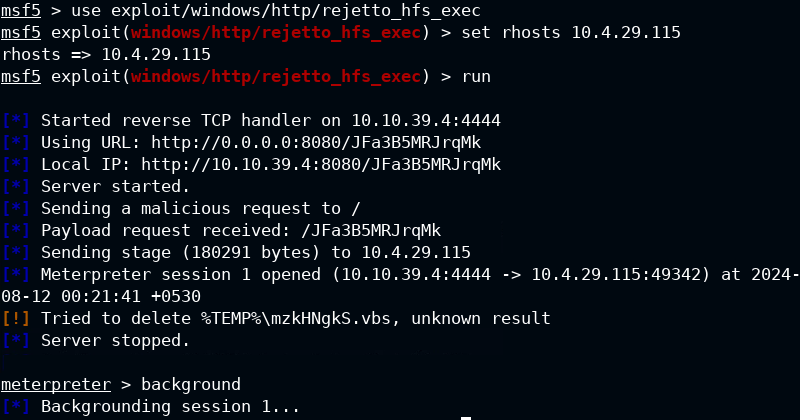
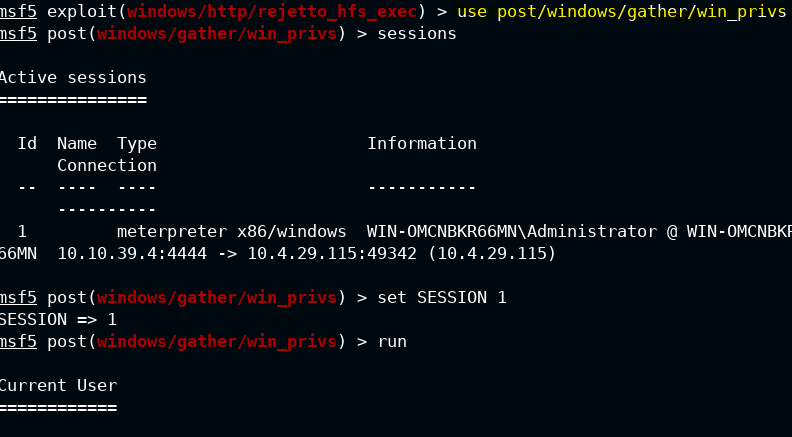
Scenario;

A teammate already fingerprinted this ip address target as 10.4.29.115

It’s running http file server, and we know it’s vulnerable to rejetto hfs exec, so we’ll use exactly that exploit to get a foot in the door

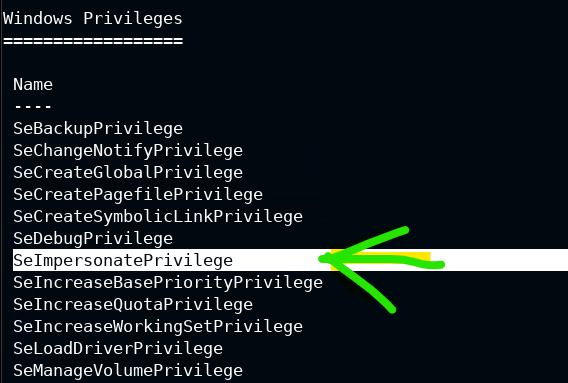


Put the meterpreter session in the background; get some data

Command: use post/windows/gather/win\_privs

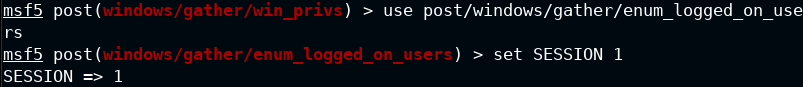
Win\_privs gives us a bunch of priv tokens that are available on the target.

We’re particularly interested in SeImpersonatePrivilege for escalation purposes

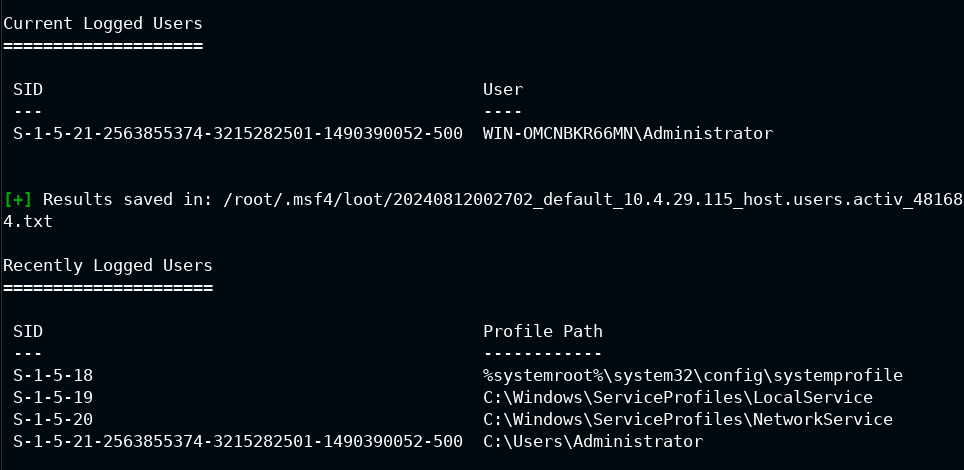


If we want to see what users are logged, we can use the enum\_logged\_on\_users.

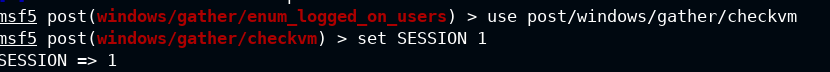
This will help as our list of others to escalate to or move laterally to



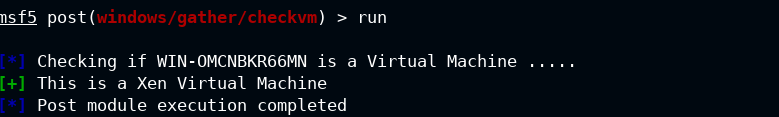
Example output below… last line shows users\Administrator



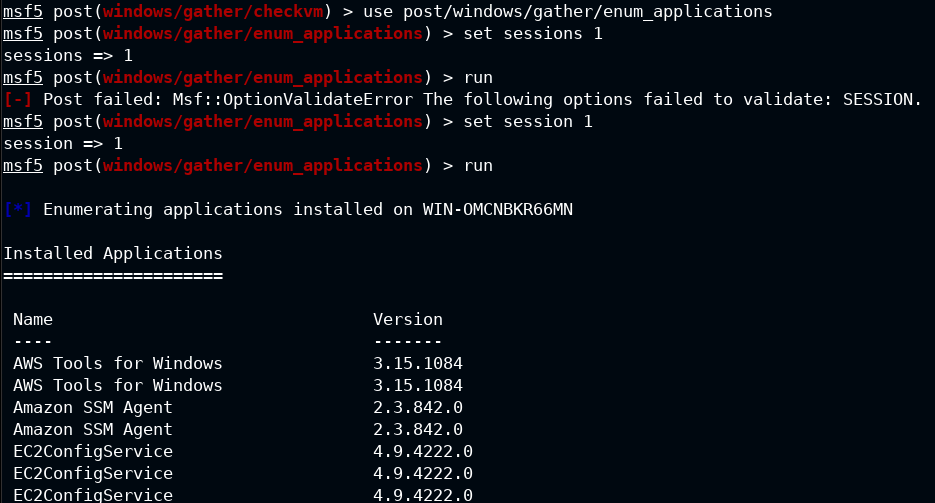
We might want to see if this is a VM or not, so we can use checkvm for that



Example output. Note the green symbol on the left, indicating a version has, indeed been found.



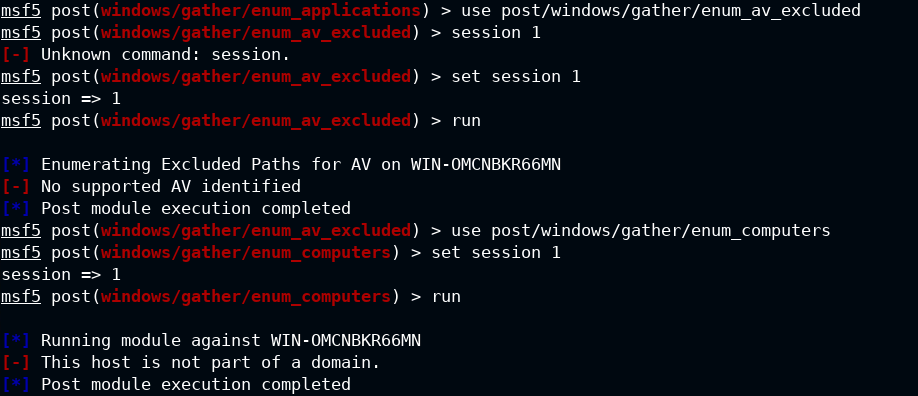
It’s a lot of info to see what apps are running, but if you have a purpose for it you can enum\_applications too. Instructors failed to explain how this was relevant.



Other non-explained info gathering for post exploit: enum \_av\_excluded.

Supposedly checks for antivirus dodging?

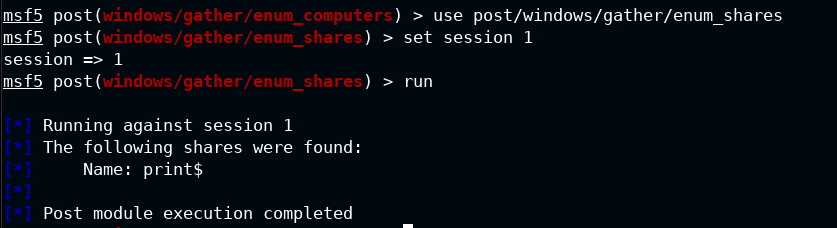
Enum computers is straightforward and looks for connected machines on the target.



Shares contain data that we might be able to grab.

This one is actually important so I’ll list the command

Use post/windows/gather/enum\_shares



And that’s the end of the overview!