Starting scenario: we know an ssh server is on a target system

The username and password have been collected by a team member and confirmed to work.

Username: jackie, password: password

We can use the ssh-login to confirm we can get a session

(in screencap, the yellow diamond is setting up a workspace to contain data related to the current project)

Finally, we upgrade the session that is running

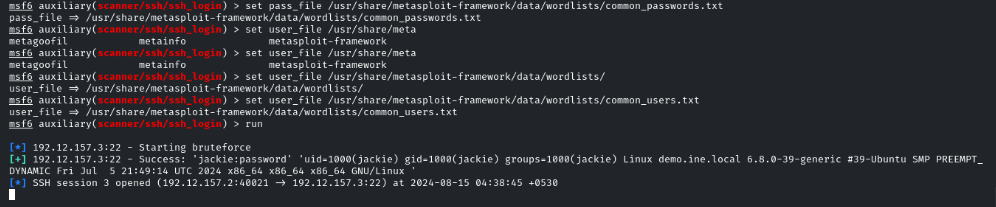


We put the meterpreter session in the background.

Scenario update: even though we’ve logged in successfully as Jackie, we are requested to check for other weak passwords and names. If one person is weak, others might be equally as weak on the same system.

Command: use auxiliary/scanner/ssh/ssh\_login

Set the user and pass files for the brute force, and run it.

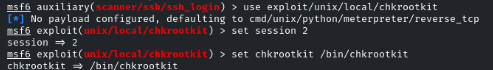


We get a success with Jackie and automatically open another ssh session with the credentials found.

Nothing else comes out of this though.

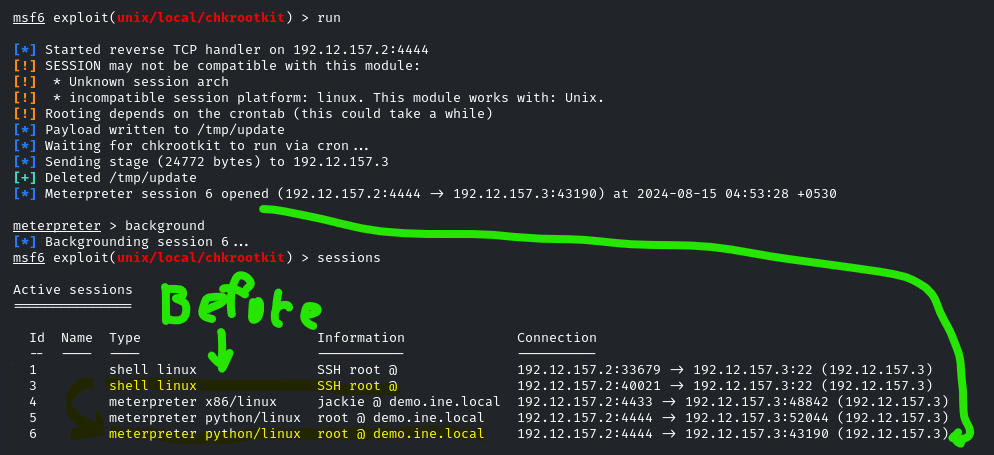
Moving forward… a teammate informs us there is chrookit running on the target.

We can use the following exploit to manage that



We get a meterpreter session upgraded from the shell session. Note that we were just the user Jackie before, but now we got a shell session, and then a meterpreter session as root.

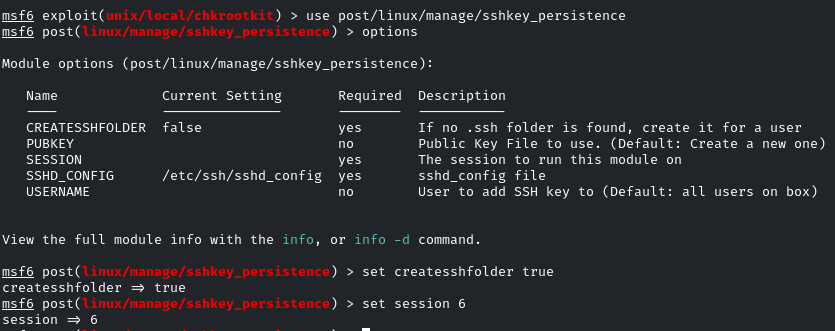
The screencap shows 2 copies of root for both shell and meterpreter because I ran the process twice in the testing environment.



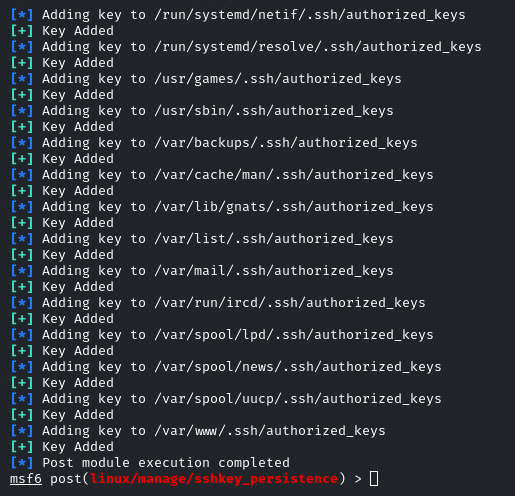
To maintain persistence, just memorize that you need command:

Use post/linux/manage/sshkey\_persistance

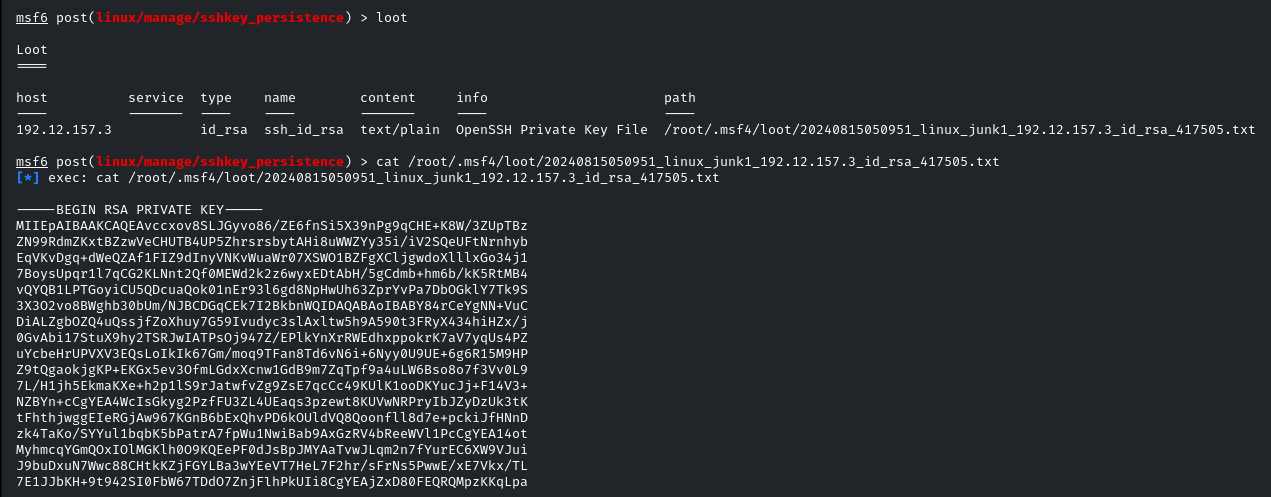
Create share folder, and set the session to the one with root and meterpreter, which is 6 in our case.



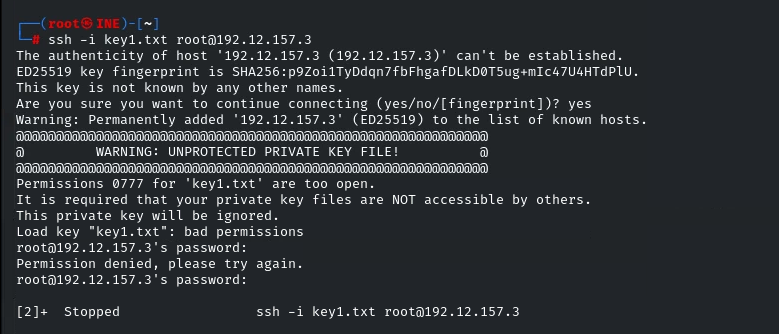
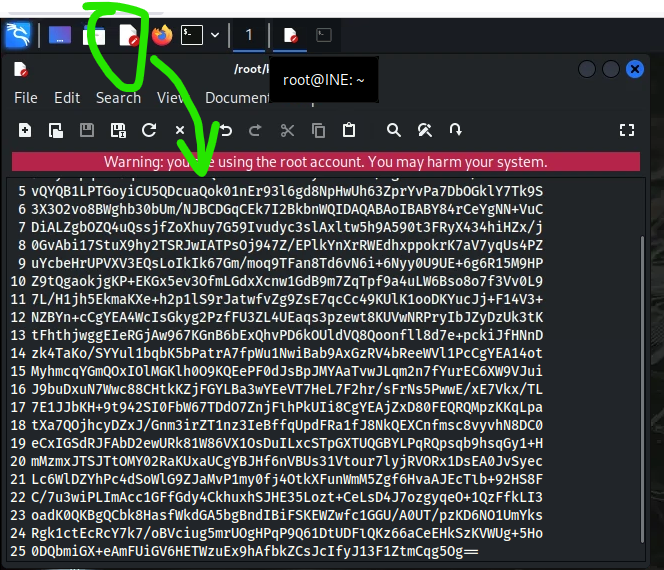
The output for running the persistence module will look something like this:



If we open up our loot file, we can get the ssh key



We can use a copy of this ssh data, like opening it in mousepad and saving all these numbers, for the purpose of manually designating the capture RSA key for future use.

Below is the graphic to actually use mousepad

This gets the ssh key, which we can use for further maintaining persistence by connecting through what would normally be an encrypted connection