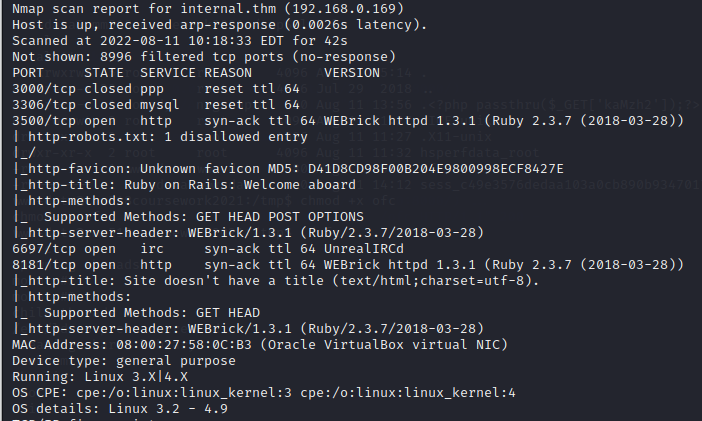
Vulnerable Machine walkthrough

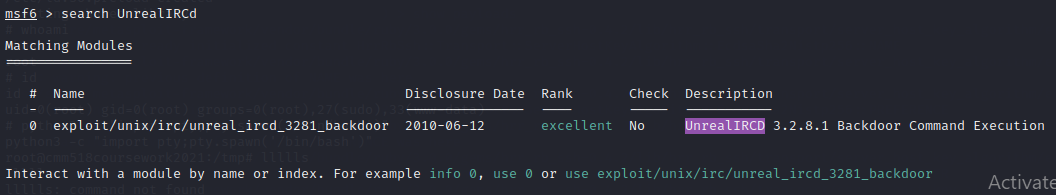
Exploitation report.

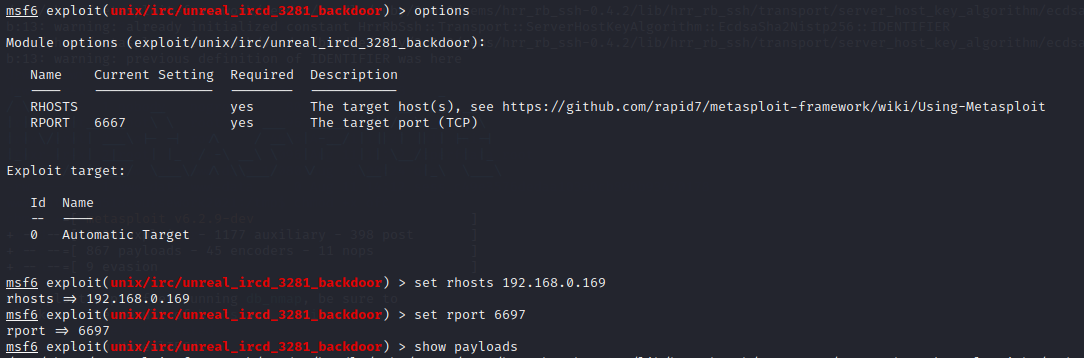
I further run nmap again using this syntax sudo nmap -sV -sC -O -p1000-10000 192.168.0.169 -vv and find out that there is another open port (port 6697) that is running ircs-u as a service and UnrealIRCd as its version. See the below screen shoots.



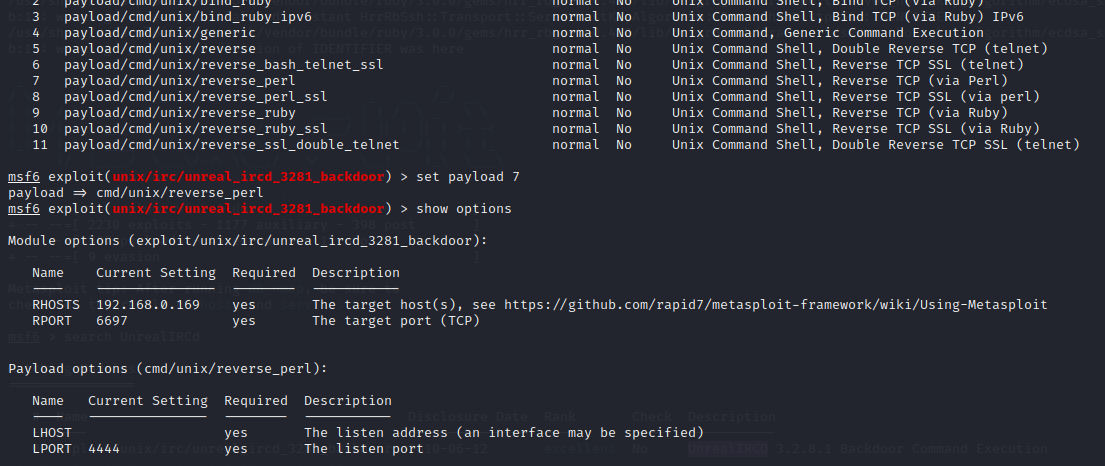
After gaining this knowledge I open I metasploit console and search for the version of open port 6697 I find above to know if there will be exploit for exact version.

And I got one which I use for this exploitation. Seen the sreen shoot

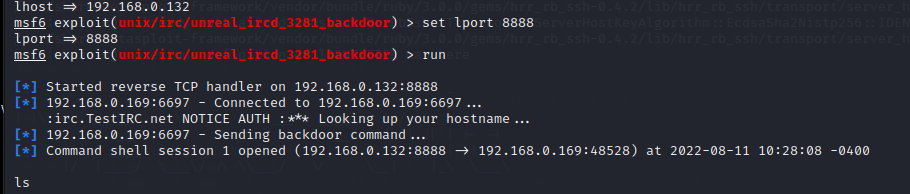




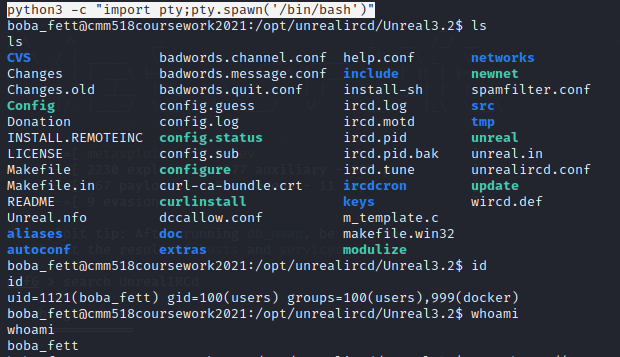
I use show options command to know which option to set for the exploit as seen in above screen shoot.



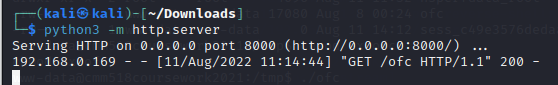
After setting the necessary options and selecting a suitable payload and setting the local ip and local port as seen on above screen short.

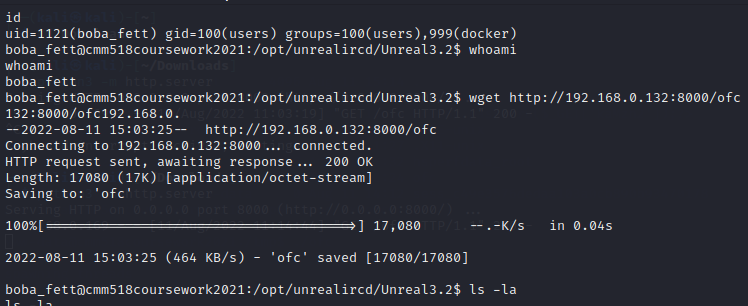


Running the exploit and getting a shell.

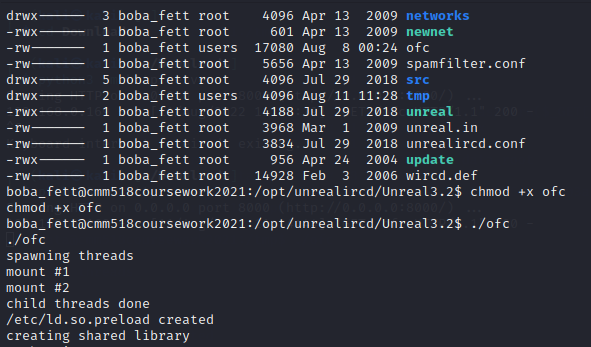


Setting a simple http server to download the privilege escalation code as seen below.

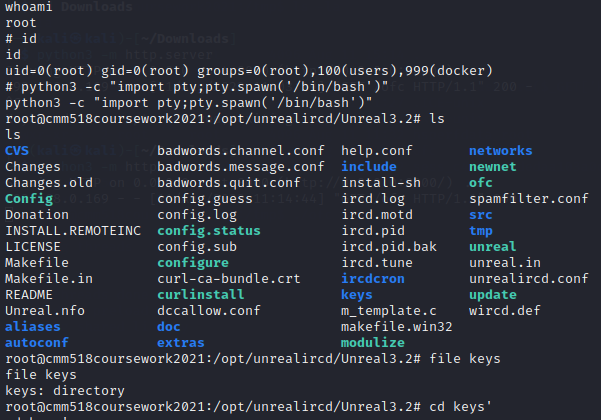




Successfully downloaded the file to the target machine.



Given the file executable option and executing it to become a root user.



Finally I am a root user.