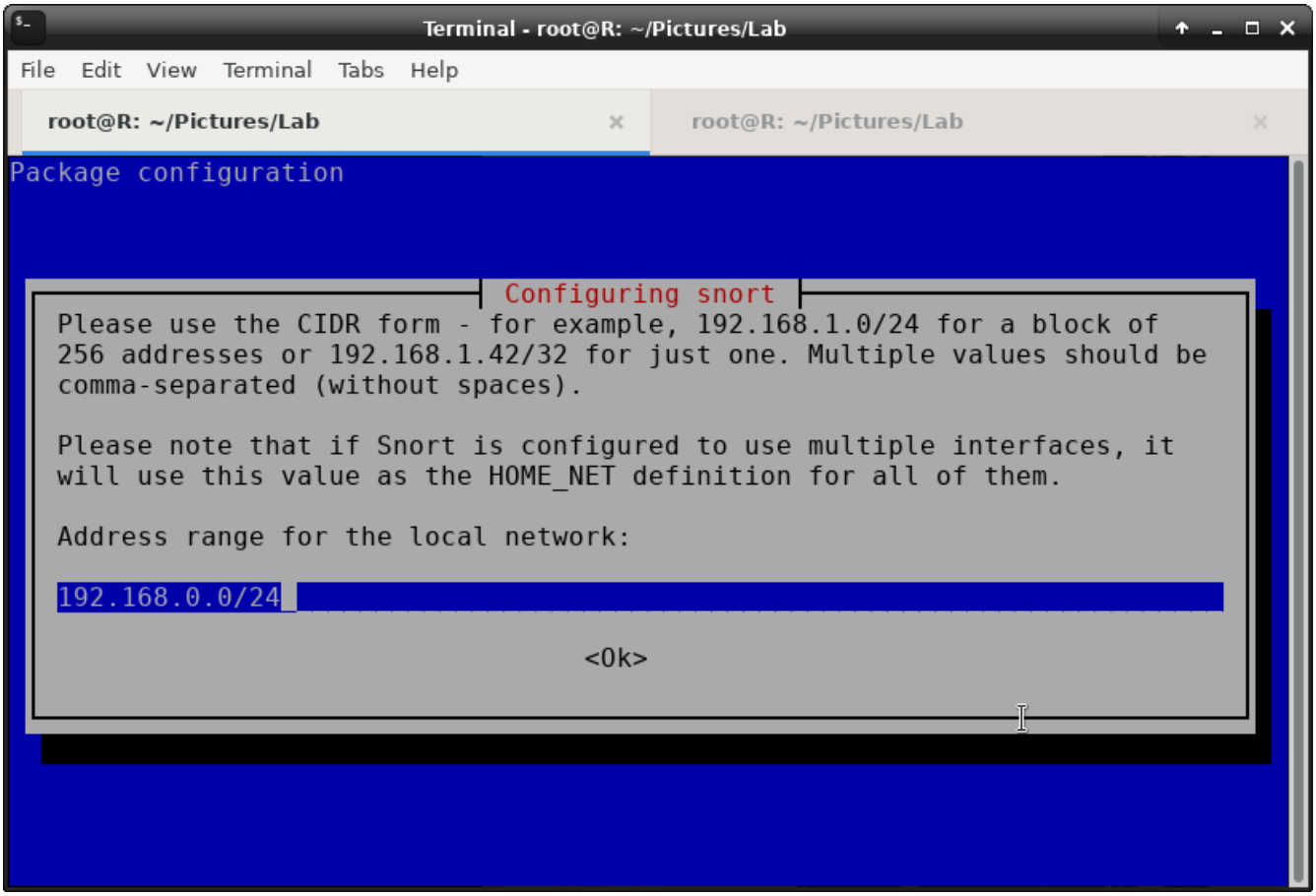
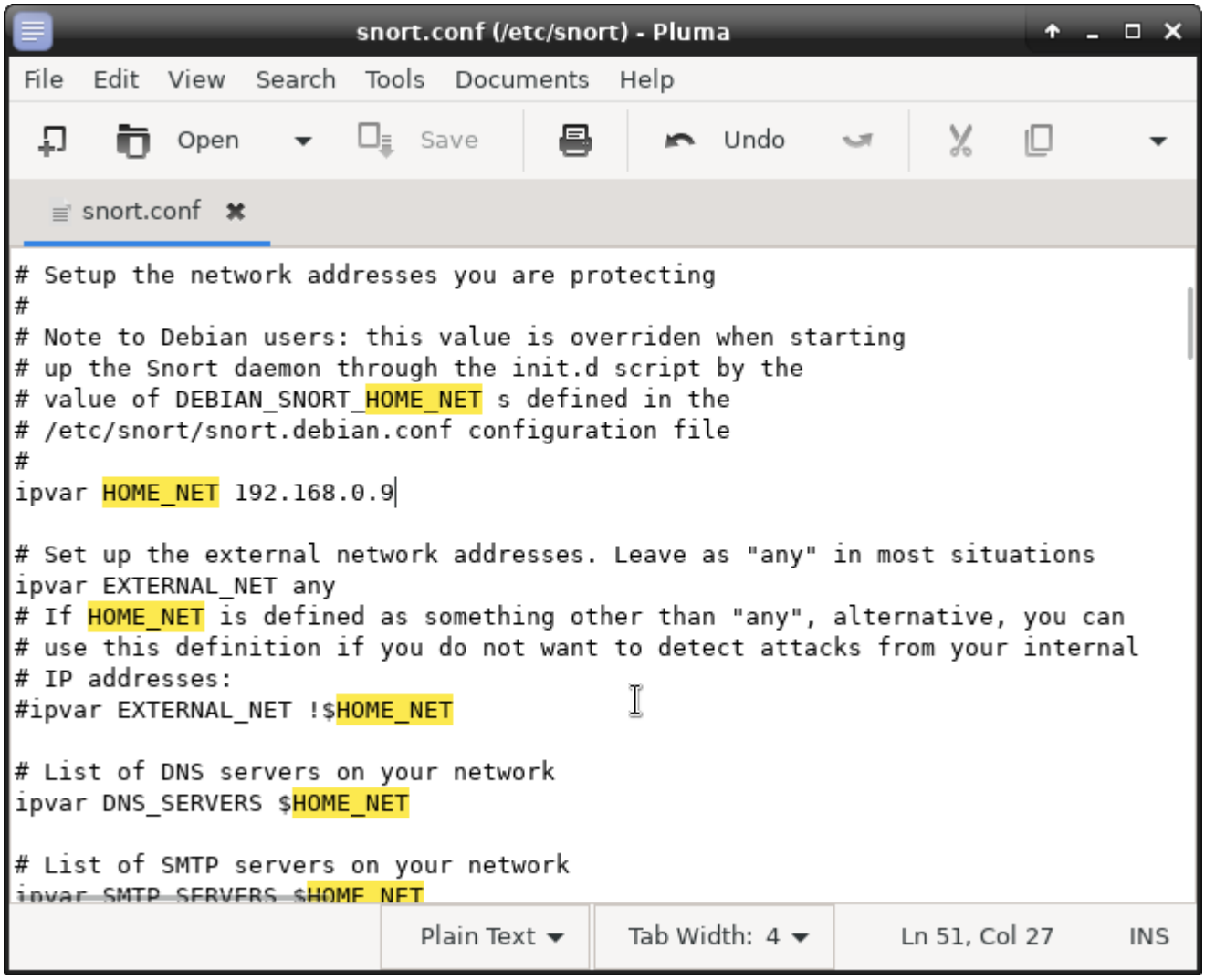
Rodrigo Castillo Camargo
Laboratorio 8: sistema de detección de intrusiones

Para el laboratorio de Detección de Intrusiones, usaremos la herramienta Snort

```
Terminal - root@R: ~/Pictures/Lab
File  Edit  View  Terminal  Tabs  Help
root@R:~/Pictures/Lab# sudo apt install snort*
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'snort-pgsql' for glob 'snort*'
Note, selecting 'snort-doc' for glob 'snort*'
Note, selecting 'snort-rules-default' for glob 'snort*'
Note, selecting 'snort-common' for glob 'snort*'
Note, selecting 'snort-mysql' for glob 'snort*'
Note, selecting 'snort' for glob 'snort*'
Note, selecting 'snort-common-libraries' for glob 'snort*'
Note, selecting 'snort-rules' for glob 'snort*'
The following package was automatically installed and is no longer required:
  libisl19
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libdaq2 libdumbnet1 oinkmaster
The following NEW packages will be installed:
  libdaq2 libdumbnet1 oinkmaster snort snort-common snort-common-libraries
  snort-doc snort-rules-default
0 upgraded, 8 newly installed, 0 to remove and 84 not upgraded.
Need to get 4,356 kB of archives.
After this operation, 15.5 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

en la máquina víctima, la cuál está corriendo un servidor de apache.


Terminal - root@R: ~/Pictures/Lab
File Edit View Terminal Tabs Help
root@R: ~/Pictures/Lab
root@R: ~/Pictures/Lab
Package configuration
Configuring snort
Please use the CIDR form - for example, 192.168.1.0/24 for a block of 256 addresses or 192.168.1.42/32 for just one. Multiple values should be comma-separated (without spaces).
Please note that if Snort is configured to use multiple interfaces, it will use this value as the HOME_NET definition for all of them.
Address range for the local network:
192.168.0.0/24
<Ok>



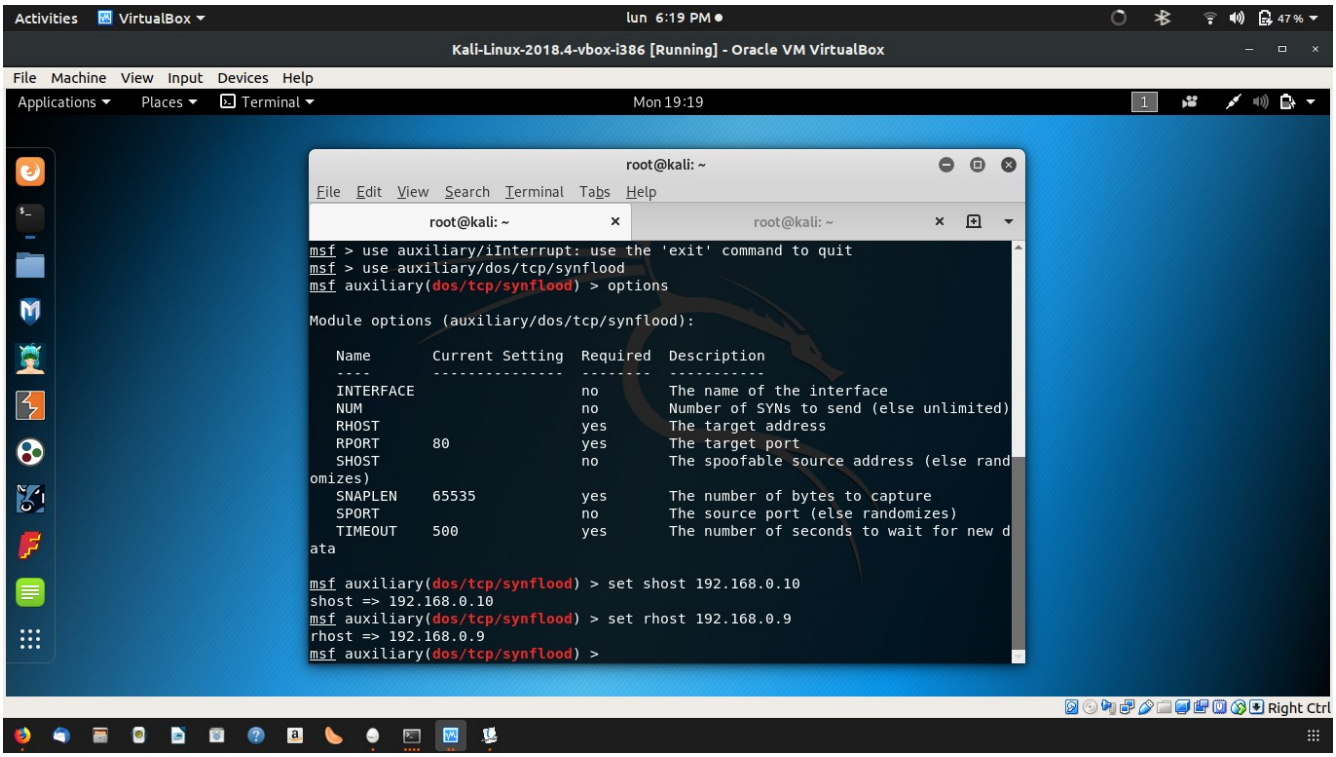
Una vez configurado Snort, revisé los archivos que contienen las reglas del sistema de detección de intrusiones

```
Terminal - root@R: /etc/snort/rules
File  Edit  View  Terminal  Tabs  Help
  GNU nano 4.4                    icmp.rules

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP ISS Pinger"; itype:8; >
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP L3retriever Ping"; ico>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Nemesis v1.1 Echo"; ds>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING NMAP"; dsize:0; i>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP icmpenum v1.1.1"; dsiz>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP redirect host"; icode:>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP redirect net"; icode:0>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP superscan echo"; dsize>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP traceroute ipopts"; ip>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP webtrends scanner"; ic>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Source Quench"; icode:>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Broadscan Smurf Scanne>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING speedera"; itype:>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP TJPingPro1.1Build 2 Wi>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING WhatsupGold Windo>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING CyberKit 2.2 Wind>
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING Sniffer Pro/NetXR>
alert icmp any any -> any any (msg:"ICMP Destination Unreachable Communication >
alert icmp any any -> any any (msg:"ICMP Destination Unreachable Communication >
                              [ Cancelled ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line
```

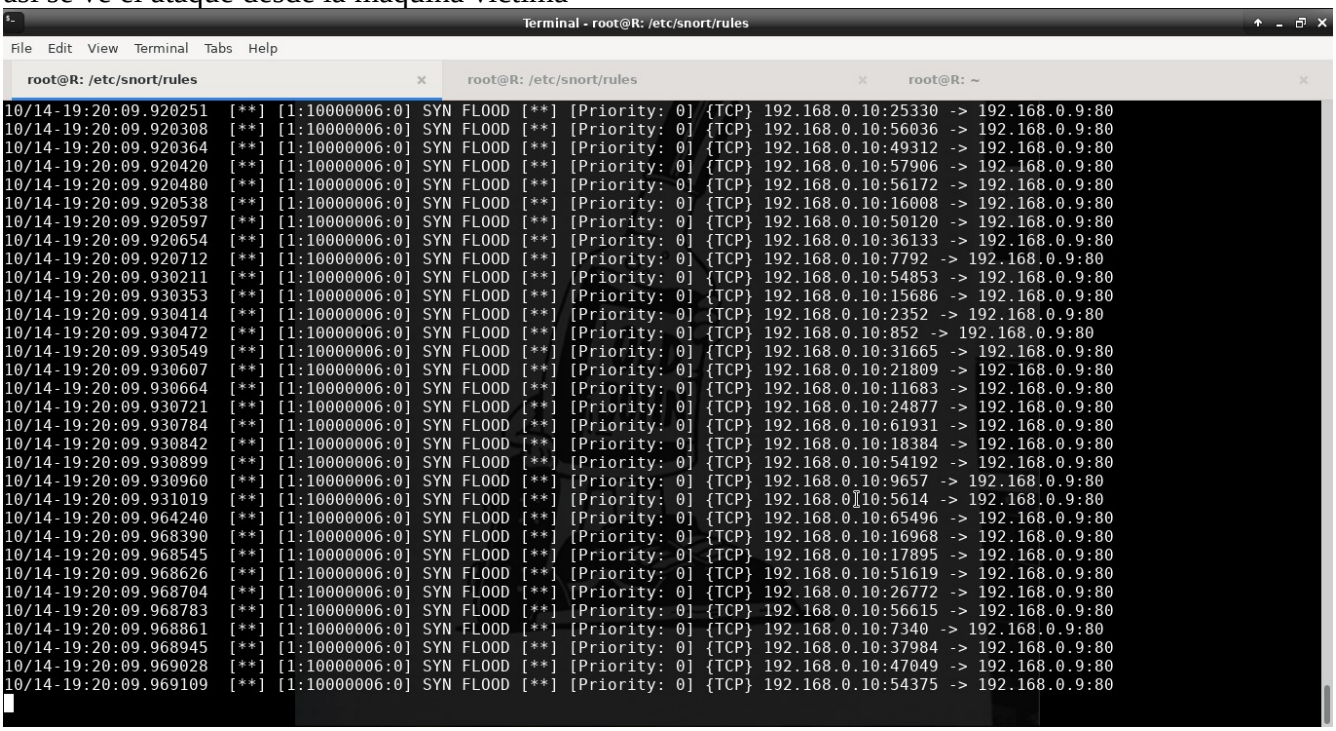
Configuración para la regla de TCP – SYN FLOOD

```
Terminal - root@R: /etc/snort/rules
File  Edit  View  Terminal  Tabs  Help
  GNU nano 4.4                    local.rules                    Modified
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert tcp any any -> 192.168.0.9 (msg :" SYN Flood Dos" ; fags: S ; sid : 1000006;)

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo      M-A Mark Text
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo      M-6 Copy Text
```

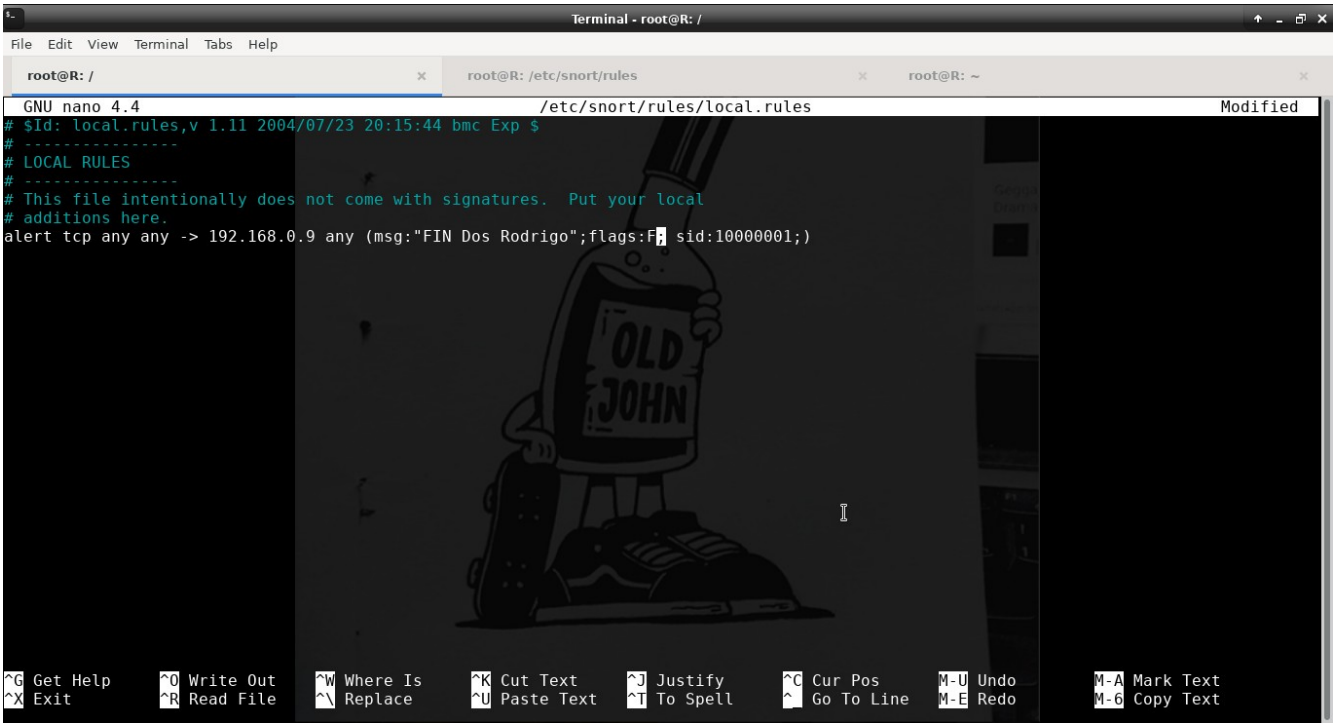
una vez configurado, lo ataqué desde la máquina atacante

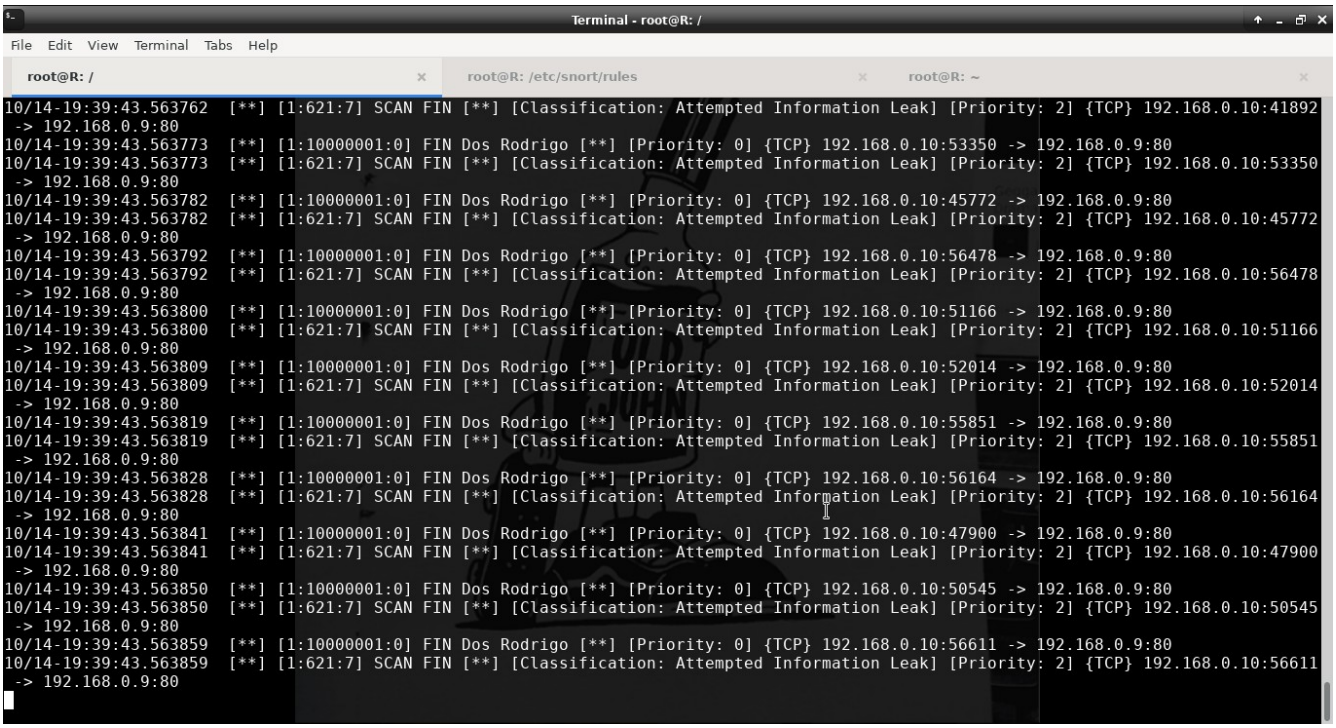


así se ve el ataque desde la máquina víctima



Ahora, con el ataque FIN Flood





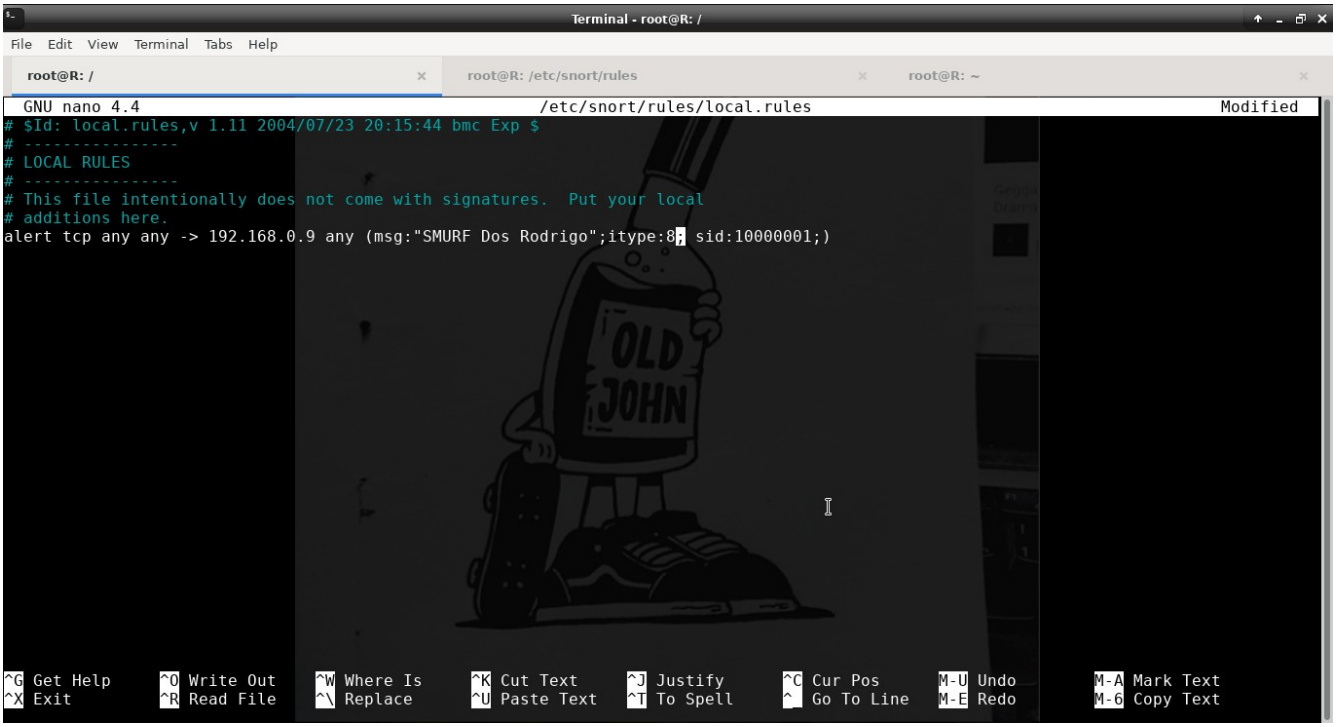
ahora con el ataque PUSH ACK Flood

```
Terminal - root@R: /
File  Edit  View  Terminal  Tabs  Help
root@R: /        root@R: /etc/snort/rules        root@R: ~
10/14-19:32:41.432551  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:18512 -> 192.168.0.9:80
10/14-19:32:41.432594  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:21118 -> 192.168.0.9:80
10/14-19:32:41.432637  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:24540 -> 192.168.0.9:80
10/14-19:32:41.432688  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:23135 -> 192.168.0.9:80
10/14-19:32:41.432740  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:24569 -> 192.168.0.9:80
10/14-19:32:41.432793  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:23086 -> 192.168.0.9:80
10/14-19:32:41.432845  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:24789 -> 192.168.0.9:80
10/14-19:32:41.432898  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:23370 -> 192.168.0.9:80
10/14-19:32:41.432950  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:24702 -> 192.168.0.9:80
10/14-19:32:41.433002  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:24206 -> 192.168.0.9:80
10/14-19:32:41.433053  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:23829 -> 192.168.0.9:80
10/14-19:32:41.433105  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:24969 -> 192.168.0.9:80
10/14-19:32:41.433161  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:24426 -> 192.168.0.9:80
10/14-19:32:41.433215  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:19722 -> 192.168.0.9:80
10/14-19:32:41.433266  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:25078 -> 192.168.0.9:80
10/14-19:32:41.433318  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:22189 -> 192.168.0.9:80
10/14-19:32:41.433369  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:20451 -> 192.168.0.9:80
10/14-19:32:41.433421  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:24559 -> 192.168.0.9:80
10/14-19:32:41.433474  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:23254 -> 192.168.0.9:80
10/14-19:32:41.433524  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:24996 -> 192.168.0.9:80
10/14-19:32:41.433569  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:24169 -> 192.168.0.9:80
10/14-19:32:41.433620  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:24383 -> 192.168.0.9:80
10/14-19:32:41.433672  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:19769 -> 192.168.0.9:80
10/14-19:32:41.433723  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:20725 -> 192.168.0.9:80
10/14-19:32:41.433775  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:22188 -> 192.168.0.9:80
10/14-19:32:41.433828  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:24378 -> 192.168.0.9:80
10/14-19:32:41.433876  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:24549 -> 192.168.0.9:80
10/14-19:32:41.433928  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:22260 -> 192.168.0.9:80
10/14-19:32:41.433977  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:18972 -> 192.168.0.9:80
10/14-19:32:41.434027  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:24682 -> 192.168.0.9:80
10/14-19:32:41.434078  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:24692 -> 192.168.0.9:80
10/14-19:32:41.434129  [**] [1:10000001:0] PUSH-ACK Flood Dos Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:24353 -> 192.168.0.9:80
```

ahora con el ataque RESET FLOOD:

```
Terminal - root@R: /
File  Edit  View  Terminal  Tabs  Help
root@R: /        root@R: /etc/snort/rules        root@R: ~
10/14-19:36:08.382266  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:54858 -> 192.168.0.9:80
10/14-19:36:08.382281  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:50431 -> 192.168.0.9:80
10/14-19:36:08.382296  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:50958 -> 192.168.0.9:80
10/14-19:36:08.382309  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:56335 -> 192.168.0.9:80
10/14-19:36:08.382323  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:56514 -> 192.168.0.9:80
10/14-19:36:08.382337  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:58762 -> 192.168.0.9:80
10/14-19:36:08.382351  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:60001 -> 192.168.0.9:80
10/14-19:36:08.382365  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:51907 -> 192.168.0.9:80
10/14-19:36:08.382379  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:57758 -> 192.168.0.9:80
10/14-19:36:08.382393  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:58249 -> 192.168.0.9:80
10/14-19:36:08.382406  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:52414 -> 192.168.0.9:80
10/14-19:36:08.382420  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:55279 -> 192.168.0.9:80
10/14-19:36:08.382456  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:56966 -> 192.168.0.9:80
10/14-19:36:08.382493  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:46287 -> 192.168.0.9:80
10/14-19:36:08.382528  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:61637 -> 192.168.0.9:80
10/14-19:36:08.382564  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:61784 -> 192.168.0.9:80
10/14-19:36:08.382598  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:47417 -> 192.168.0.9:80
10/14-19:36:08.382640  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:51237 -> 192.168.0.9:80
10/14-19:36:08.382674  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:59291 -> 192.168.0.9:80
10/14-19:36:08.382708  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:51177 -> 192.168.0.9:80
10/14-19:36:08.382743  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:62087 -> 192.168.0.9:80
10/14-19:36:08.382776  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:62088 -> 192.168.0.9:80
10/14-19:36:08.382809  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:62093 -> 192.168.0.9:80
10/14-19:36:08.382845  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:62101 -> 192.168.0.9:80
10/14-19:36:08.382878  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:62113 -> 192.168.0.9:80
10/14-19:36:08.382912  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:62136 -> 192.168.0.9:80
10/14-19:36:08.382946  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:62139 -> 192.168.0.9:80
10/14-19:36:08.382979  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:62141 -> 192.168.0.9:80
10/14-19:36:08.383011  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:62149 -> 192.168.0.9:80
10/14-19:36:08.383043  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:62155 -> 192.168.0.9:80
10/14-19:36:08.383081  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:62158 -> 192.168.0.9:80
10/14-19:36:08.383118  [**] [1:10000001:0] Reset DoS Rodrigo [**] [Priority: 0] {TCP} 192.168.0.10:54133 -> 192.168.0.9:80
```

Finalmente con el ataque SMURF tuve problemas:



pues me decía que no existían reglas para ese ataque.