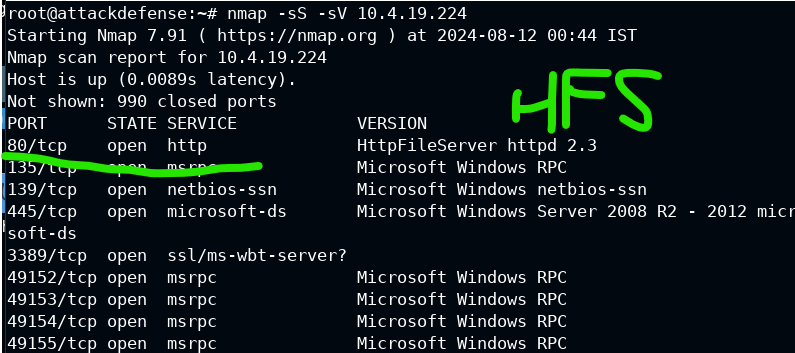
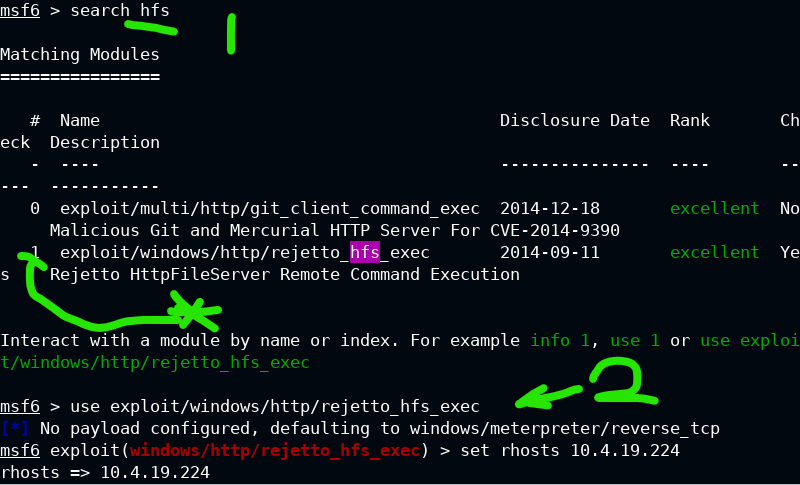
Scanning a target ip address, we begin by finding http file server

This is vulnerable to an HFS exploit. Remember “HttpFileServer = HFS” for the purposes of Metasploit modules.

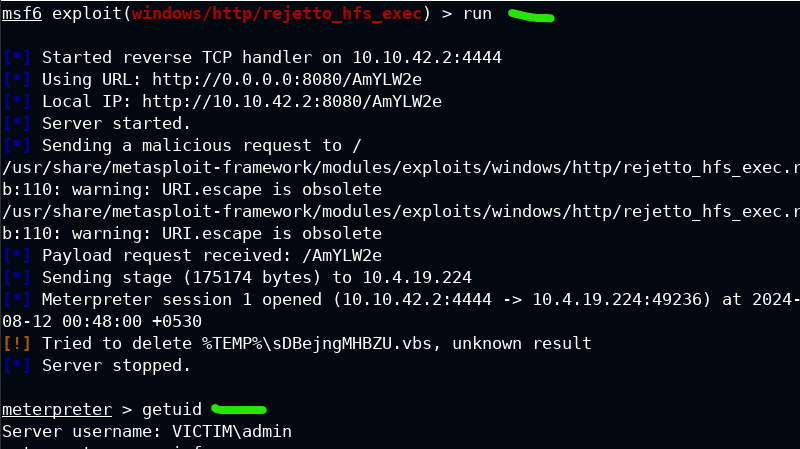


Search for our good friend to see if the common Rejetto architecture is being used, so we can hijack it.



The default payload of that reverse\_tcp is typically fine. Just set the target ip address to our opponent.

After running it, we can check with getuid who the account is on the other side that we’ve connected as

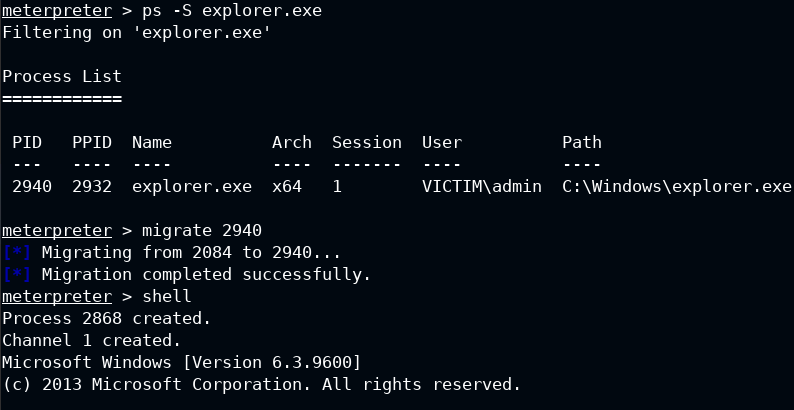


…

Just gotta memorize that we migrate meterpreter sessions into explorer.exe for persistence.

Check what process is running explorer with

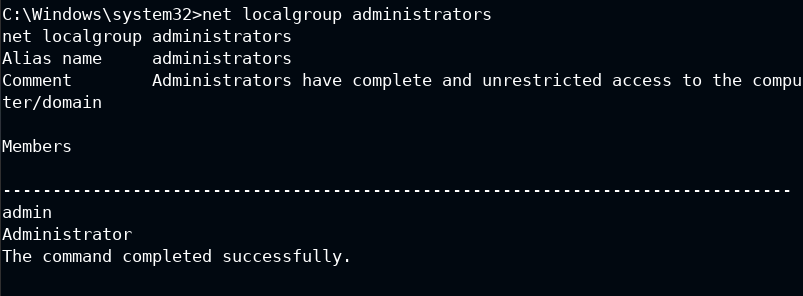
Command: ps -S explorer.exe



Check who is in the group called administrators on a machine

Command: net localgroup administrators

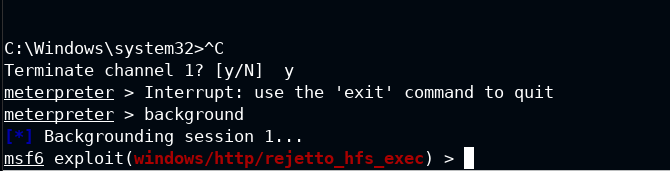
This should exist on every windows machine as a default



Set meterpreter into the background (ctrl + c)

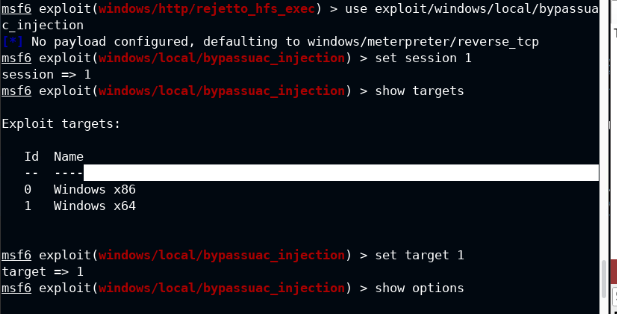
Remember, in command line ctrl + c means (cancel currently running program).

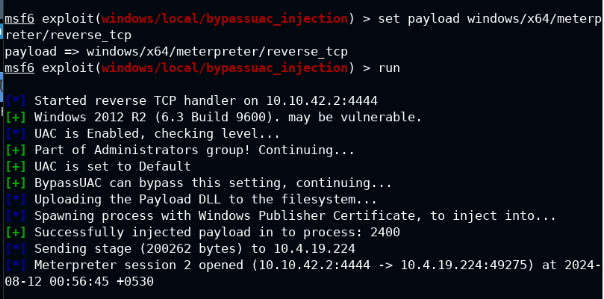
This predates the text-editor mapping that most people are familiar with as “copy”



Use exploit/windows/local/bypassuac\_injection

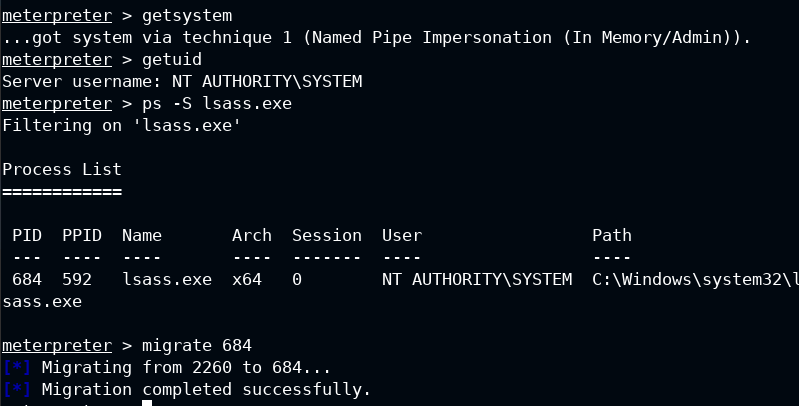
This’ll give us a reverse tcp shell. But we have to set the **session**, **target**, and **payload** before we can run it. See the screencaps for some guidance on that.





Getsystem will let us hijack the pipe, and we should check that we become the NT Authority, confirming we got the highest privs from the exploit.

With that out of the way, check out ps -S lsass.exe since we want to exfil some data



After that, hashdump. The hash at the last chunk of colons is the password info

