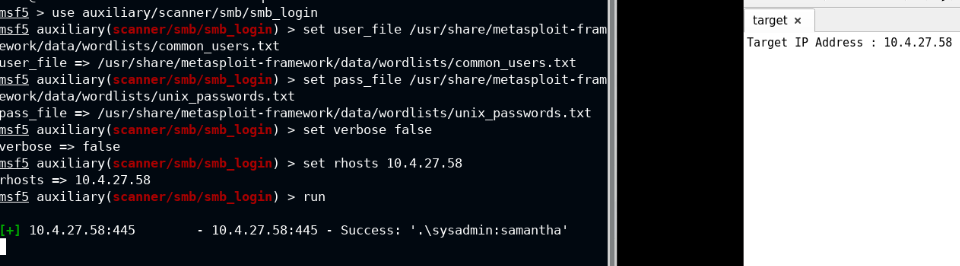
Starting scenario: smb is active on a target system, 10.4.27.58

We need to first brute force the credentials, which we can do with the exploit smb\_login.

Set the user and pass lists, then let it run.

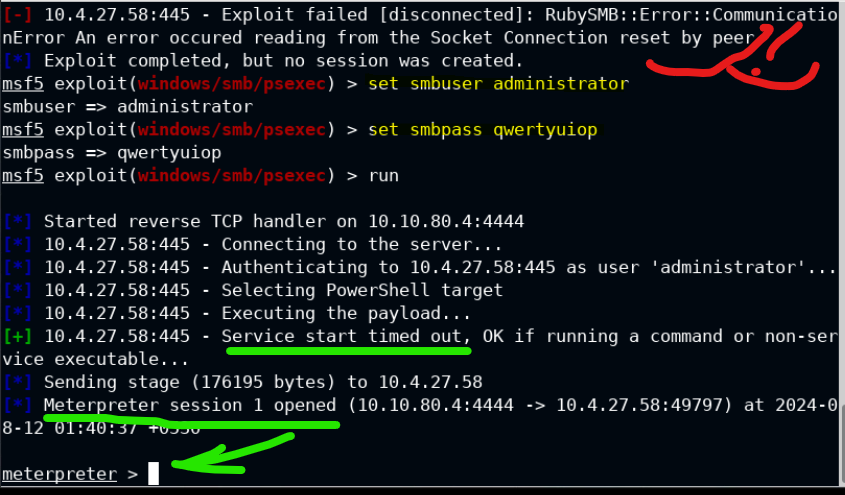
At the bottom of the related screencap, see how we found success with the sysadmin having the password “Samantha”



Next, use psexec to use our credentials and get in

The minus below shows that something went wrong with psexec. This is the output that is bad. Check that the user and pass match one of the positive results from our brute force.

In my case, I just had some kind of typo, thus the failure. I resolved it by setting the smbuser and smb pass parameters again before running. The bottom part of the screencap shows the success state, whereby a meterpreter session is opened.



From there, just navigate to find the flag, and that’s the game

