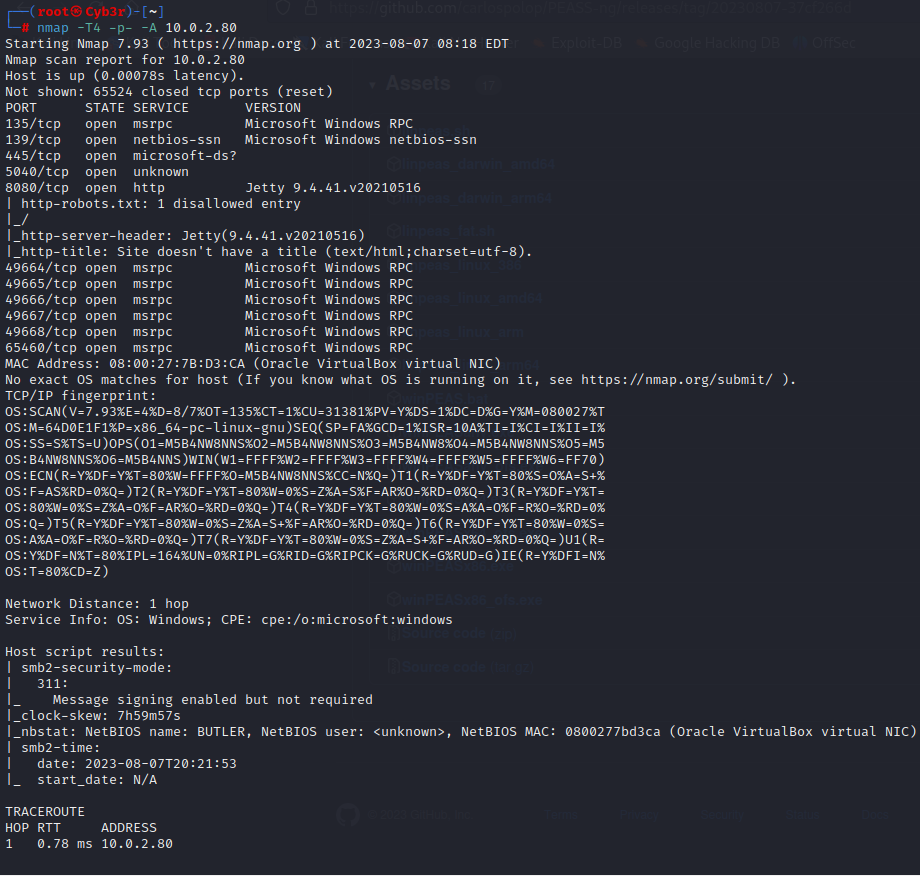
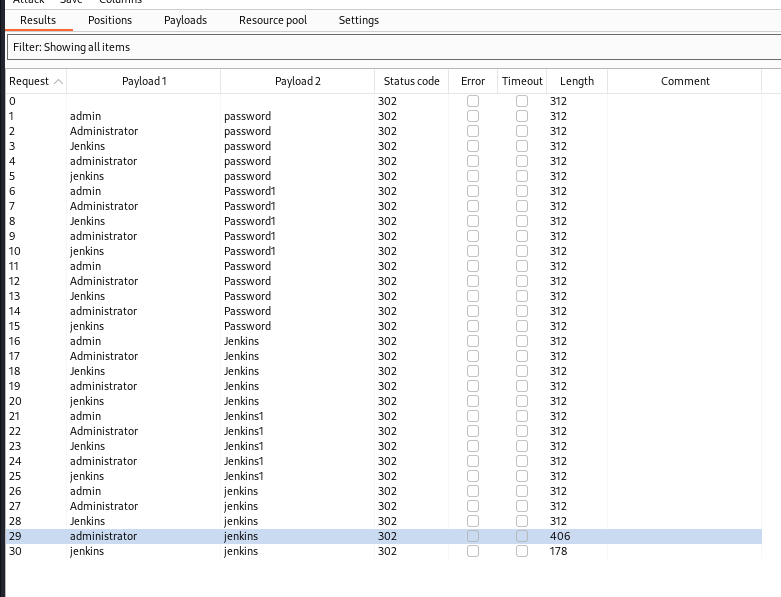
**JENKINS**

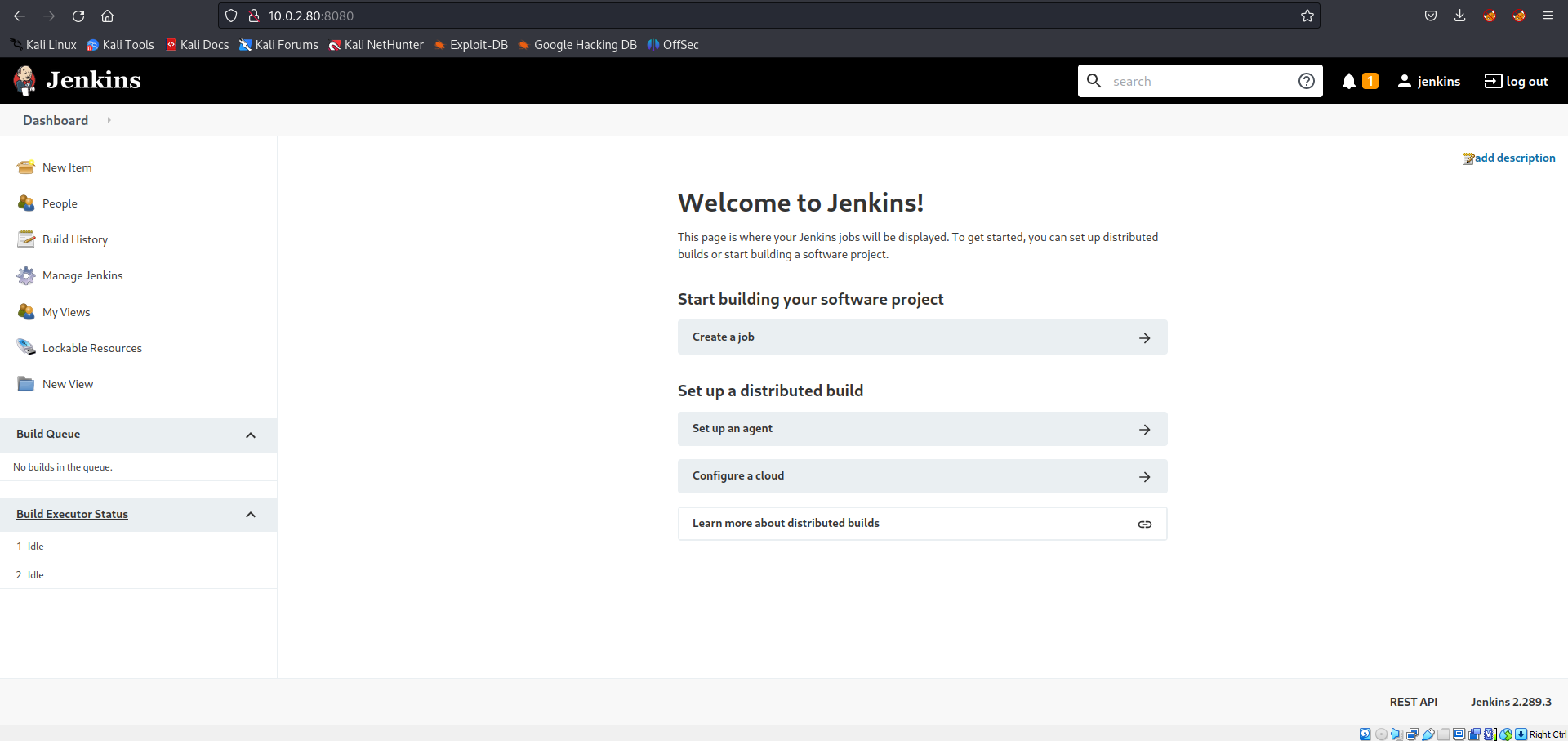
**Other Privilege Xcalation tools are Power Up and Excalation tools on the web**

****

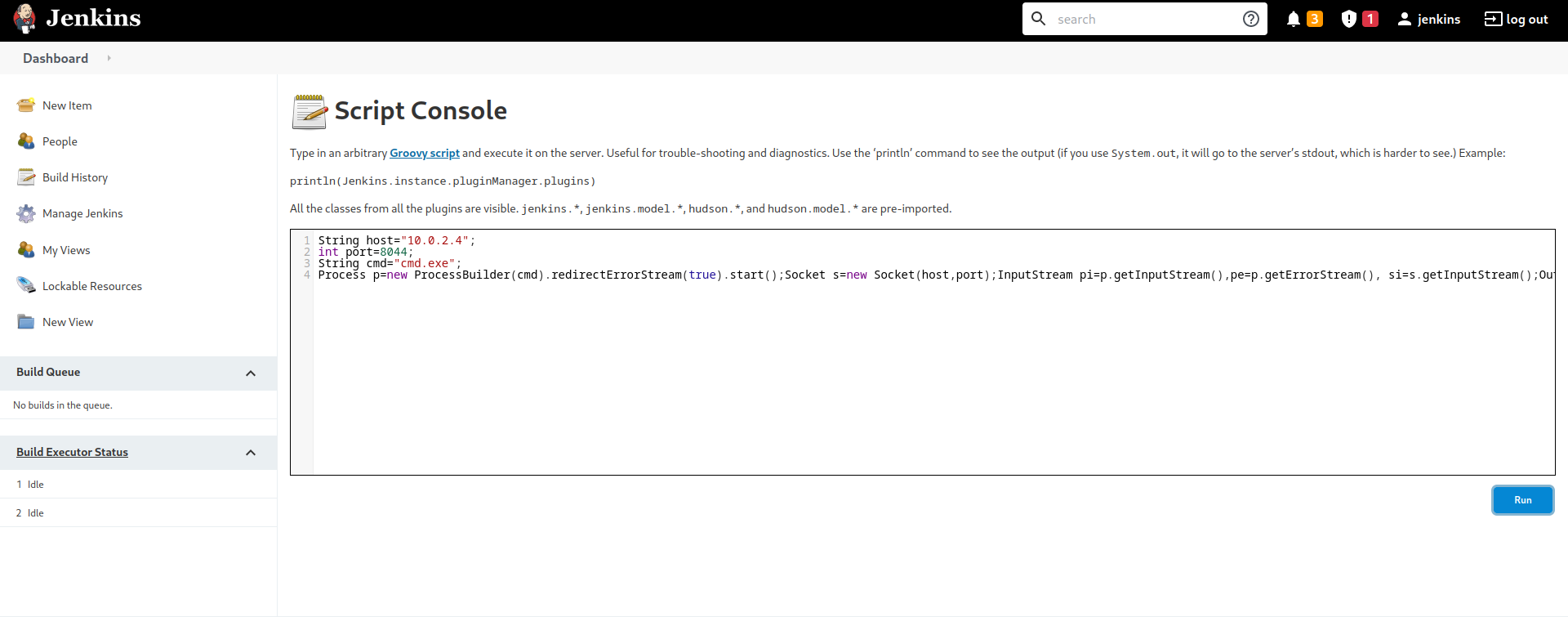
this web server is available because port 8080 is opened i.e, 10.0.2.80:8080

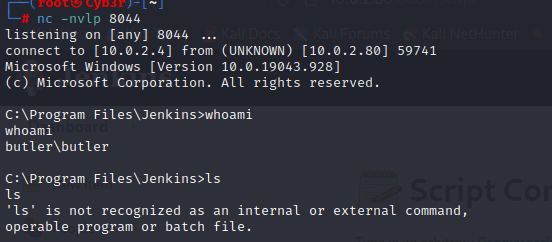
then we used burpsuite to bruteforce the login, username and password is highlighted



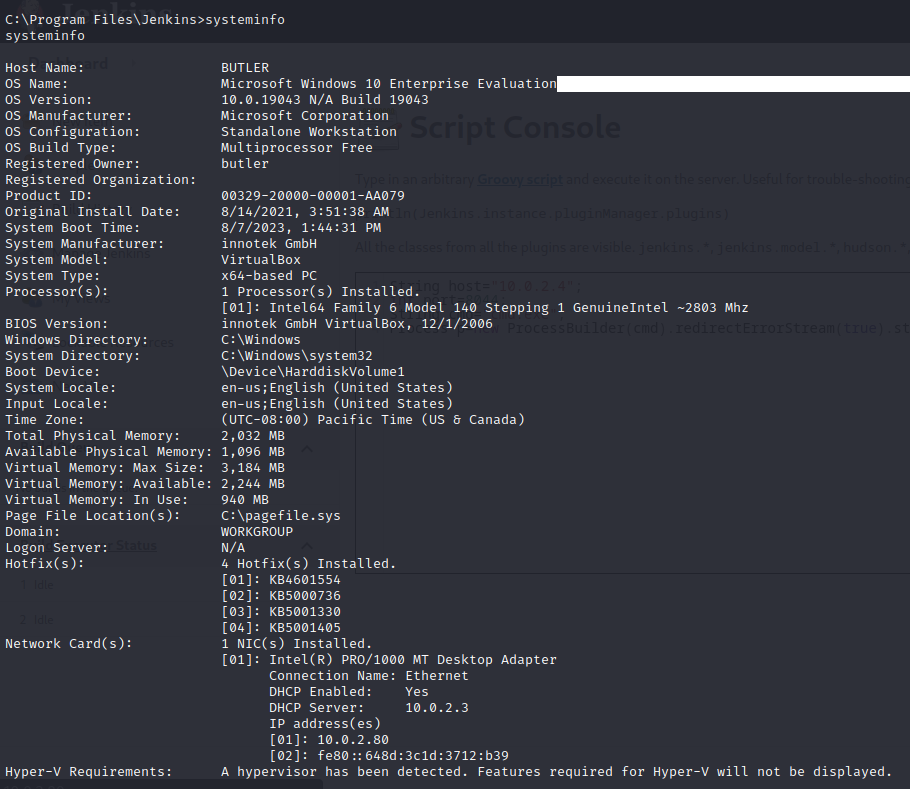
****

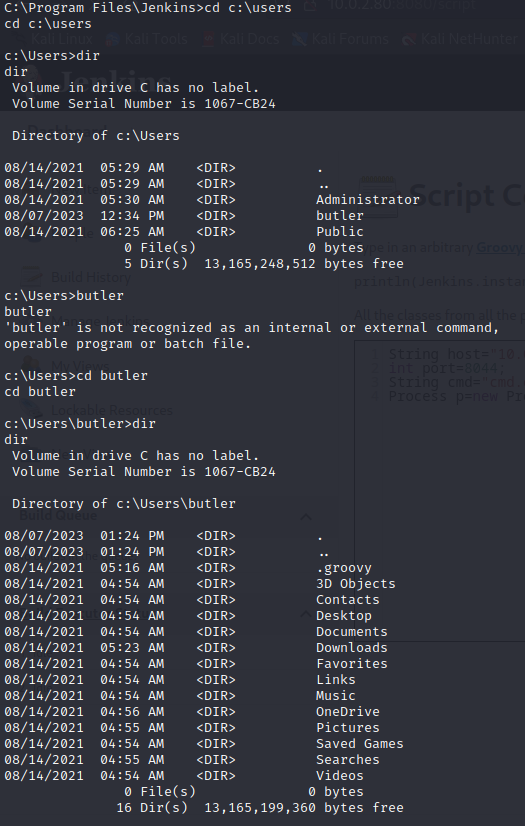
Next we scroll around to see what is available and we see a script console on the manage Jenkins tab,

and we can run a Grovvy script, so we went out to the internet and searched for Grovvy Script console exploit and a reverse shell came up. The script is written in Groovy as shown above in the console; we changed the hos to our attacker IP, and then opened a listener shown below

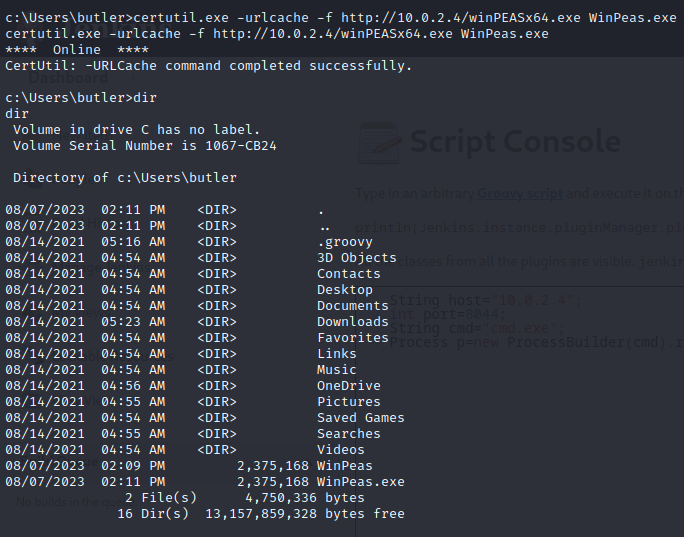


Systeminfo gives a lot of info about the operating system and different services on it

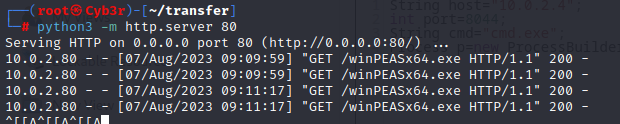




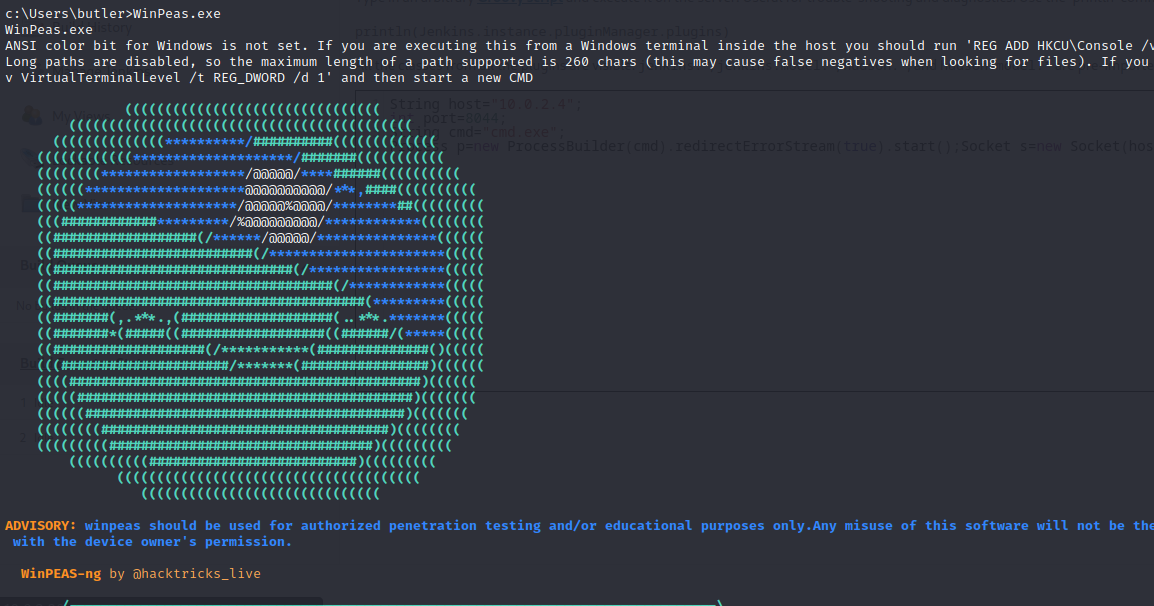
Next we downloaded winpeas for windows priv escalation

And move it to transfers folder den the command below moves the winpease into the machine we have a shell 

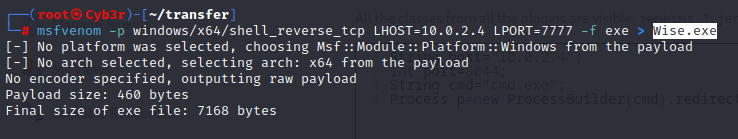
We have a winpeas.exe above and next we can host up a python server in same directory as the winpease



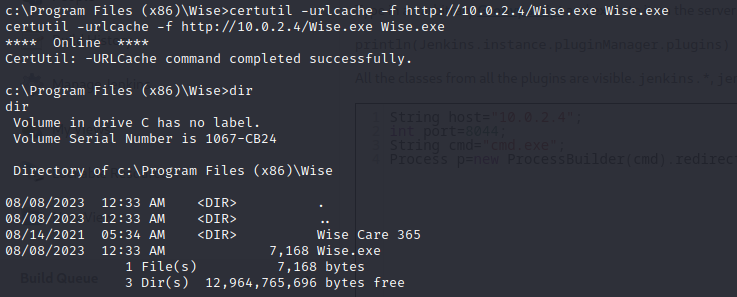
Next up we run the script in the shelled machine



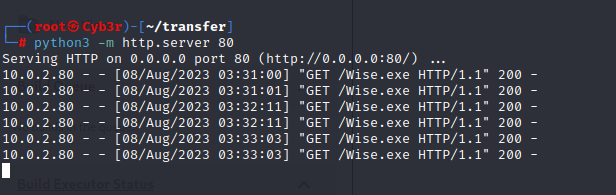
We have to escalate privilege and winpeas is not doing that but just giving us information, **NOTE YOU CAN GET PRIV ESCALATION IN VARIOUS EASIER WAYS BUT THIS IS ALSO CUTE**



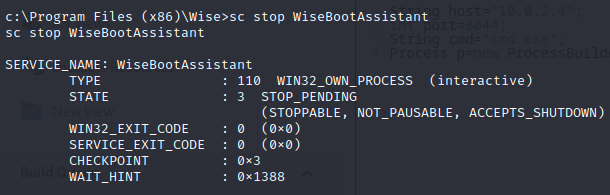
We use msfvenom to create a reverse shell malware for windows



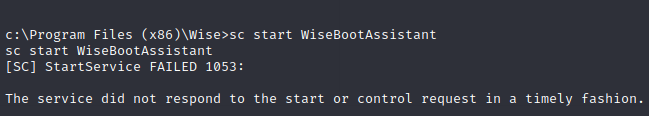
Next we use use certutil to copy the malware unto the machine with shell access as shown above, a dir unlike linux ls shows the output and we have wise.exe.  
**IF YOU RUN IT LIKE THIS U HAVE SAME SHELL AND NO HIGH PRIV SO WE END SERVICE AND RESTART BUT FIRST OPEN A LISTENER ON SAME PORT AS ON IMAGE ABOVE, 7777**

****

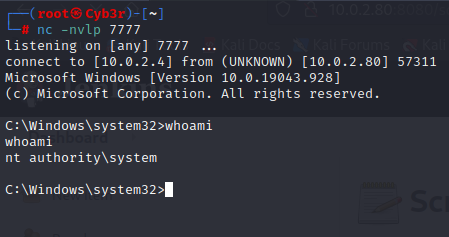
Remember to host a server, then run



Stop and start the service



Once restarted, ignore the below error and check ur listening port



And we have root. Yipeeeeeee