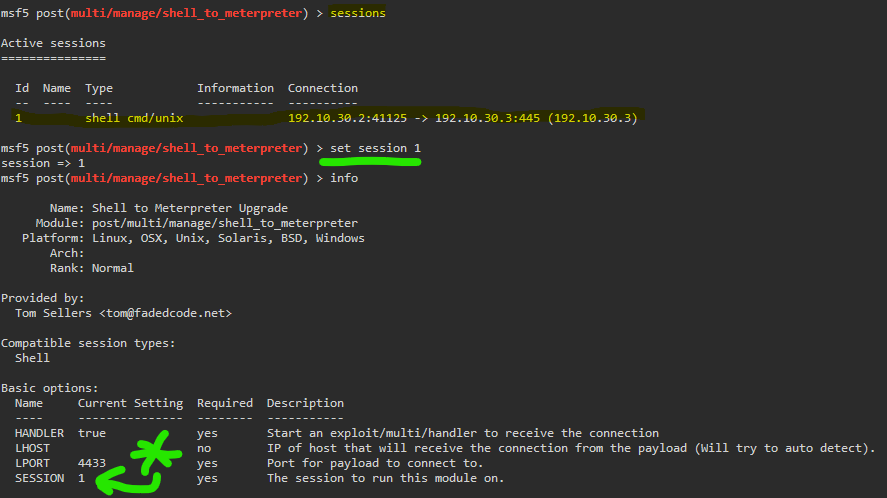


Below, you don’t actually have to search for the module to get the shell to meterpreter

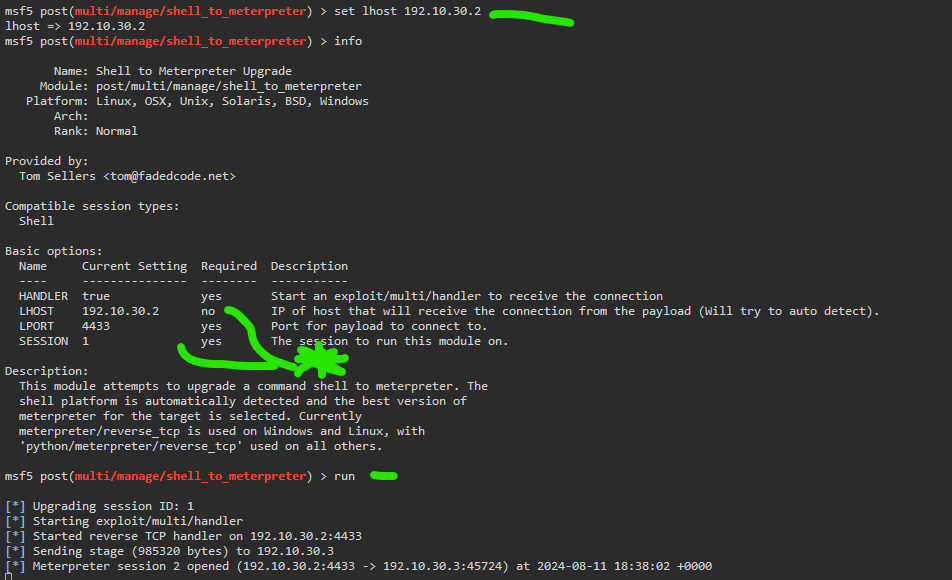
Set our session variable, and run



Running this is one way to upgrade the session.

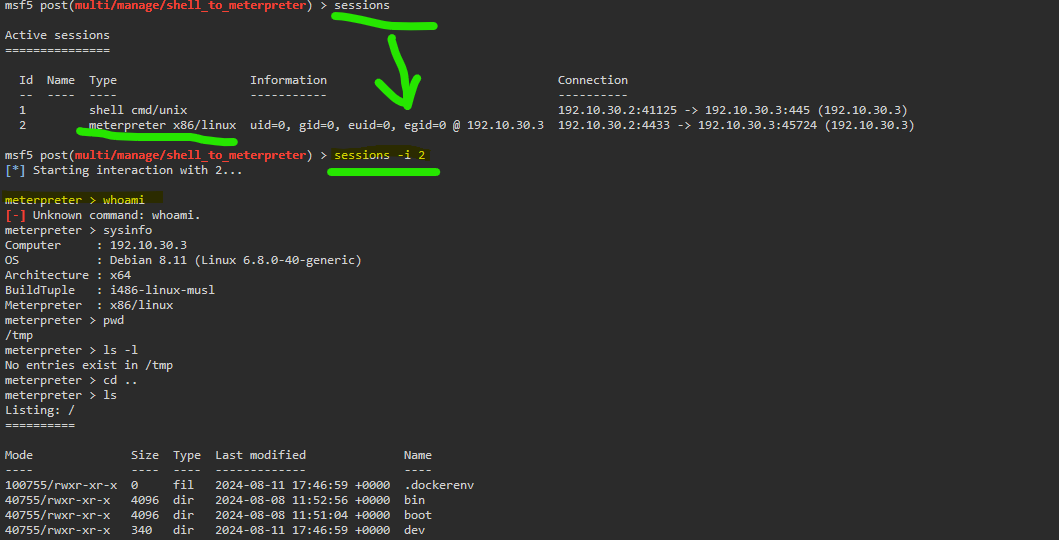


Make sure the lhost is set to the ip of your attack machine



Switch to the upgraded session

Command: sessions -i 2



Also, screencap mistake, it’s not whoami but getuid



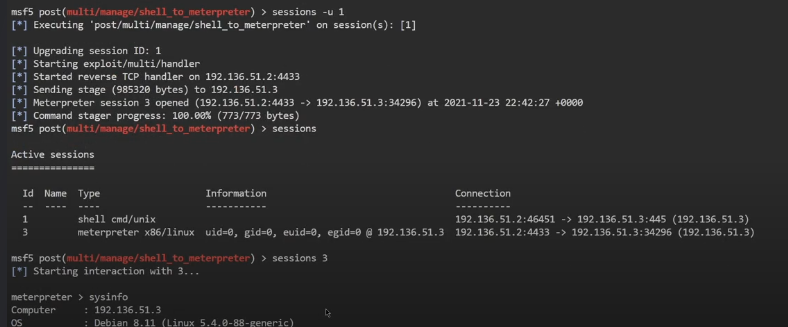
!!! ------------------------------ BELOW is treading similar ground from a different angle -------------- !!!

------------------------------ Clearly marked as an impractical demo ------------------------------

Alternatively, might be able to use command : sessions -u 1

Note that the active sessions below have the number 3.

The second session was done with the shell\_to\_meterpreter exploit, but that got overwritten with the extra command : sessions -u 1



We then have a meterpreter session on 3, and can get the systeminfo.