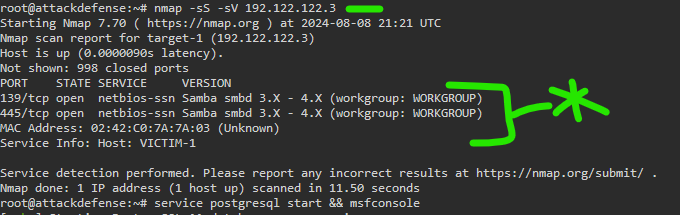
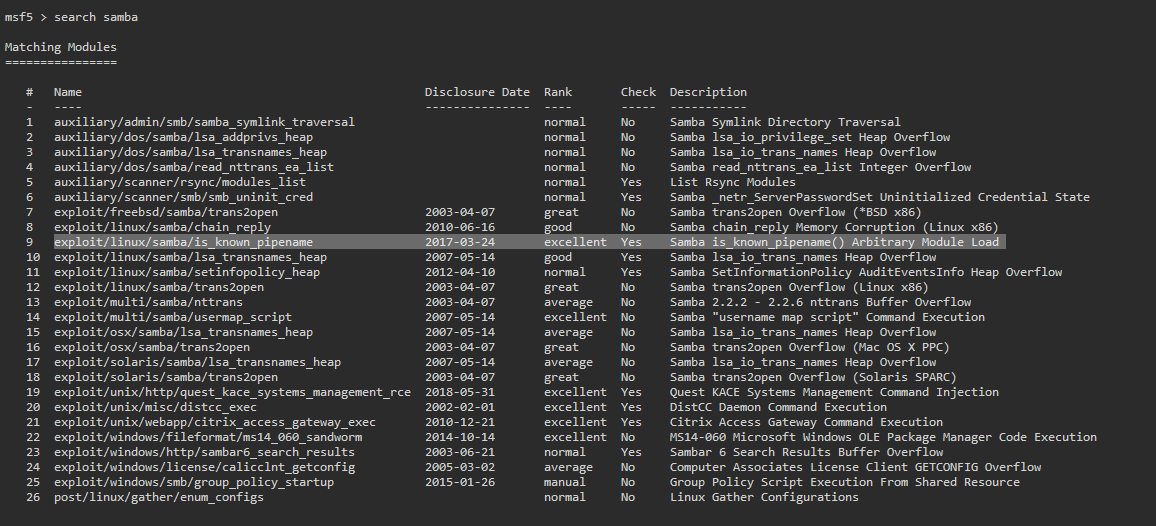
Start with an nmap on target ip address 192.122.122.3

We’re also searching for service version in a stealth scan.

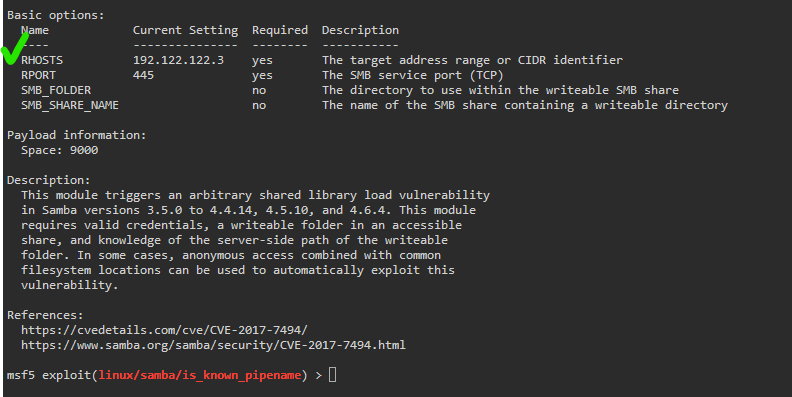
We reveal some kind of samba server up and running.

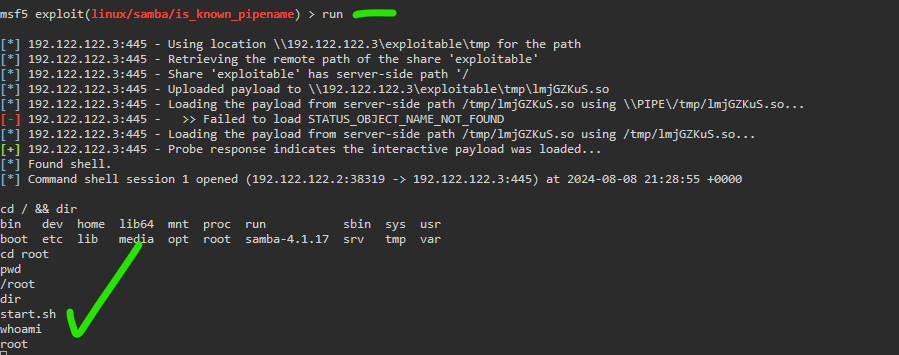


I am going to skip over an absurd amount of trial and error, and magic my way into the next step. Out of available modules, the one we want is exploit/linux/samba/is\_know\_pipename

There was no methodology for finding this other than the name, reading descriptions, and trying, thus the classification as “magic”.

Set rhosts, and if the rport is something non-standard, change it here. On our nmap scan, the 445 port was active, running smb, so we keep the default as it is.





No flag in this environment, but show proof of root with directory traversal and whoami printout.