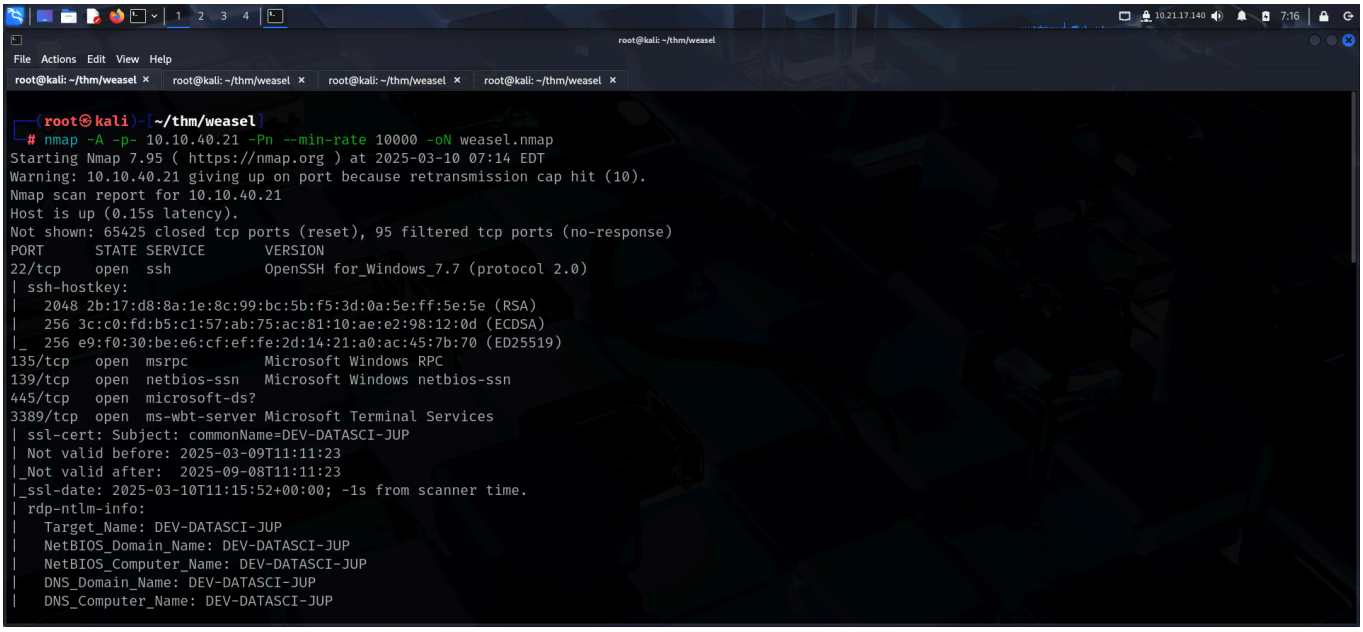
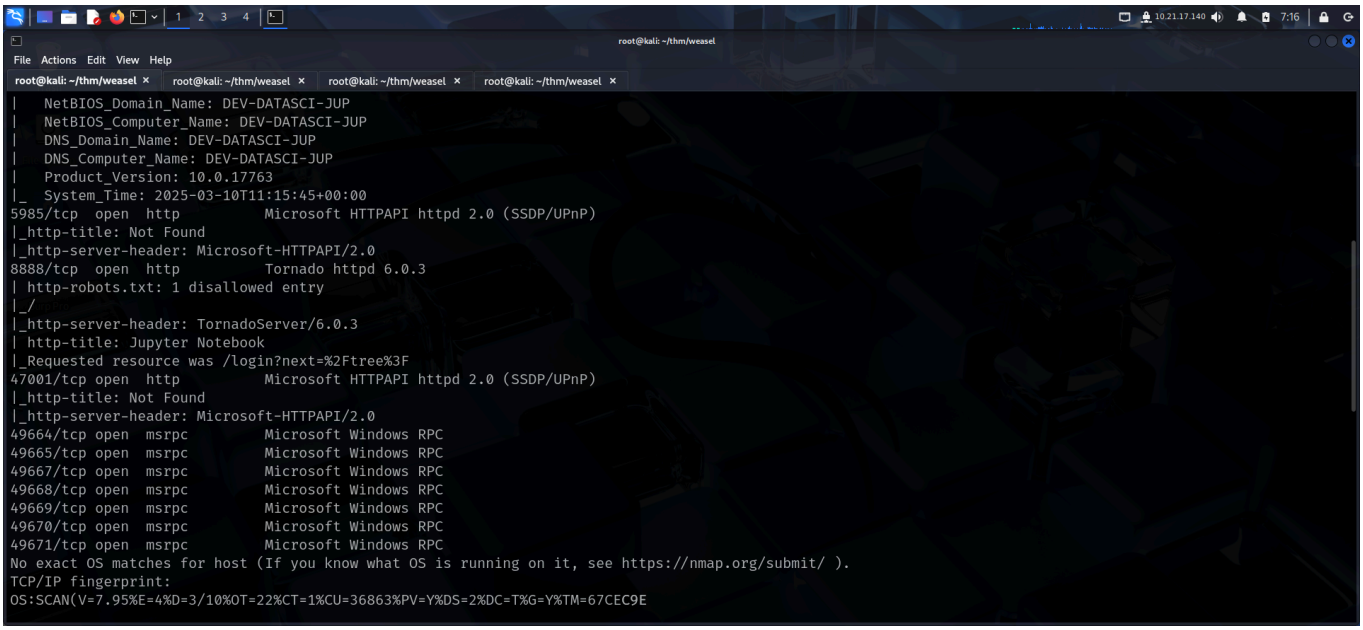
WEASEL

Link to machine : https://tryhackme.com/room/weasel

RECONAISSANCE

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

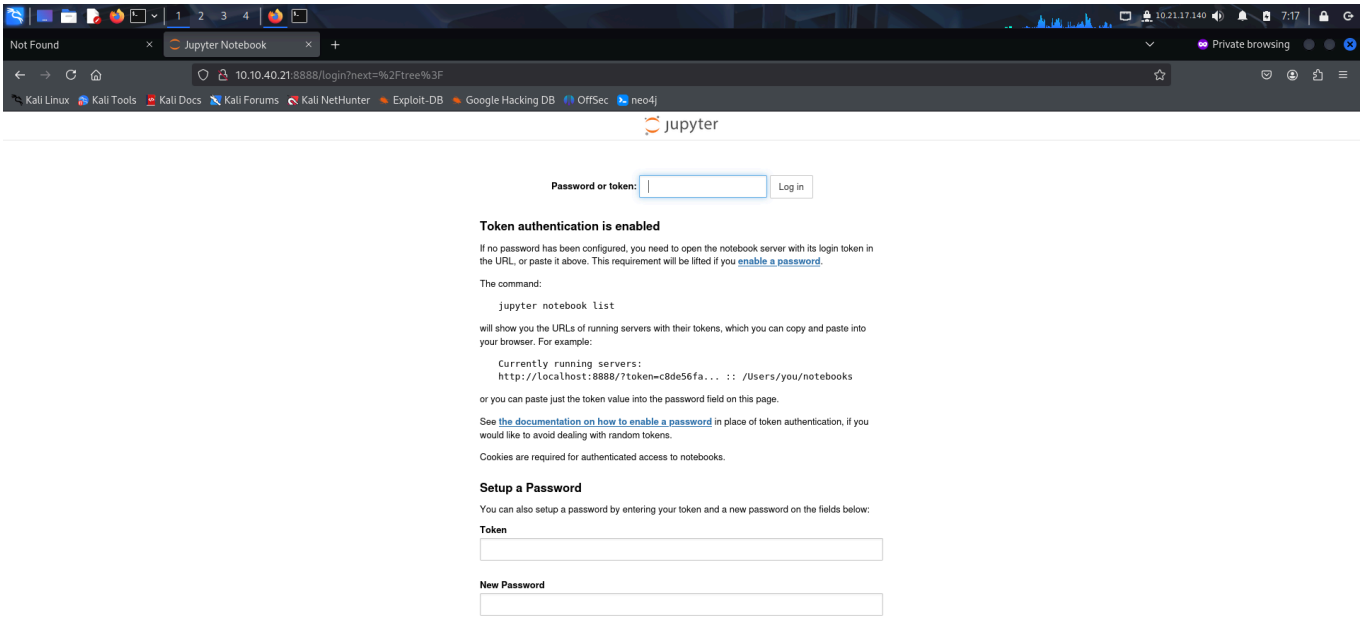




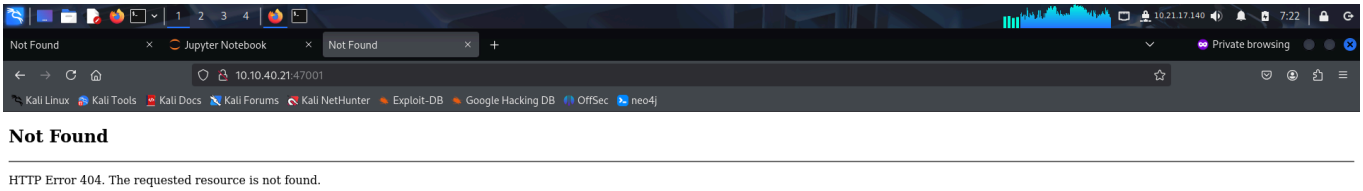
FOOTHOLD

The nmap scan revealed multiple services running like **ssh**, **rpc**, **smb**, **http**, **winrm** etc.

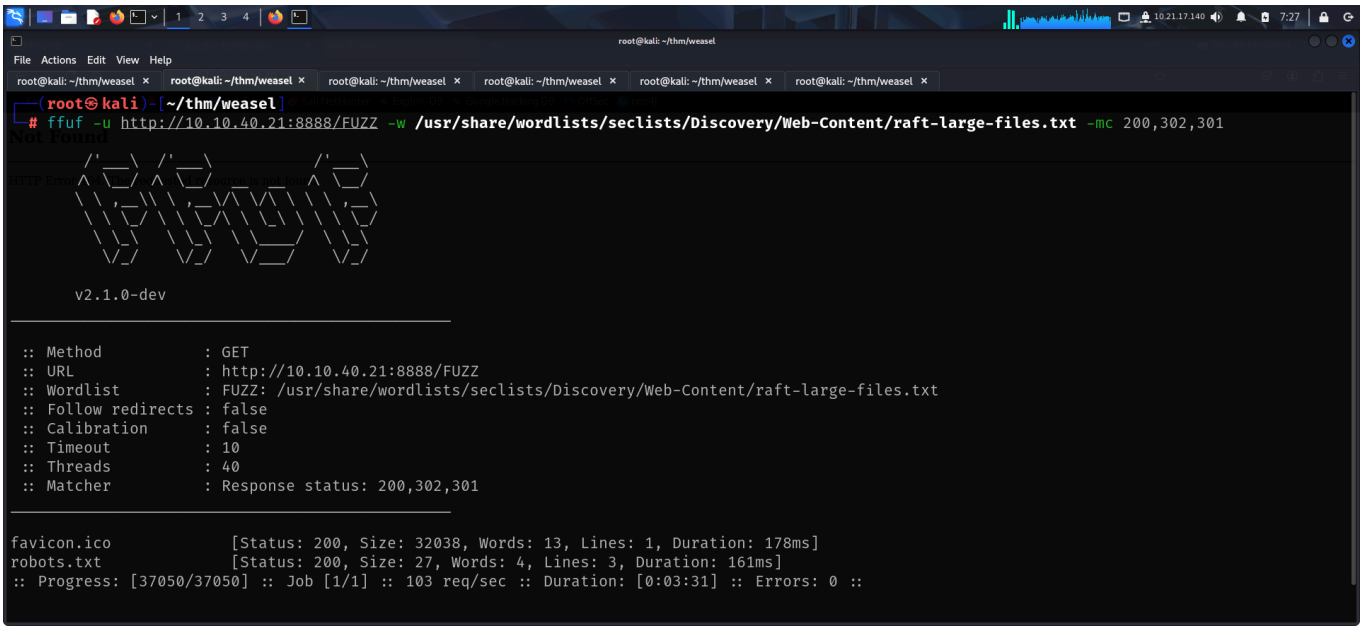
I started enumeration with **http**. I accessed it on my browser and found a jupyter notebook login page.

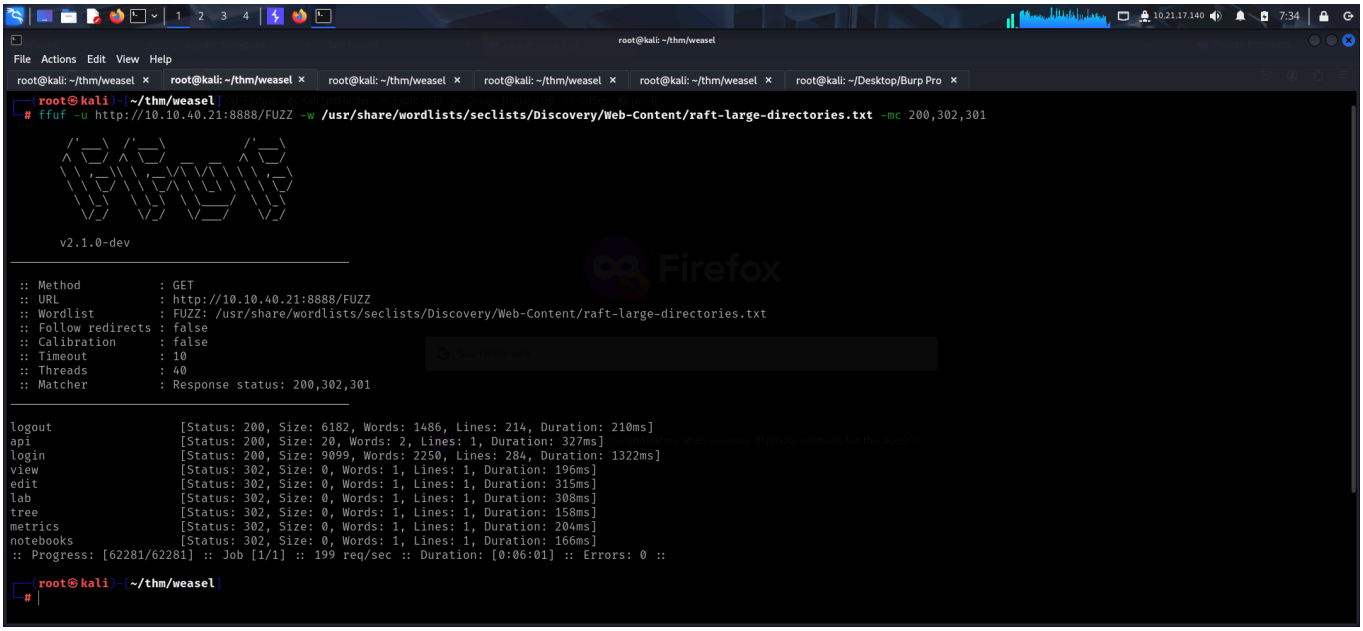


I also checked the other port that was running **http** just to leave out nothing.

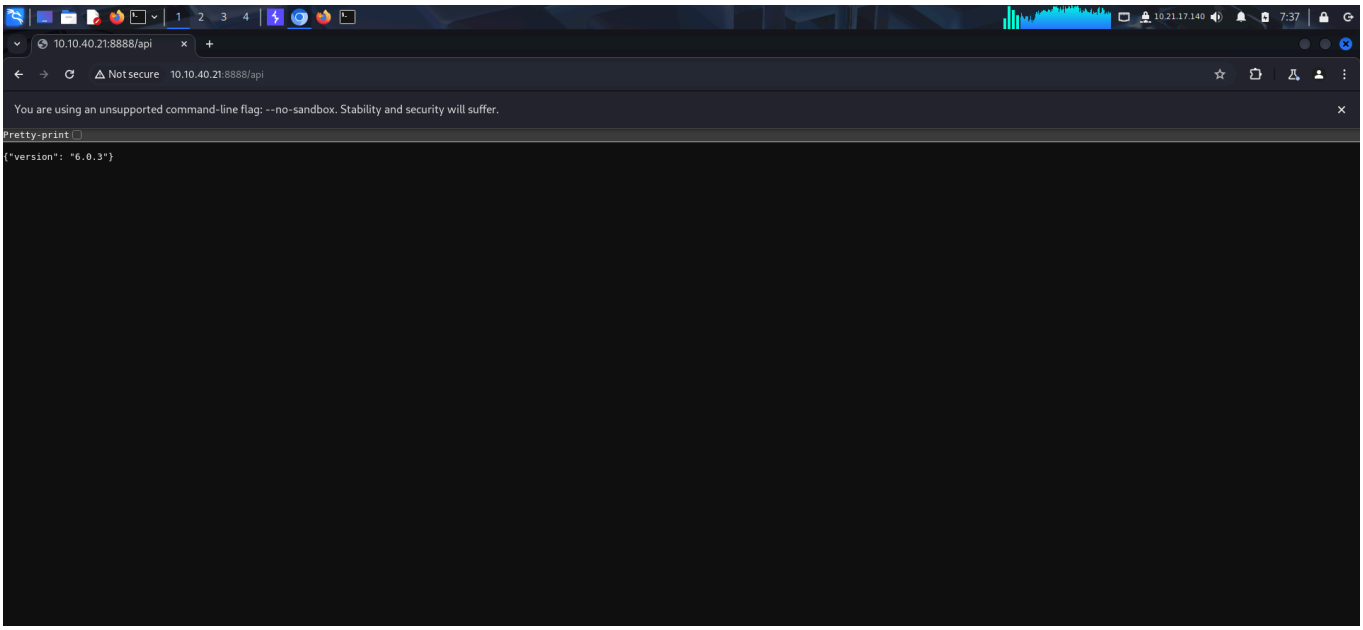


I then looked for hidden files and directories using **ffuf** on the jupyter notebook page.

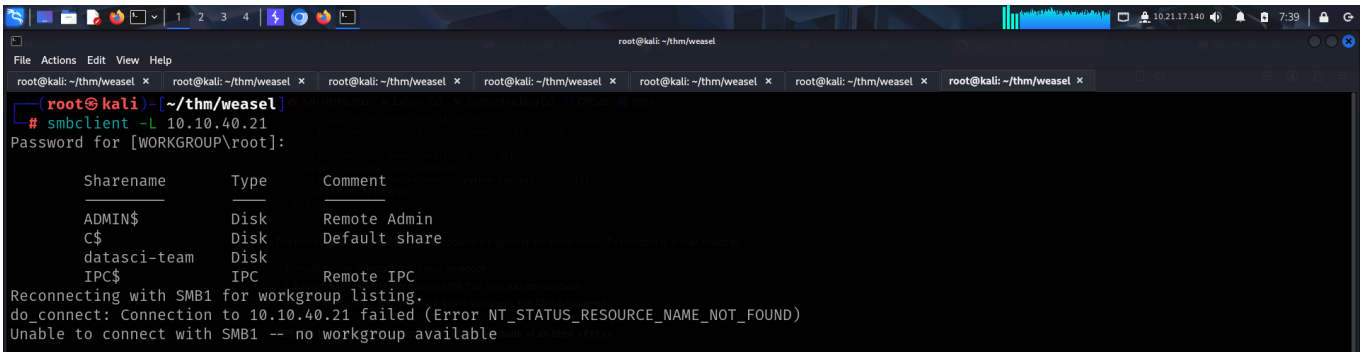




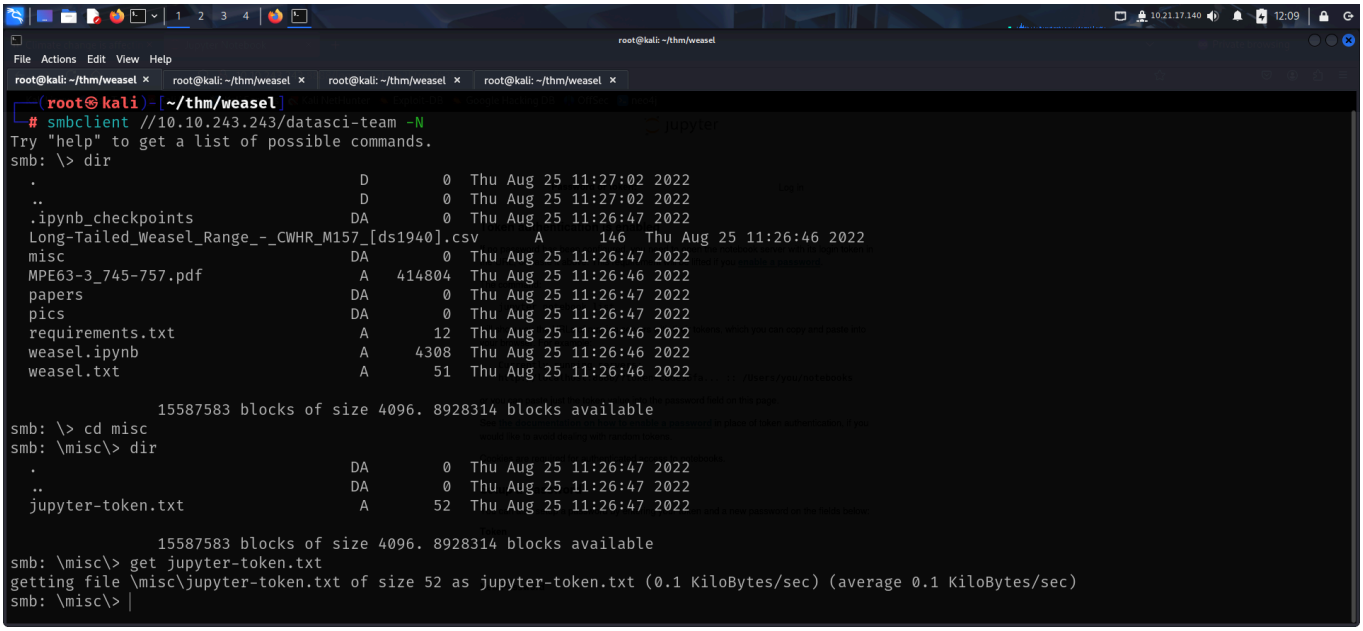
I found an *api* endpoint but found nothing interesting their.

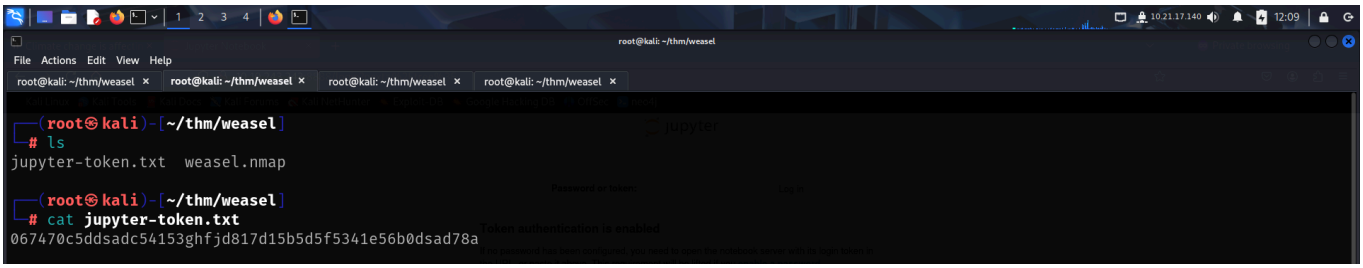


I then enumerated **smb** and listed the shares on the target.

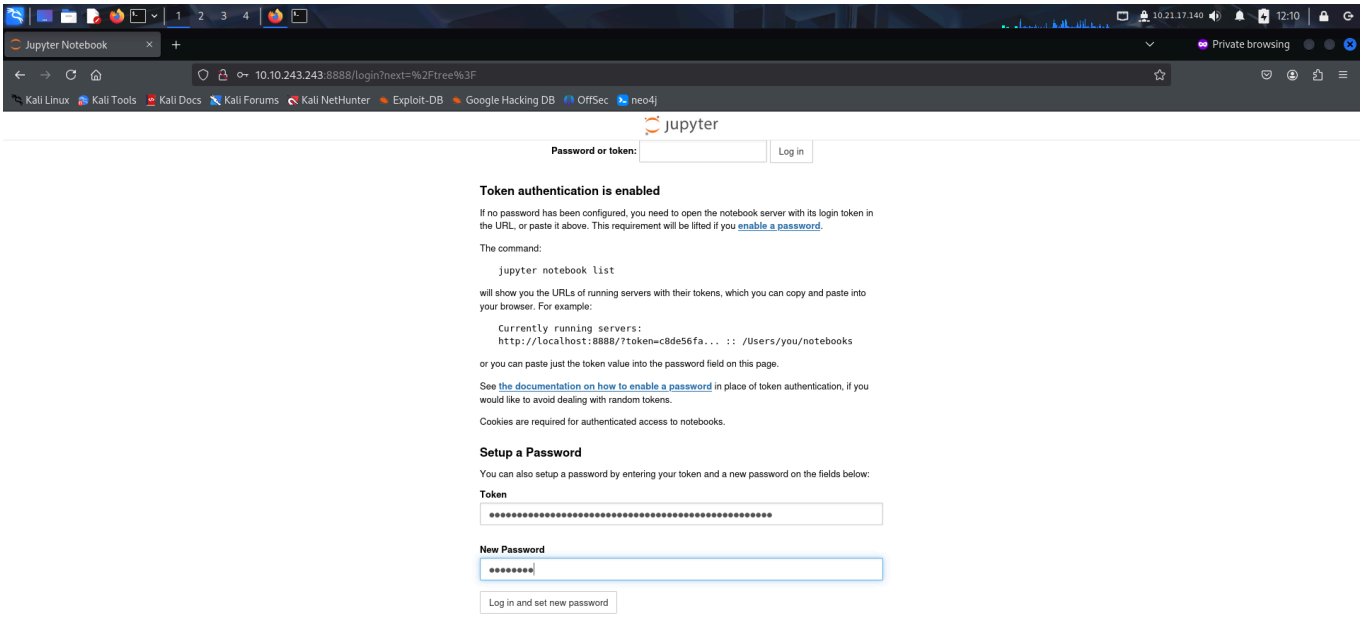


There was an interesting share called *datasci-team*. I then used **smbclient** to connect to the share and found the jupyter token. I could use this token to log into the jupyter notebook. So I downloaded this token.

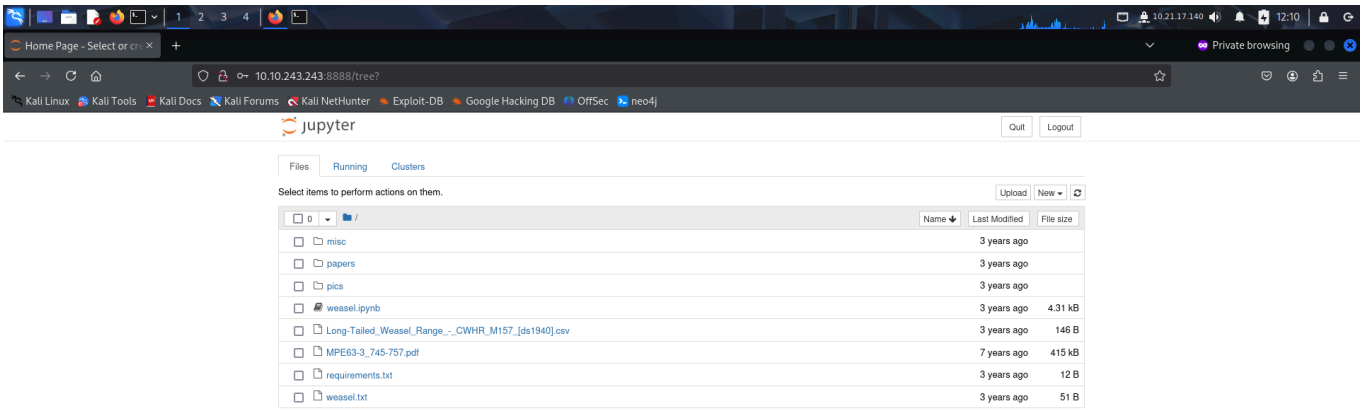




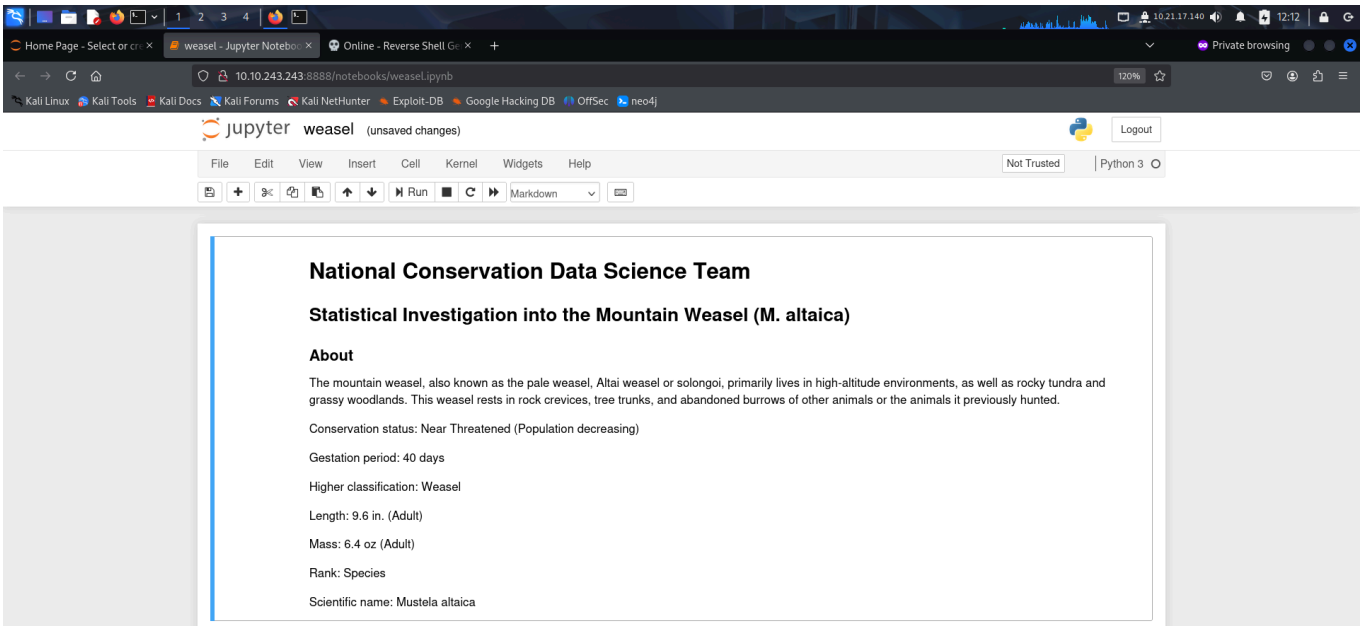
I pasted the token and used it to set the password as **password**



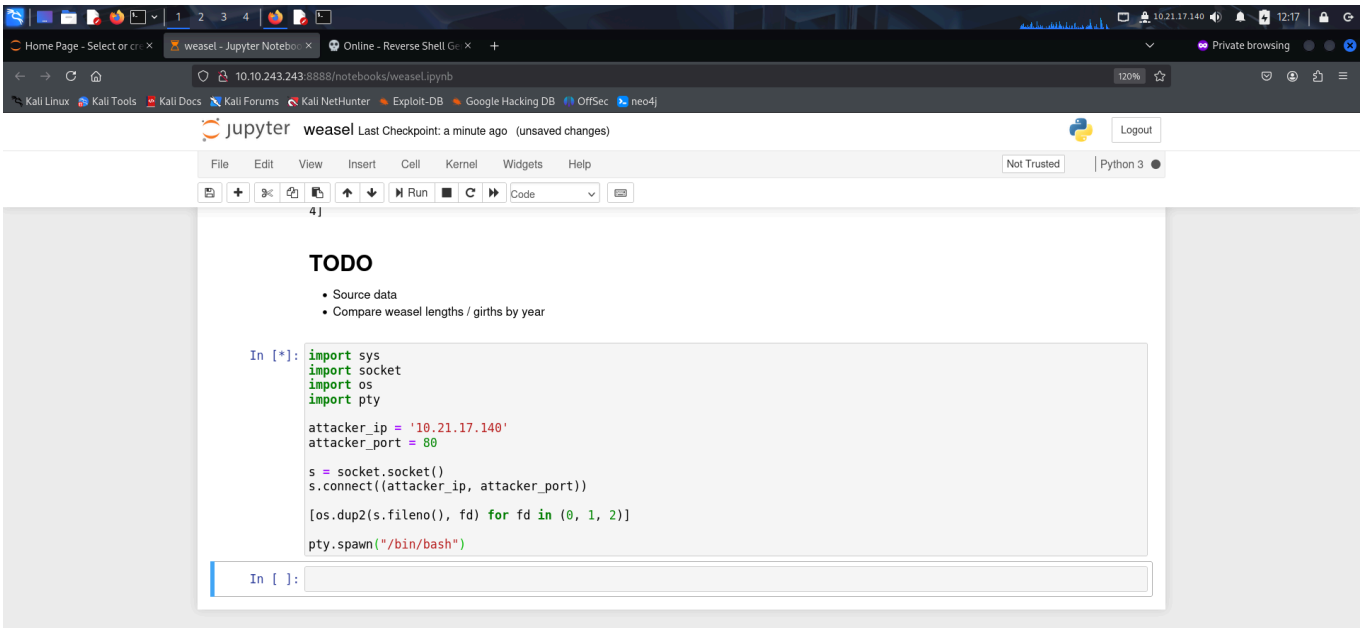
I found a bunch of files. The *workbook* file seemed interesting so I opened it.



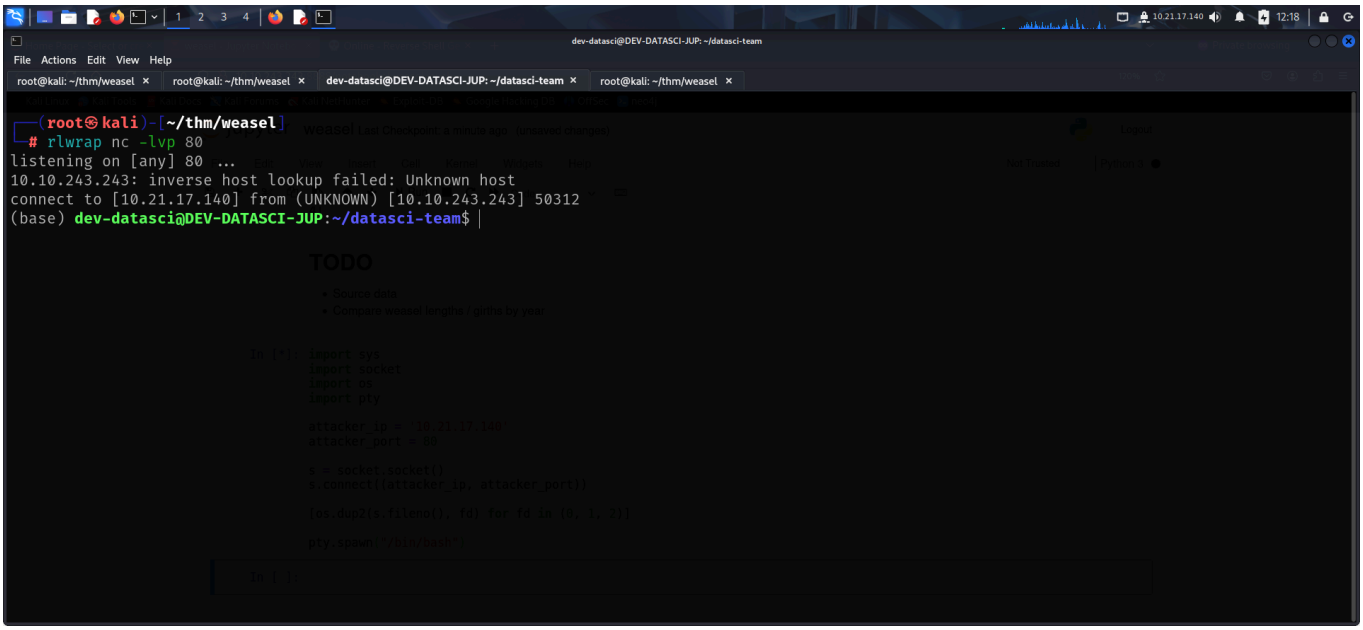
I was allowed to run **python** code in this workbook.



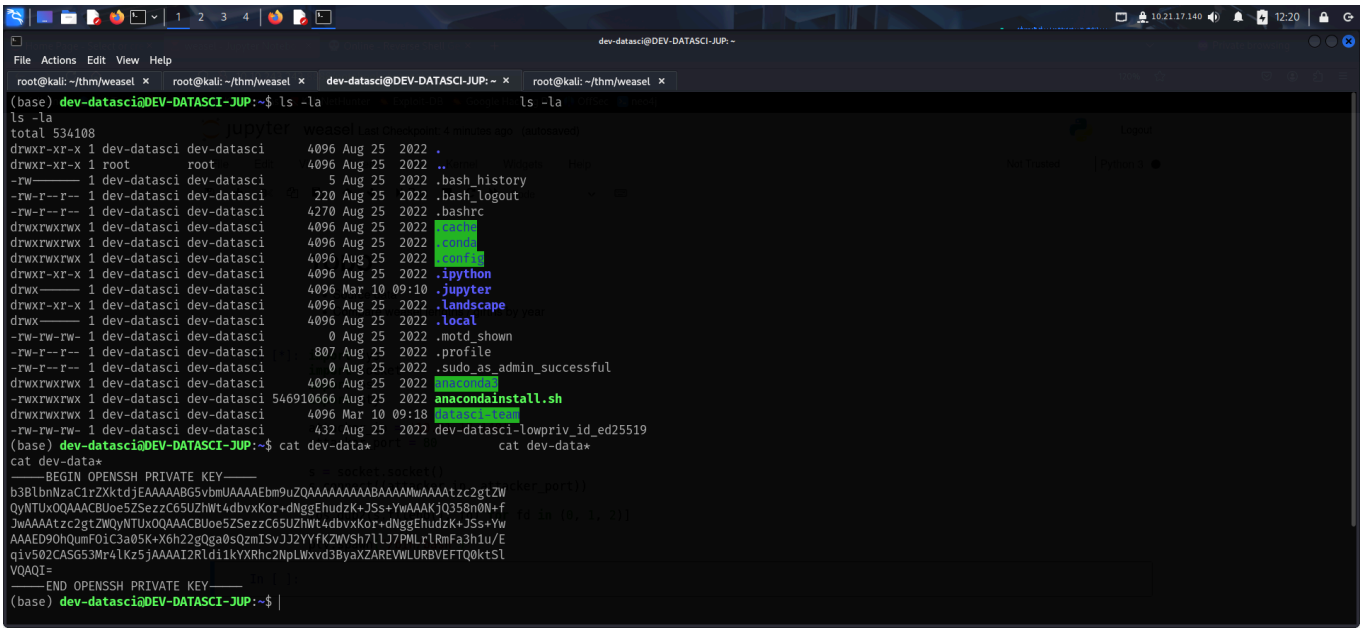
So I added a new code block and a simple **python** code to get a reverse shell.



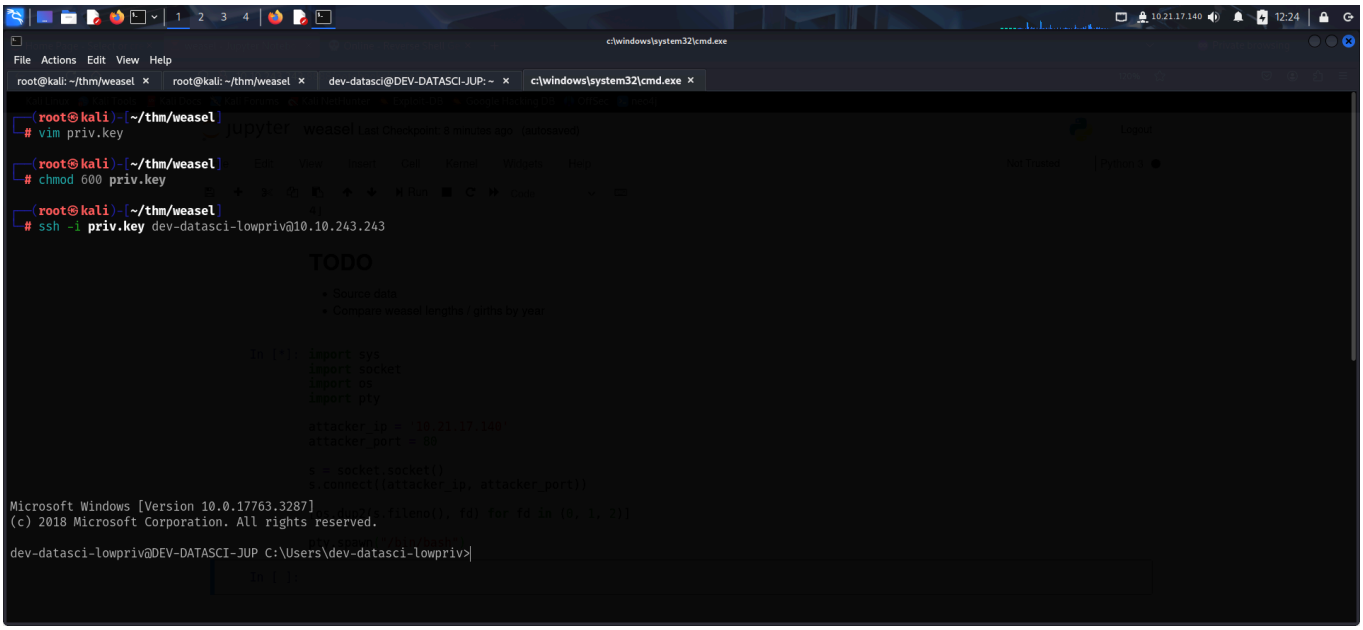
I started a listener and executed the code to get a reverse shell from the target.



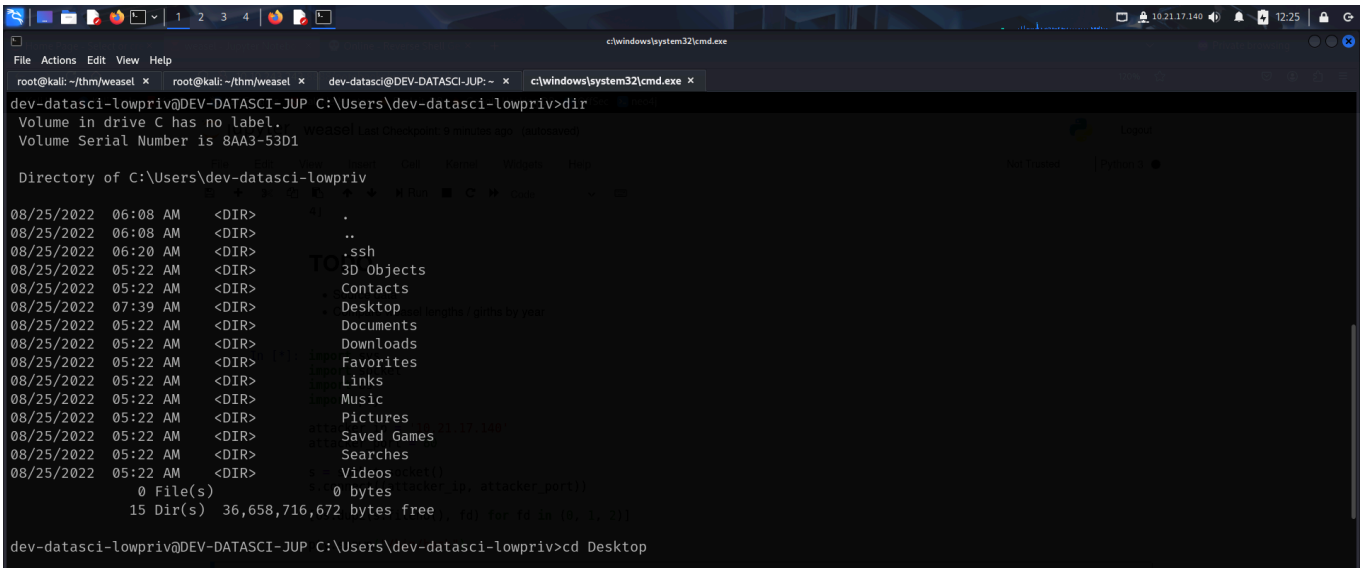
I found an **ssh** private key of the *dev-datasci-lowpriv* user.



I saved this private key on my local system and used it to log in through **ssh**.

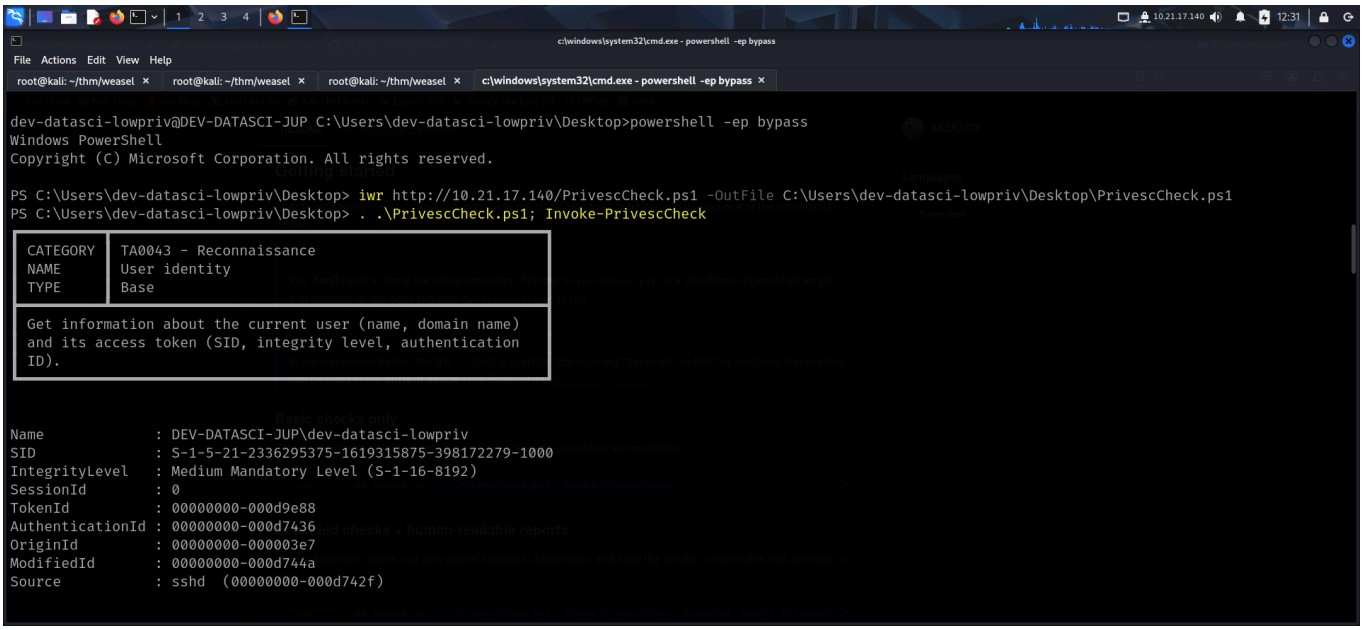


Finally, I got the user flag from *Desktop*.

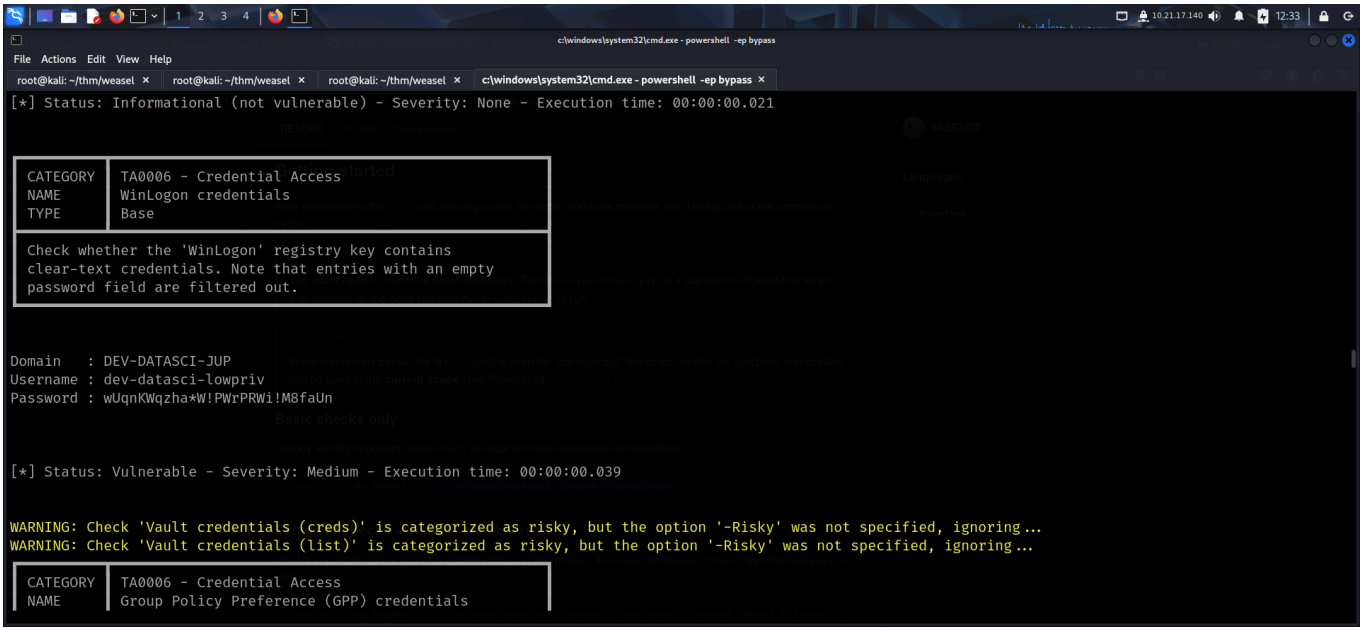


PRIVILEGE ESCALATION

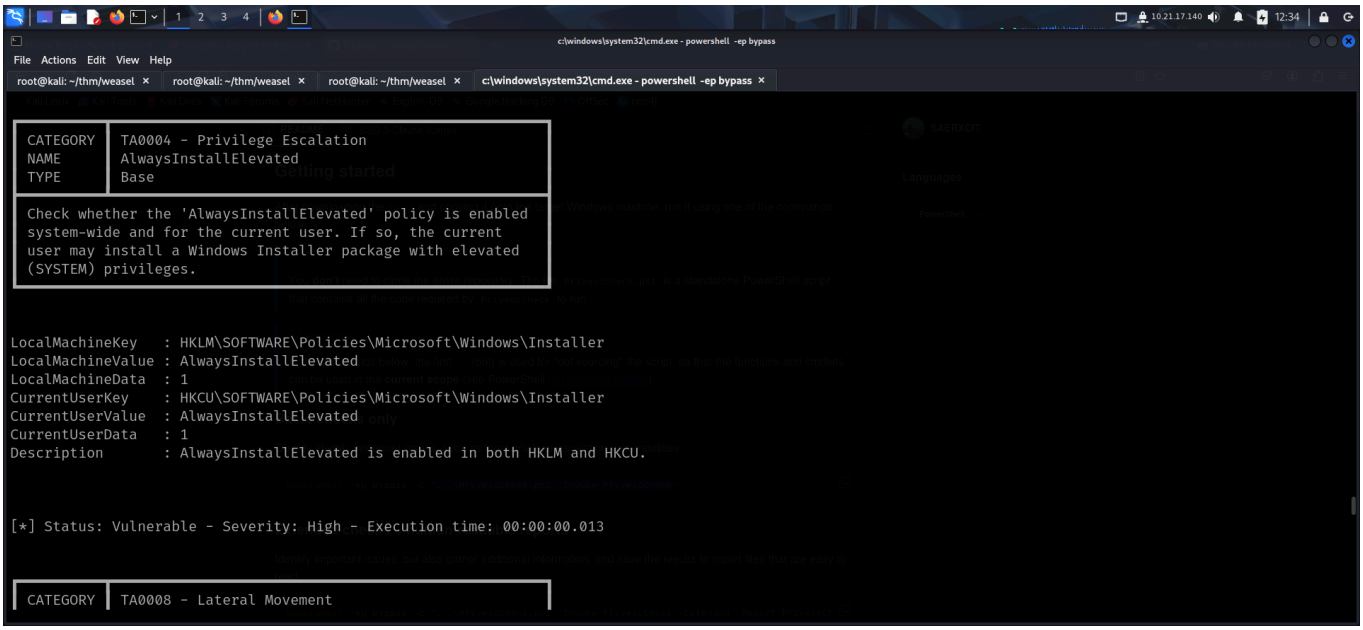
To enumerate misconfigurations, I downloaded **PrivescCheck** and ran it on the system.



It discovered and extracted the **winlogon** credentials.

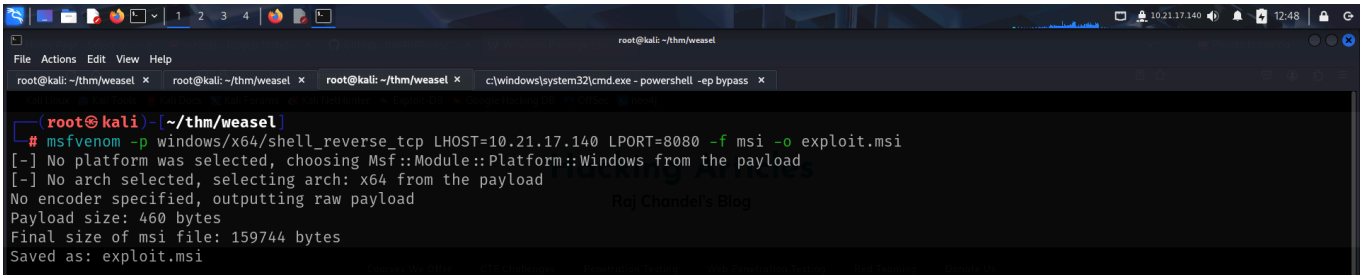


It then found a vulnerability that could be used to escalate our privilege.

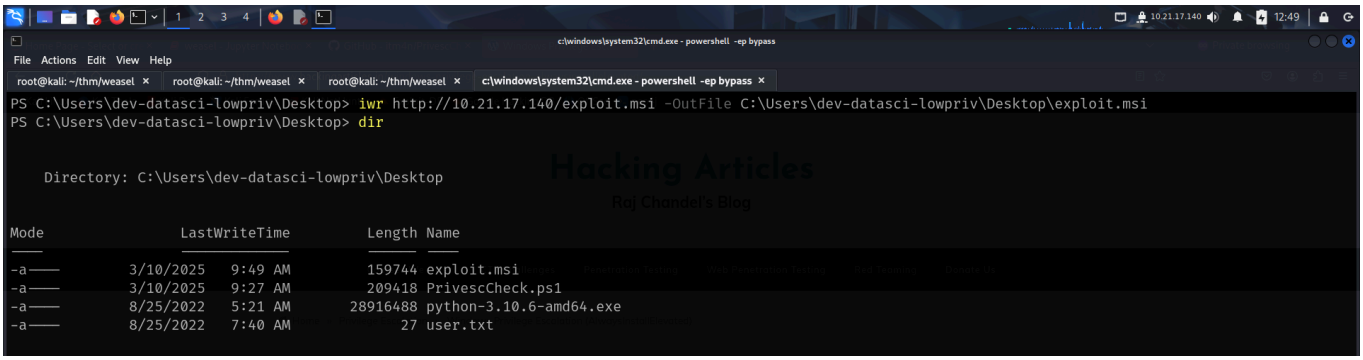


I referred to the below article to use the **AlwaysinstallElevated** policy to get admin access : https://www.hackingarticles.in/windows-privilege-escalation-alwaysinstallelevated/

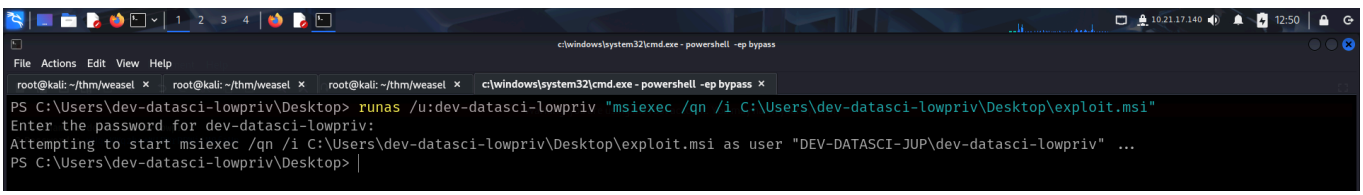
Hence, I created a payload using **msfvenom**.



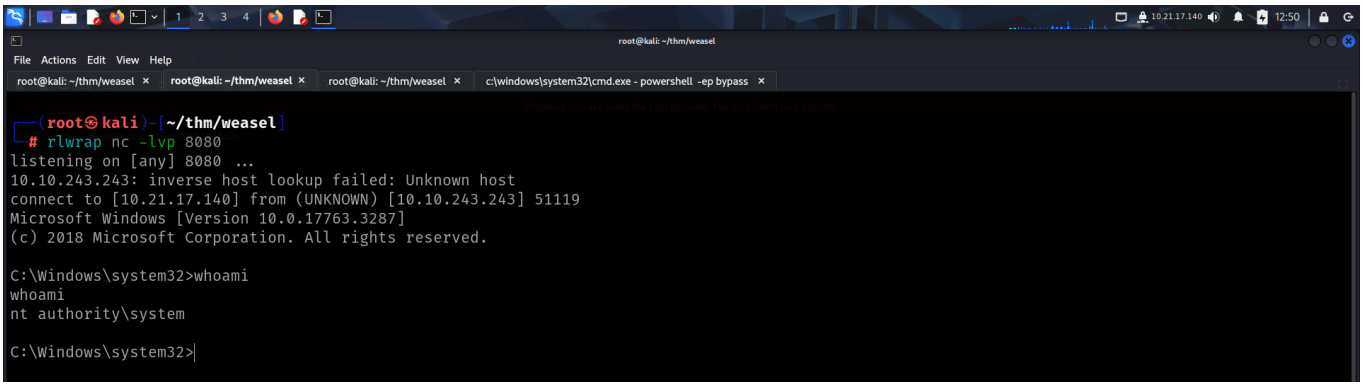
I downloaded this payload on the system and started a **netcat** listener on my local machine.



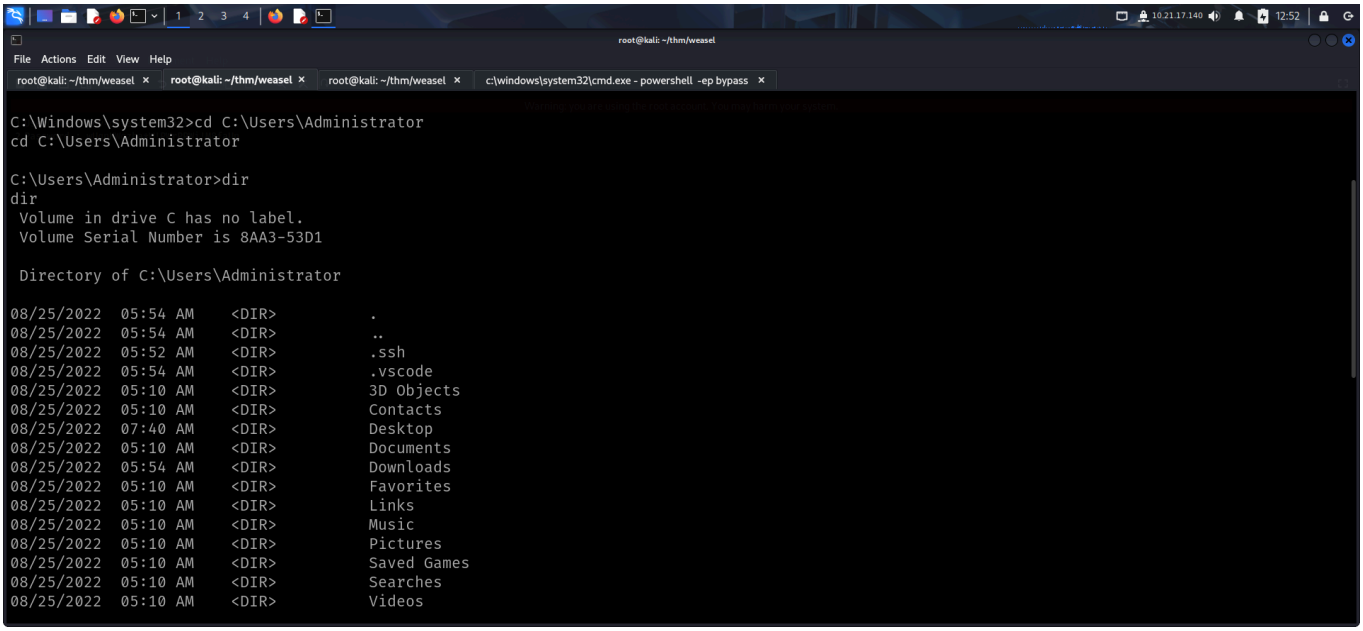
I ran the payload with **msiexec** as *dev-datasci-lowpriv* user.

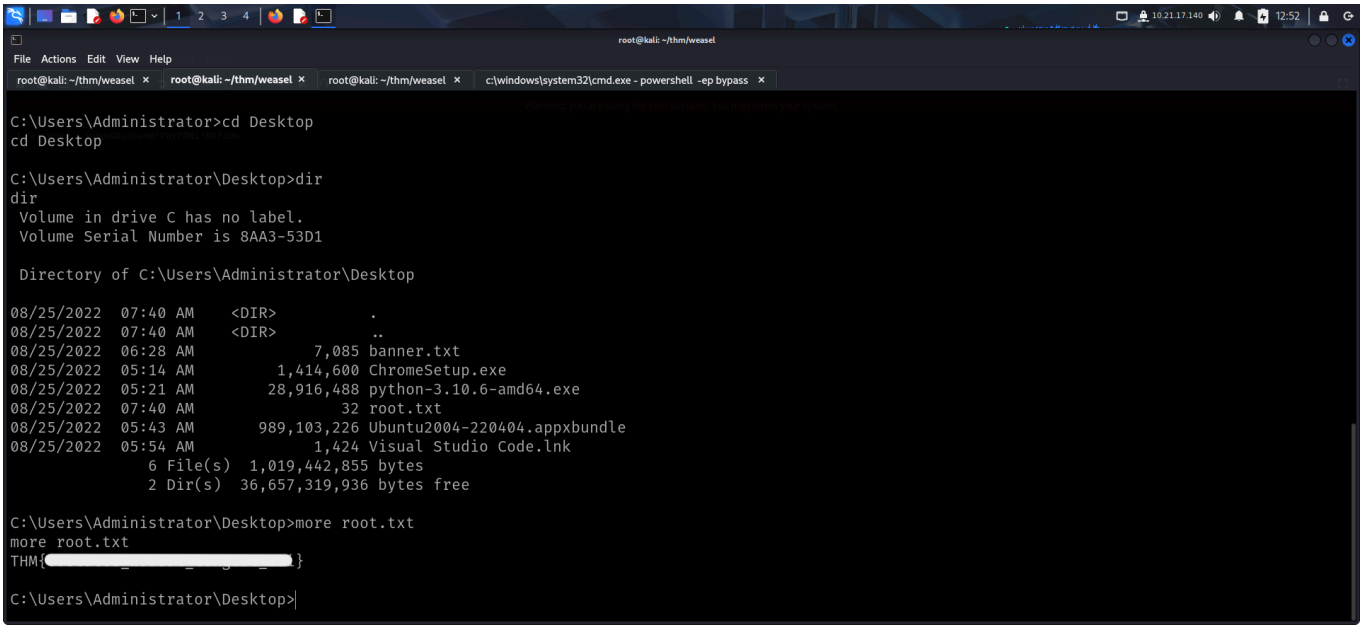


Finally, I got a reverse shell as **nt authority system**.



I then captured the root flag from *Administrator*'s Desktop.





That's it from my side! Until next time :)