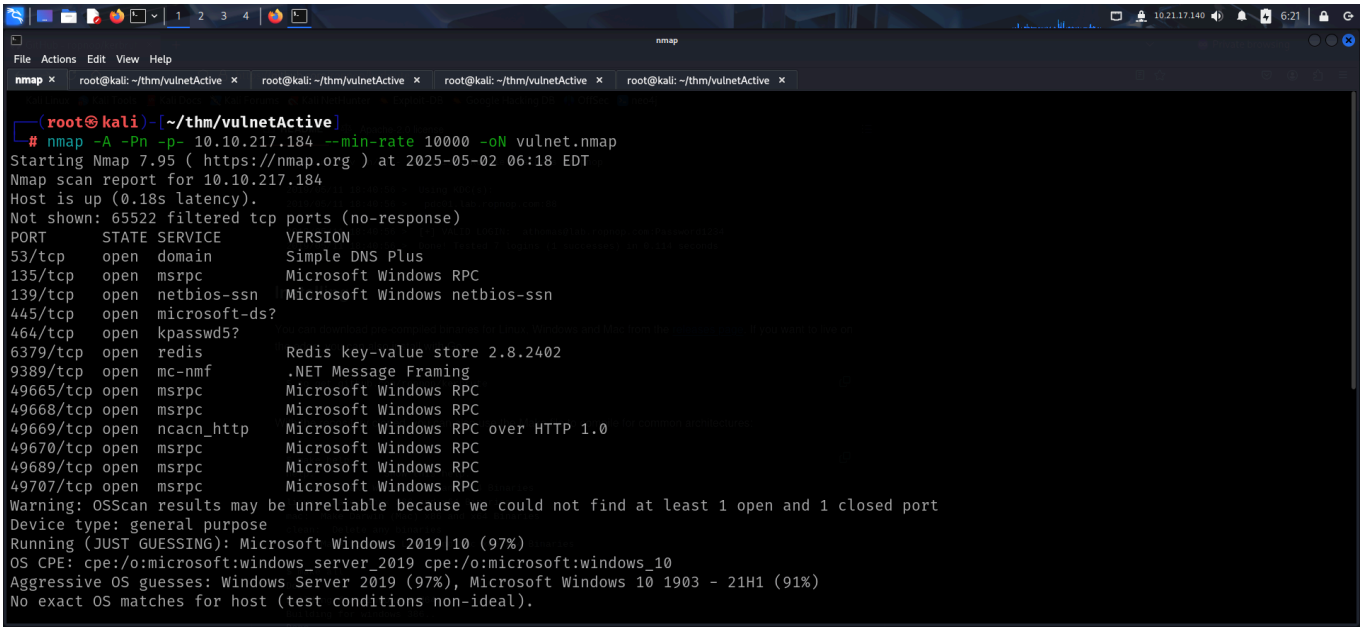
VULNET ACTIVE

To access the machine, click on the link given below:
https://tryhackme.com/room/vulnnetactive

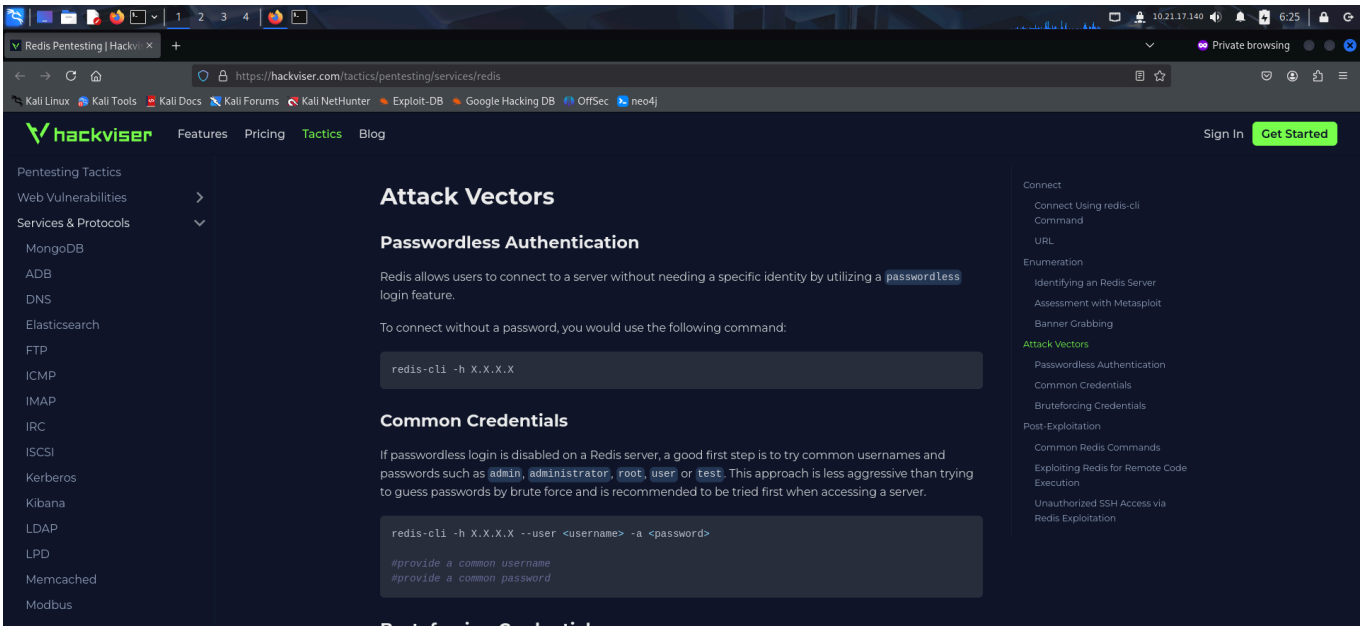
SCANNING

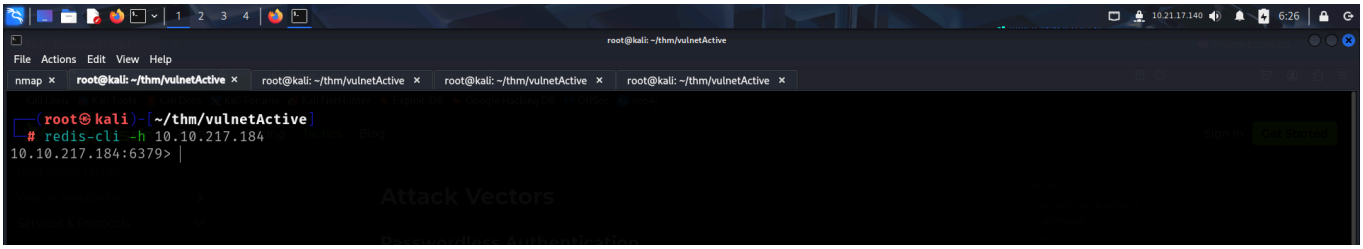
I performed an **nmap** aggressive scan on the target to find open ports and the services running on them.



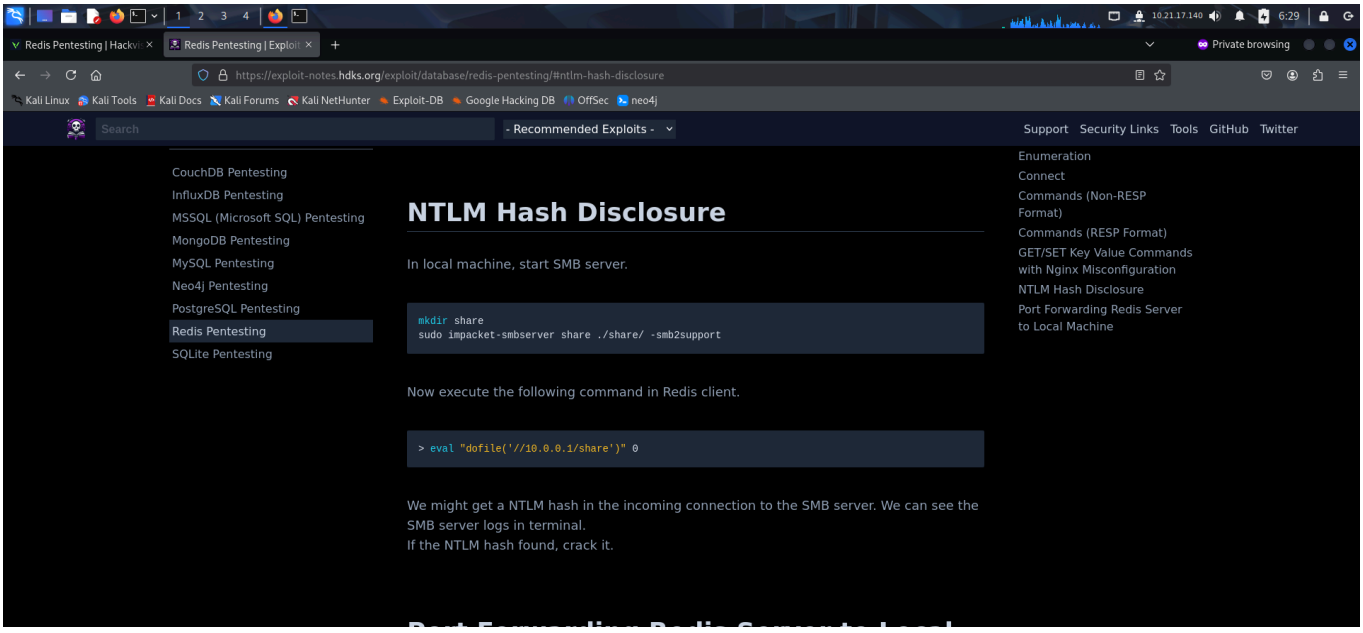
FOOTHOLD

I found **redis** to be running so I searched online for ways I could interact with the service and found this article: https://hackviser.com/tactics/pentesting/services/redis

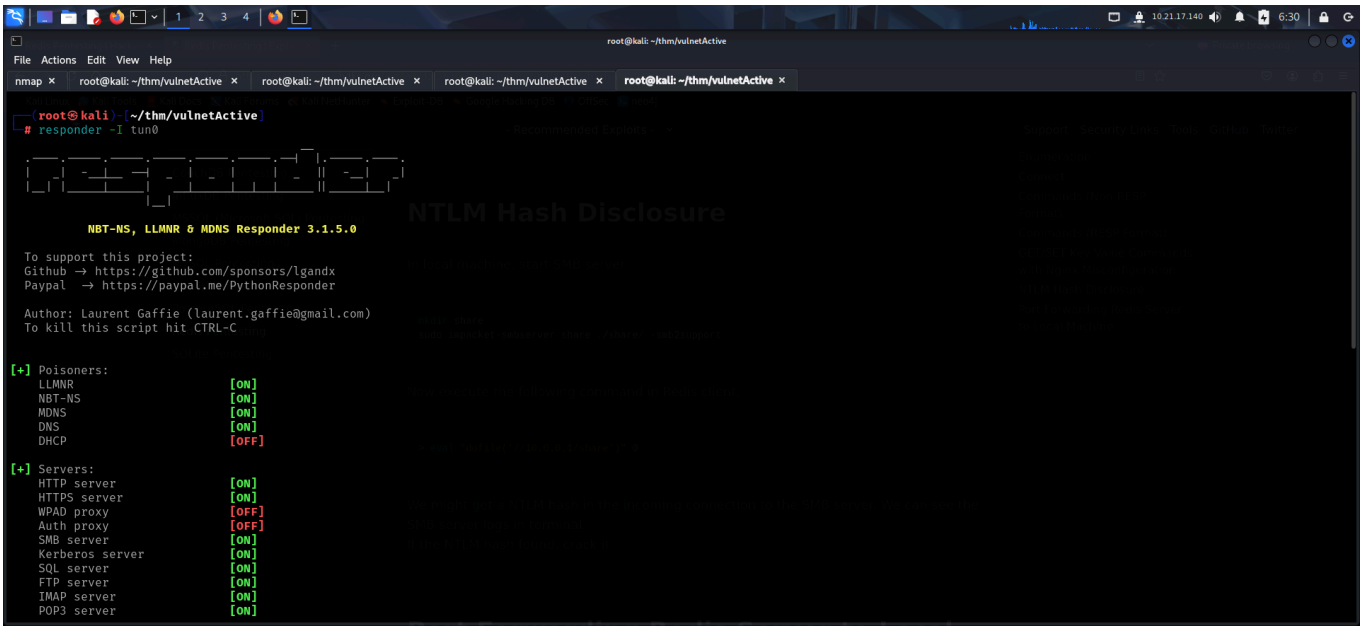




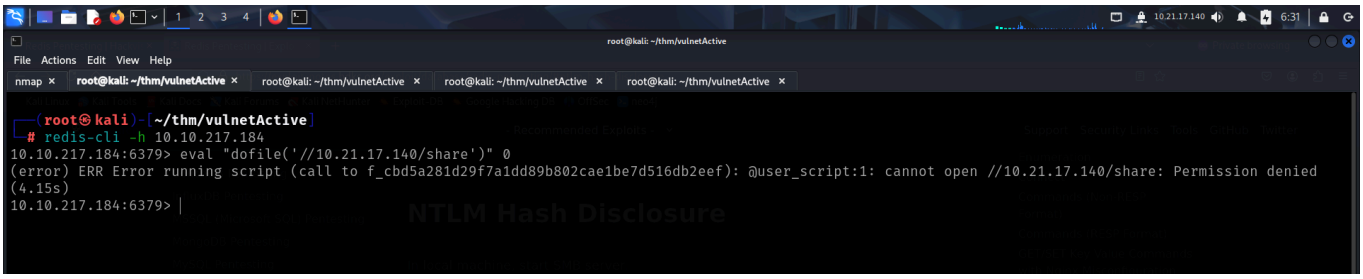
I looked for ways I could exploit this and found this article. It seems I could relay my ntlm credentials through smb.

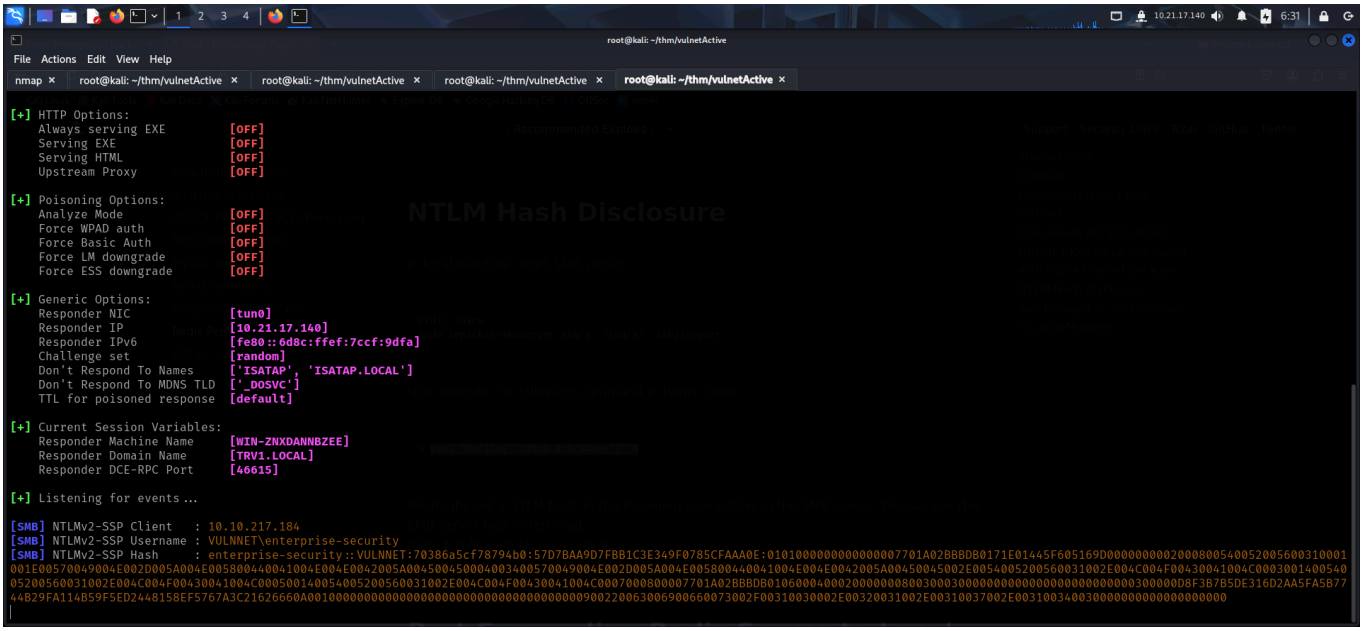


I started responder on my interface

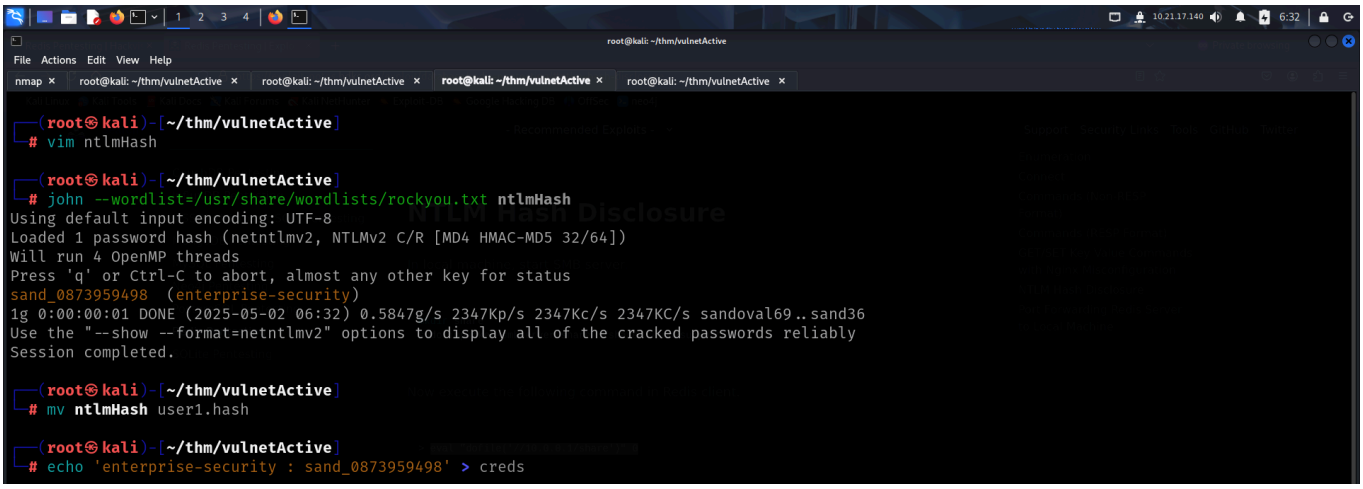


I then tried accessing a share on my system and found the NLTM hash on responder.

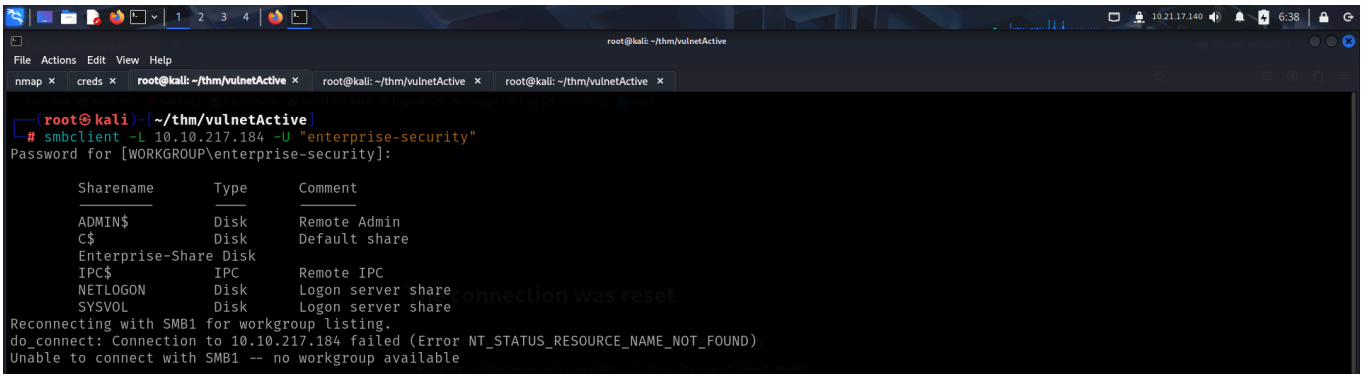




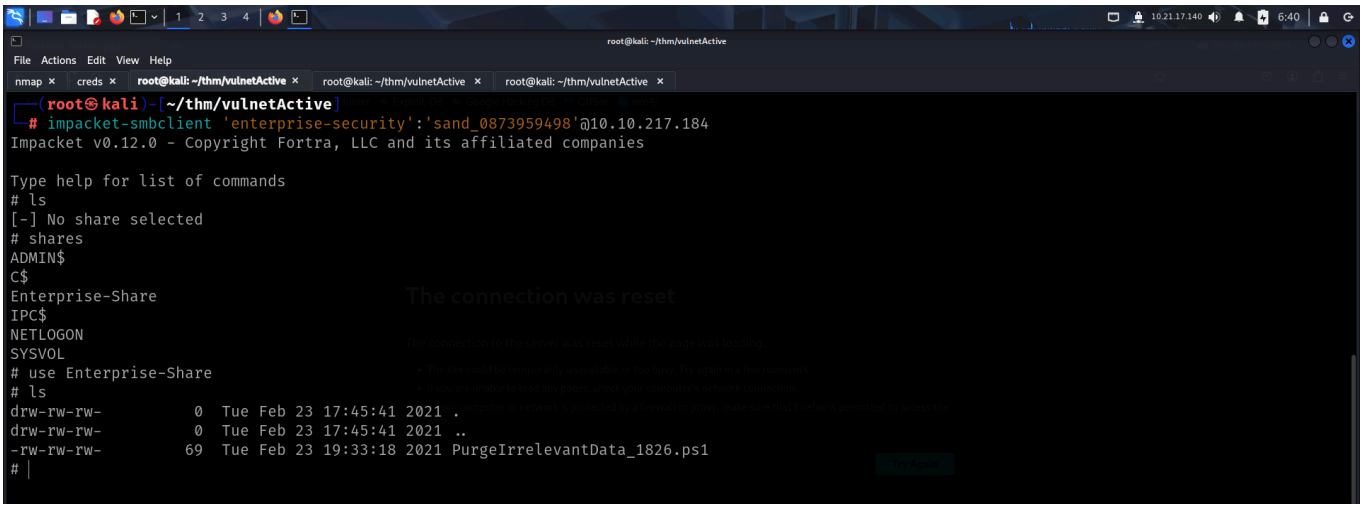
I saved the hash and cracked it using **john**.



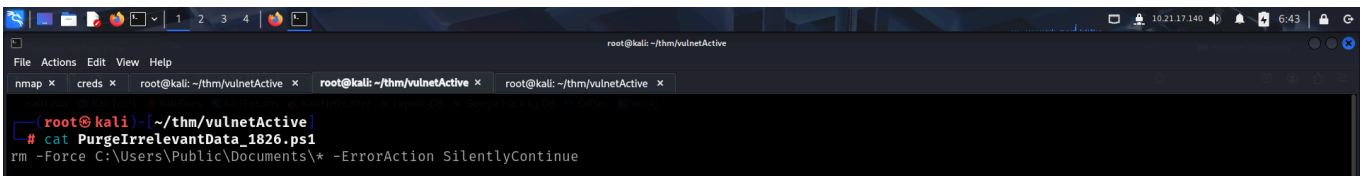
I then listed the shares using the newly discovered credentials.



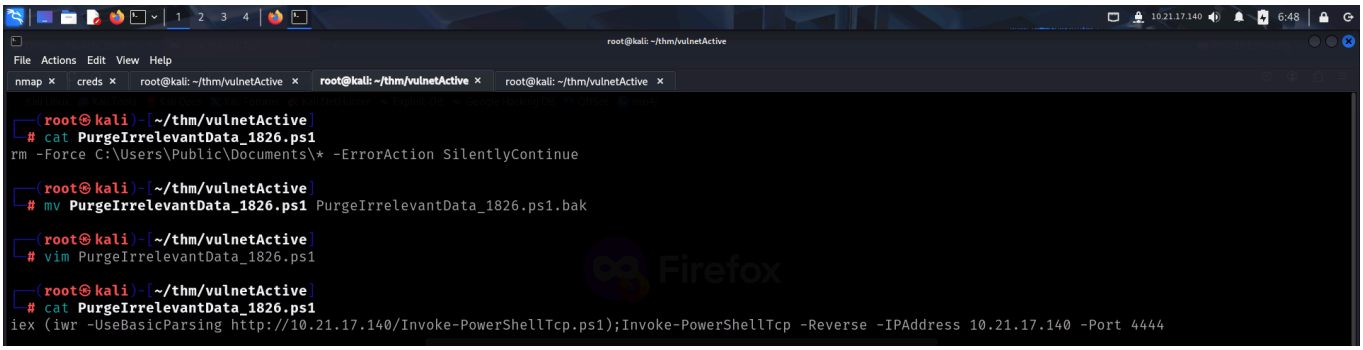
I connected to the server using my credentials and accessed `Enterprise-Share`

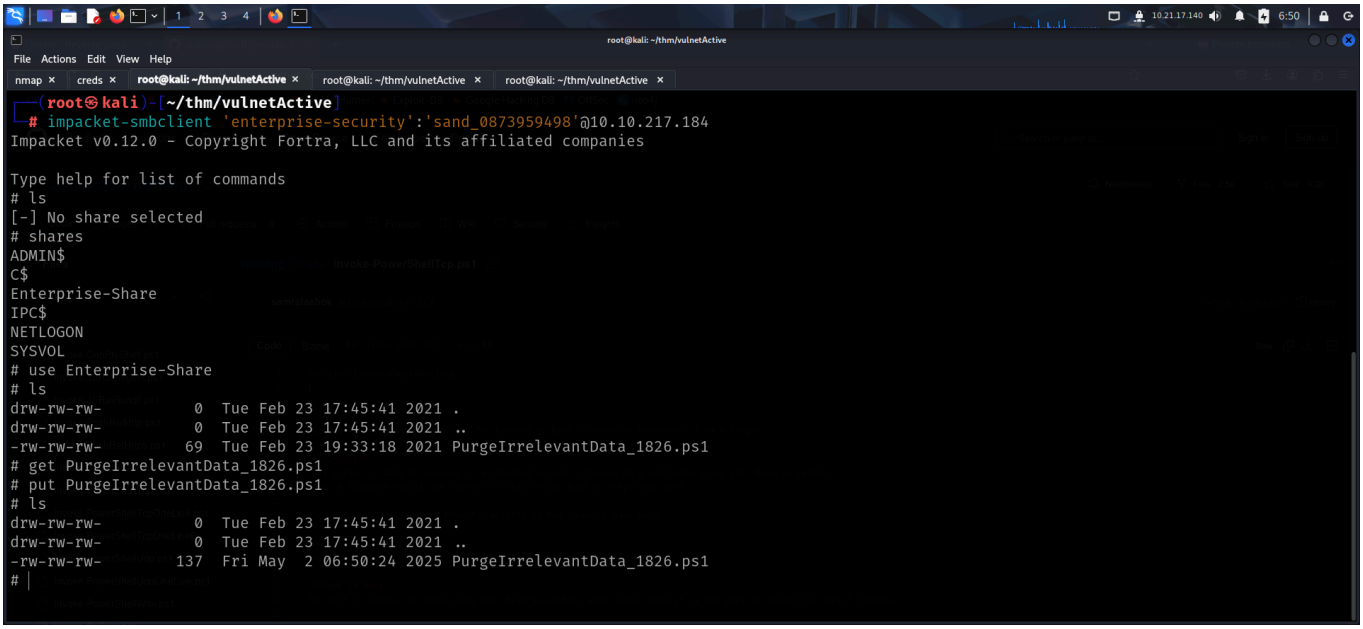


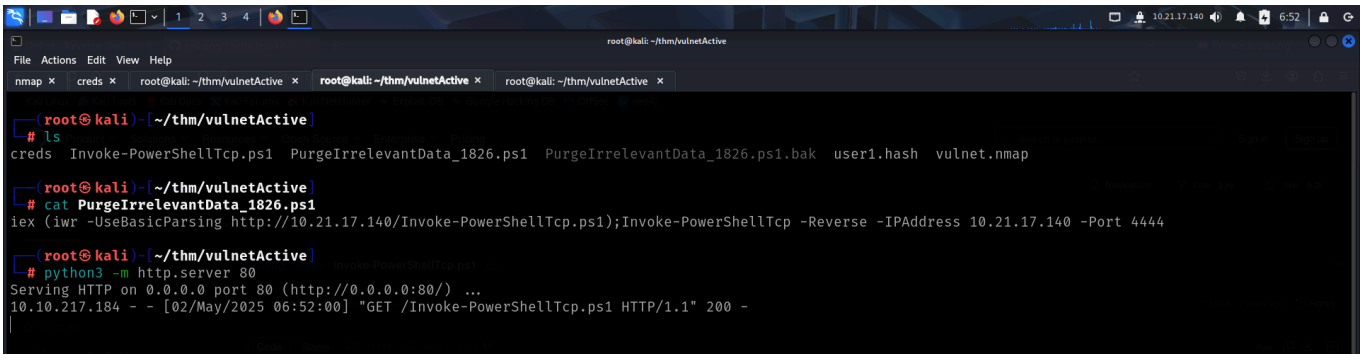
I then downloaded the ps1 script and it seemed like it deleted the contents of the Documents directory.



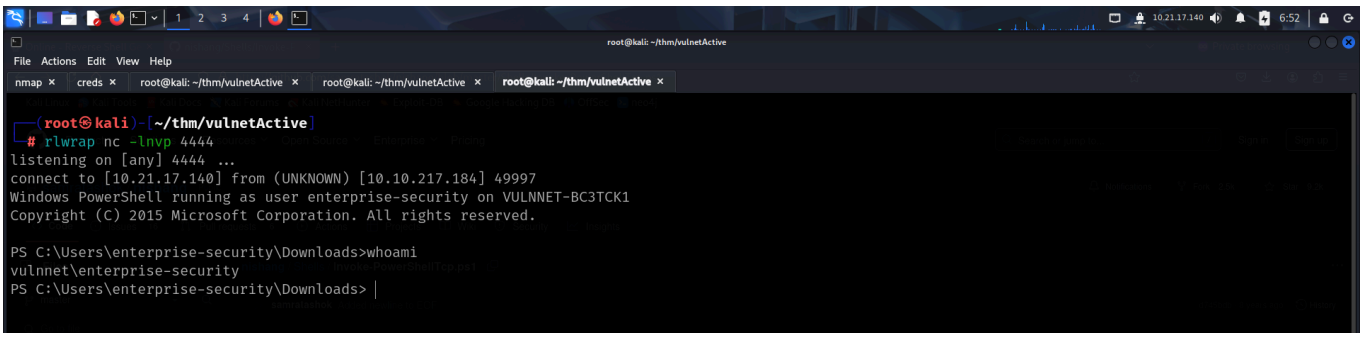
I replaced the contents with a reverse shell and uploaded it back into the system.







I soon got a reverse shell.



I navigated to Desktop and found the user flag.

```
PS C:\Users\enterprise-security> cd Desktop
PS C:\Users\enterprise-security\Desktop> dir


    Directory: C:\Users\enterprise-security\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/23/2021   8:24 PM             37 user.txt


PS C:\Users\enterprise-security\Desktop> more user.txt
THM{3e[redacted]}

PS C:\Users\enterprise-security\Desktop>
```

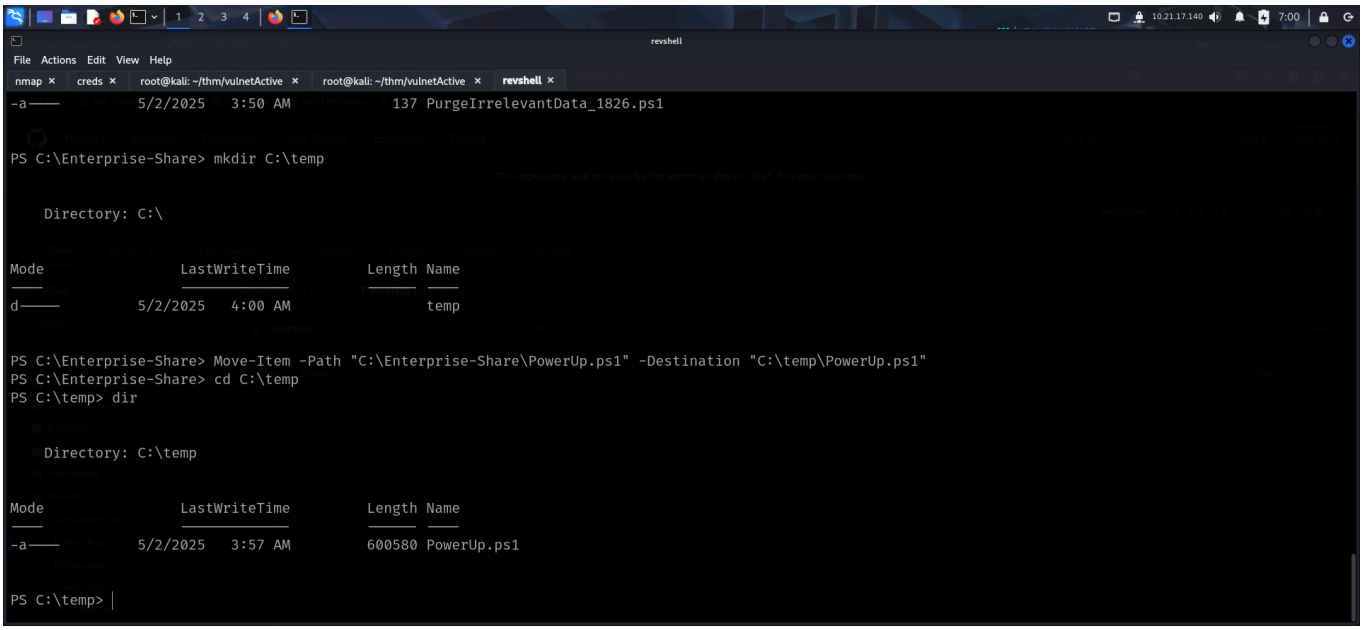
PRIVILEGE ESCALATION

I then uploaded **PowerUp** for local enumeration.

```
# shares
ADMIN$
C$
Enterprise-Share
IPC$
NETLOGON
SYSVOL
# use Enterprise-Share
# ls
drw-rw-rw-          0  Tue Feb 23 17:45:41 2021 .
drw-rw-rw-          0  Tue Feb 23 17:45:41 2021 ..
-rw-rw-rw-         69  Tue Feb 23 19:33:18 2021 PurgeIrrelevantData_1826.ps1
# get PurgeIrrelevantData_1826.ps1
# put PurgeIrrelevantData_1826.ps1
# ls
drw-rw-rw-          0  Tue Feb 23 17:45:41 2021 .
drw-rw-rw-          0  Tue Feb 23 17:45:41 2021 ..
-rw-rw-rw-        137  Fri May  2 06:50:24 2025 PurgeIrrelevantData_1826.ps1
# put PowerUp.ps1
# ls
drw-rw-rw-          0  Fri May  2 06:57:54 2025 .
drw-rw-rw-          0  Fri May  2 06:57:54 2025 ..
-rw-rw-rw-     600580  Fri May  2 06:57:57 2025 PowerUp.ps1
-rw-rw-rw-        137  Fri May  2 06:50:24 2025 PurgeIrrelevantData_1826.ps1
#
```

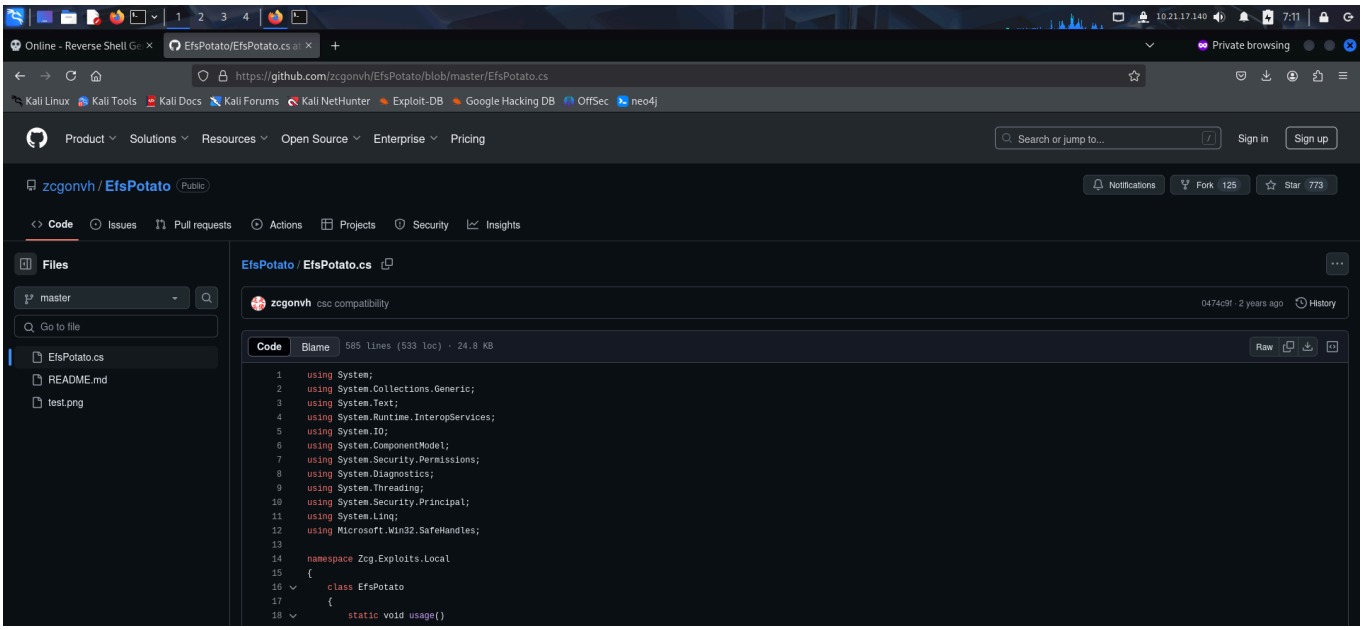
```
PS C:\Users\enterprise-security\Downloads> cd C:\Enterprise-Share
PS C:\Enterprise-Share> dir


    Directory: C:\Enterprise-Share


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          5/2/2025   3:57 AM         600580 PowerUp.ps1
-a----          5/2/2025   3:50 AM            137 PurgeIrrelevantData_1826.ps1


PS C:\Enterprise-Share>
```

I created a temp directory and shifted the script to it.

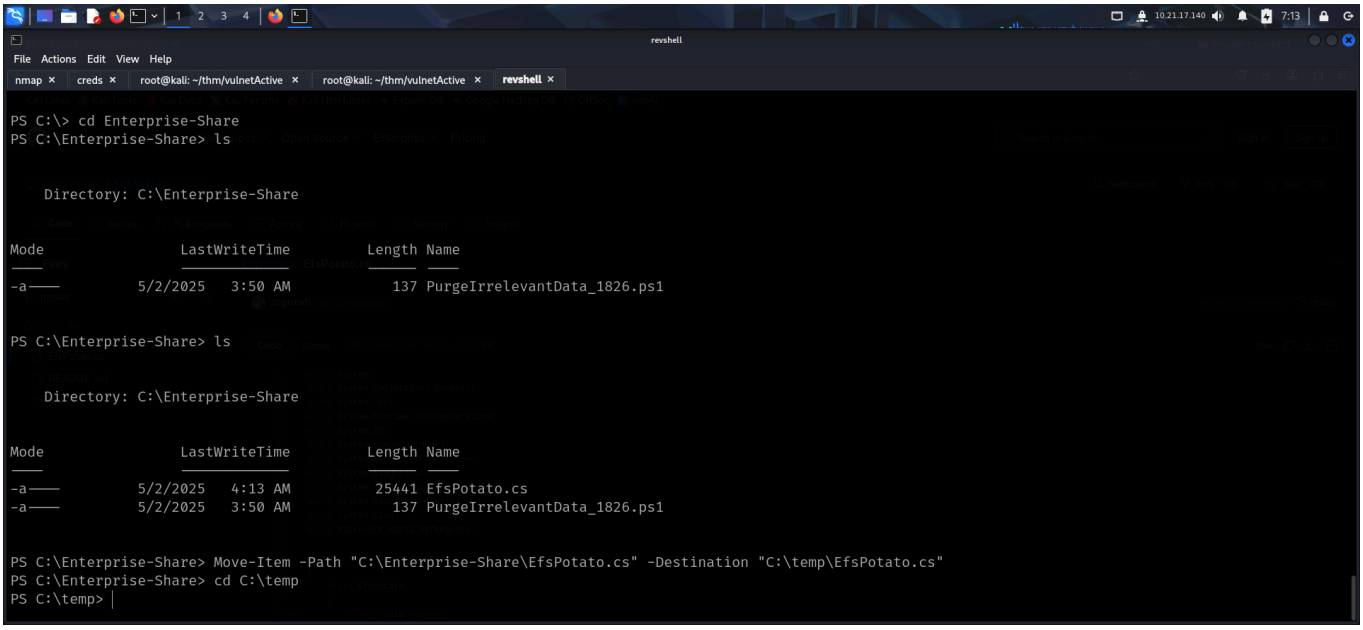


Finally, I executed the script and found interesting configs. I seemed to have the **SeImpersonatePrivilege**.

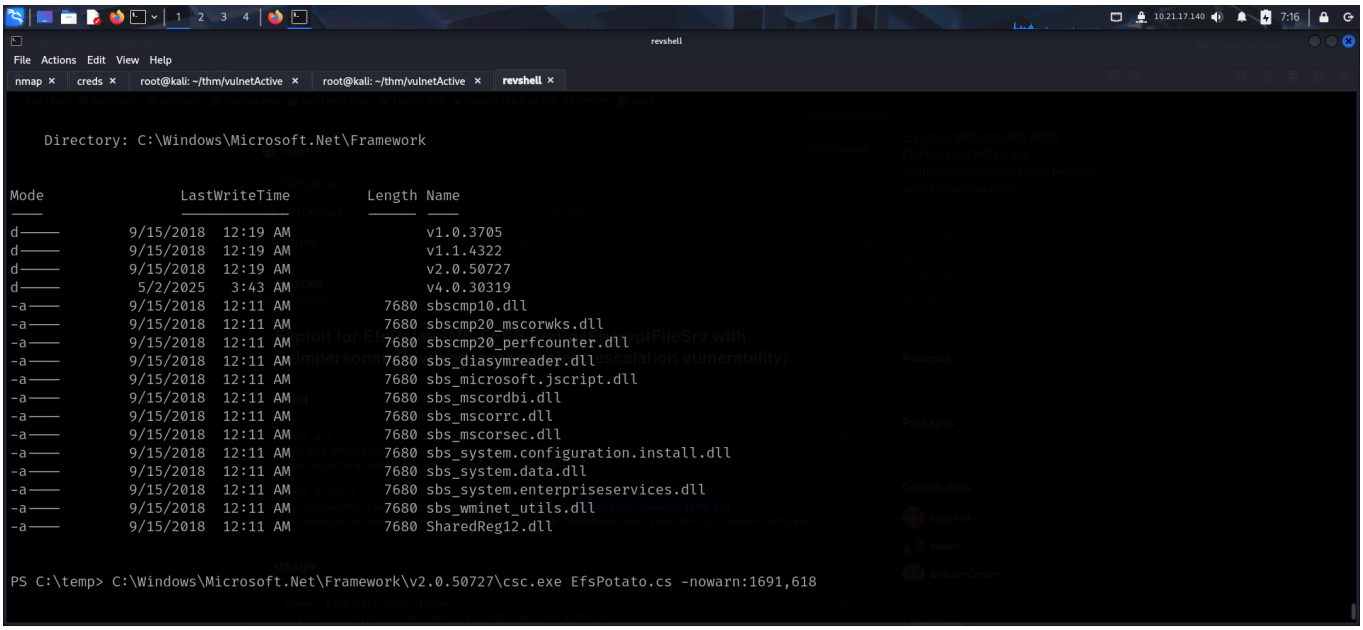
This could be used to launch a potato attack and gain administrative access. So I tried exploiting it using **EfsPotato**.



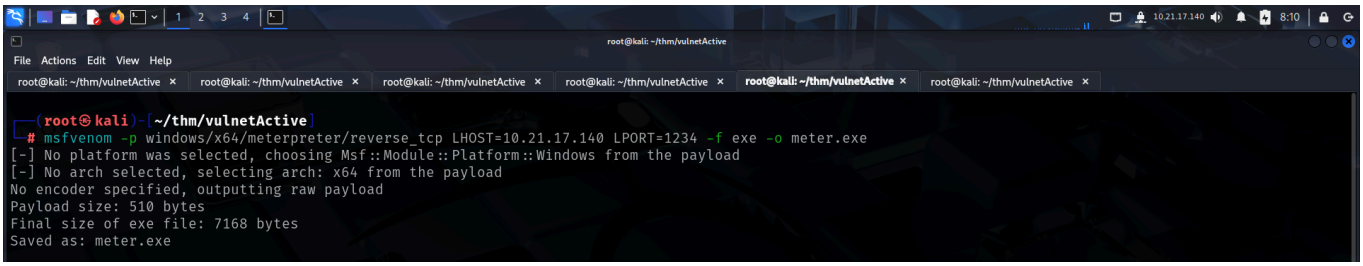

```
# use Enterprise-Share
# ls
drw-rw-rw-          0  Tue Feb 23 17:45:41 2021 .
drw-rw-rw-          0  Tue Feb 23 17:45:41 2021 ..
-rw-rw-rw-         69  Tue Feb 23 19:33:18 2021 PurgeIrrelevantData_1826.ps1
# get PurgeIrrelevantData_1826.ps1
# put PurgeIrrelevantData_1826.ps1
# ls
drw-rw-rw-          0  Tue Feb 23 17:45:41 2021 .
drw-rw-rw-          0  Tue Feb 23 17:45:41 2021 ..
-rw-rw-rw-        137  Fri May  2 06:50:24 2025 PurgeIrrelevantData_1826.ps1
# put PowerUp.ps1
# ls
drw-rw-rw-          0  Fri May  2 06:57:54 2025 .
drw-rw-rw-          0  Fri May  2 06:57:54 2025 ..
-rw-rw-rw-     600580  Fri May  2 06:57:57 2025 PowerUp.ps1
-rw-rw-rw-        137  Fri May  2 06:50:24 2025 PurgeIrrelevantData_1826.ps1
# put EfsPotato.cs
# ls
drw-rw-rw-          0  Fri May  2 07:13:06 2025 .
drw-rw-rw-          0  Fri May  2 07:13:06 2025 ..
-rw-rw-rw-      25441  Fri May  2 07:13:07 2025 EfsPotato.cs
-rw-rw-rw-        137  Fri May  2 06:50:24 2025 PurgeIrrelevantData_1826.ps1
#
```



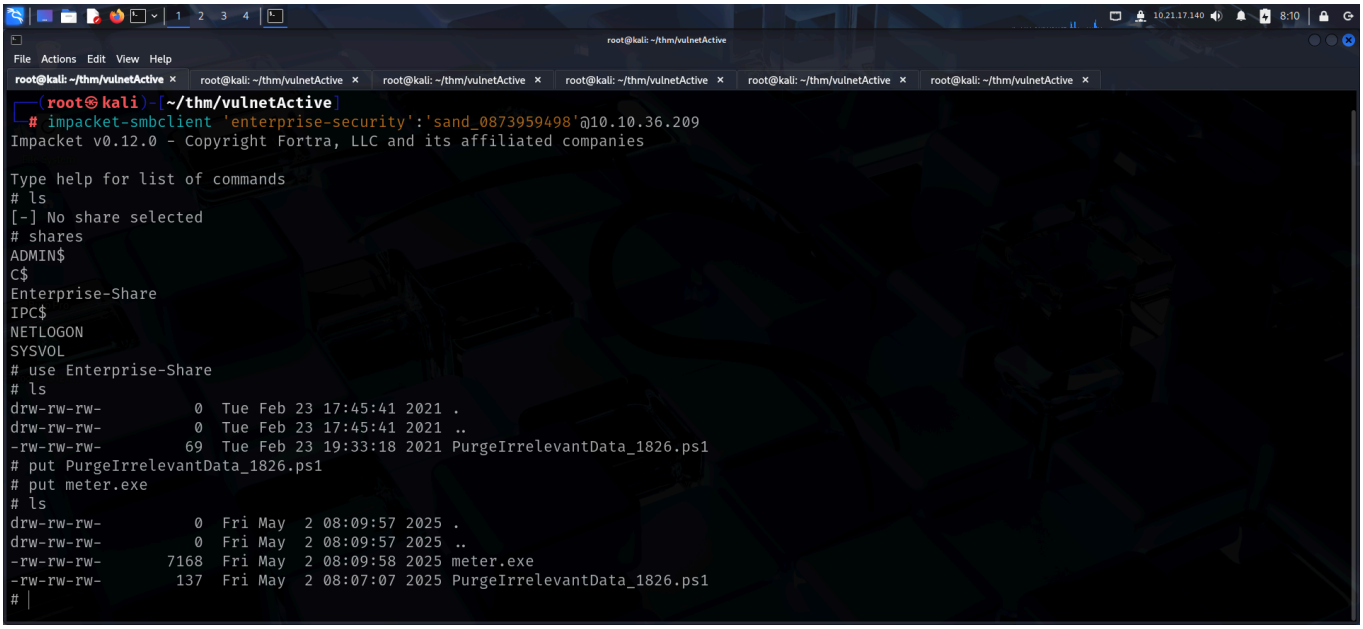
I tried executing the payload but it kept failing.

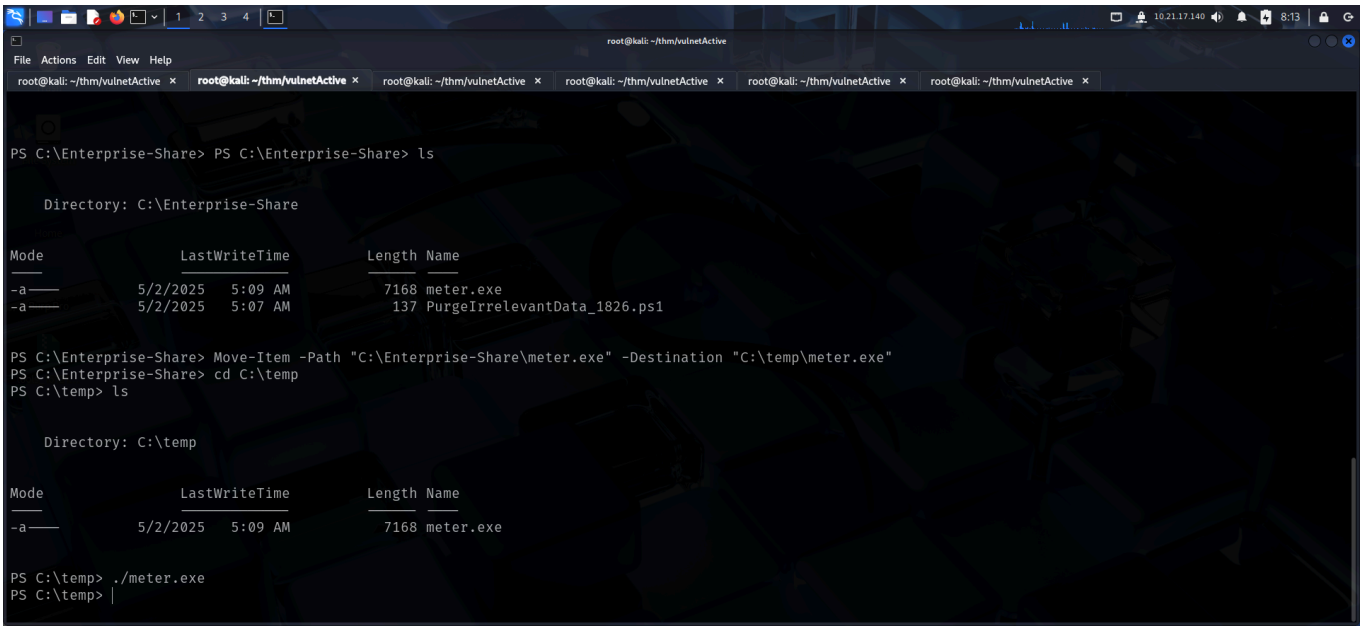


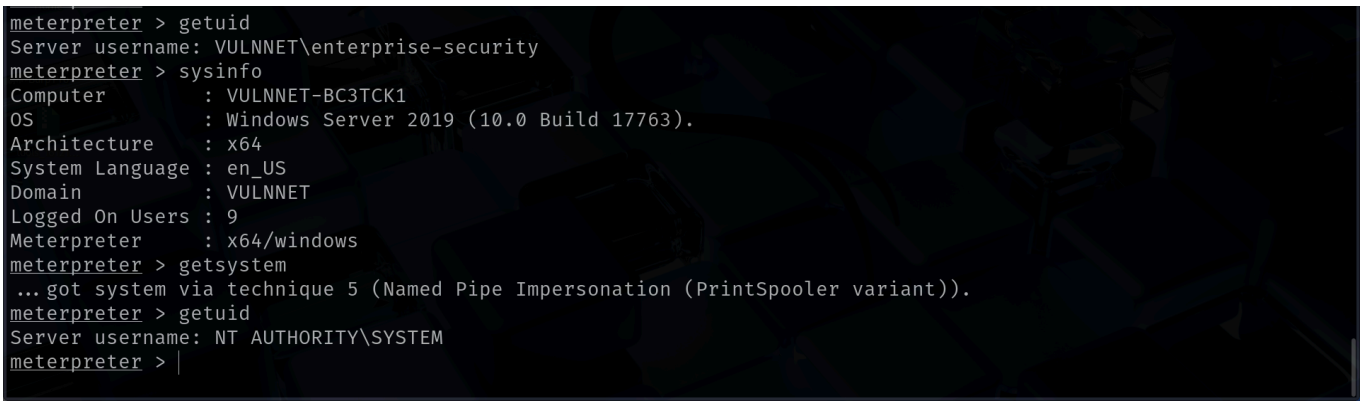
So I created an msfvenom payload to get a meterpreter shell.



I uploaded the payload through smb and executed it to get a reverse meterpreter shell on metasploit.







After getting a shell, I used `getsystem` command to automatically escalate privilege and gain NT AUTHORITY\SYSTEM access.

Finally, I captured the root flag from Administrator's desktop.