

UC: Segurança em Redes

TP5a Report – Práticas com Firewalls (IPTables)

Students (Nº / Name):

- 72362 – Miguel Costa
- 74413 – Gonçalo Pereira
- 74014 – Nuno Vieira
- 75280 – José Silva
- 76234 – Matias Araújo

Material

1. Máquinas Virtuais VirtualBox CentOS 6.8 e Khali/XubunCore

Ambas configuradas com dois Network Adapters, um NAT e uma Internal Network.

NAT para ter acesso à internet.

Internal Network para a máquina Guest Khali/Core e a máquina Server CentOS poderem comunicar por endereços IP definidos manualmente (172.16.1.1 - Khali/Core, 172.16.1.2 - CentOS), usando os seguintes comandos:

- `ip addr add 172.16.1.x dev <interface>`
- `ifconfig <interface> 172.16.1.x netmask 255.255.255.0`

Tarefa 1

1. Resultado do comando netstat -l, resultados semelhantes para todos os membros do grupo.

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address          State
tcp      0      0 *:sunrpc                 *:                        LISTEN
tcp      0      0 *:40018                  *:                        LISTEN
tcp      0      0 *:ftp                    *:                        LISTEN
tcp      0      0 *:ssh                    *:                        LISTEN
tcp      0      0 localhost:ipp            *:                        LISTEN
tcp      0      0 localhost:smtp           *:                        LISTEN
tcp      0      0 *:36130                  *:                        LISTEN
tcp      0      0 *:sunrpc                 *:                        LISTEN
tcp      0      0 *:http                   *:                        LISTEN
tcp      0      0 *:ssh                    *:                        LISTEN
tcp      0      0 localhost:ipp            *:                        LISTEN
tcp      0      0 localhost:smtp           *:                        LISTEN
udp      0      0 *:sunrpc                 *:                        LISTEN
udp      0      0 *:42225                  *:                        LISTEN
udp      0      0 *:ipp                    *:                        LISTEN
udp      0      0 *:tenfold                *:                        LISTEN
udp      0      0 *:bootpc                 *:                        LISTEN
udp      0      0 localhost:719            *:                        LISTEN
udp      0      0 *:sunrpc                 *:                        LISTEN
udp      0      0 *:tenfold                *:                        LISTEN
udp      0      0 *:36688                  *:                        LISTEN
```

2. A firewall por predefinição encontrava-se ligada.

3.

- a. Obteve-se os mesmos resultados para todos os membros

```
[jpv@jpv ~]$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source    destination    state
    0    0 ACCEPT    all  --  any    any    anywhere  anywhere       RELATED,ESTABLISHED
    0    0 ACCEPT    icmp --  any    any    anywhere  anywhere
    0    0 ACCEPT    all  --  lo     any    anywhere  anywhere
    0    0 ACCEPT    tcp  --  any    any    anywhere  anywhere       state NEW tcp dpt:ssh
    0    0 REJECT    all  --  any    any    anywhere  anywhere       reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source    destination
    0    0 REJECT    all  --  any    any    anywhere  anywhere       reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source    destination
```

- b. Podemos observar que a firewall aceita qualquer pedido de ssh.

Em termos de nível de segurança, a firewall rejeita pacotes que não pertençam a uma sessão criada (sequência de pacotes enviados-recebidos).

4. Conteúdo do ficheiro iptables.dump

```
# Generated by iptables-save v1.4.7 on Fri Dec 22 22:25:22 2017
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [1034:107423]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Fri Dec 22 22:25:22 2017
~
```

5. As iptables ficaram com o seguinte conteúdo após ter-se desligado a firewall, ou seja, deixam passar e aceitar tudo o que é tráfego na rede pelo que não é seguro.

```
[jpvs@jpvs ~]$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
```

Tarefa 2

1. O comando de ping para o server teve o seguinte resultado

```
core@XubunCORE:~$ ping 188.82.220.124
PING 188.82.220.124 (188.82.220.124) 56(84) bytes of data.
64 bytes from 188.82.220.124: icmp_req=1 ttl=63 time=1.17 ms
64 bytes from 188.82.220.124: icmp_req=2 ttl=63 time=1.01 ms
64 bytes from 188.82.220.124: icmp_req=3 ttl=63 time=1.16 ms
64 bytes from 188.82.220.124: icmp_req=4 ttl=63 time=0.950 ms
64 bytes from 188.82.220.124: icmp_req=5 ttl=63 time=0.991 ms
64 bytes from 188.82.220.124: icmp_req=6 ttl=63 time=0.702 ms
^C
--- 188.82.220.124 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
```

2. O comando nmap dá-nos os serviços ativos no server e conforme a figura seguinte temos o serviço de ssh ativo na porta 22

```
core@XubunCORE:~$ sudo nmap -sS 172.16.1.2

Starting Nmap 5.21 ( http://nmap.org ) at 2017-12-22 23:35 WET
Nmap scan report for 172.16.1.2
Host is up (0.00020s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:90:7C:D6 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 5.13 seconds
```

3. Após o comando w3m <http://172.16.1.2> obtivemos o seguinte. Tal resultado é explicado pelo motivo de não termos autorizado na firewall o protocolo de http como input no server.

```
core@XubunCORE:~$ w3m http://172.16.1.2
w3m: Can't load http://172.16.1.2.
```

4. A resposta do servidor foi a seguinte e pelo mesmo motivo que na anterior alínea, não demos autorização na firewall do servidor ao protocolo ftp. Pelo que não conseguimos aceder ao servidor.

```
core@XubunCORE:~$ ftp 172.16.1.2
ftp: connect: No route to host
```

5. Não conseguimos aceder ao servidor.

```
core@XubunCORE:~$ ssh 172.16.1.2
The authenticity of host '172.16.1.2 (172.16.1.2)' can't be established.
RSA key fingerprint is fa:00:cb:53:e5:bb:9b:b0:e6:c6:2a:35:bc:b6:49:37.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.1.2' (RSA) to the list of known hosts.
core@172.16.1.2's password:
Permission denied, please try again.
core@172.16.1.2's password:
Permission denied, please try again.
core@172.16.1.2's password:
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
```

Tarefa 3

2. Após a alteração das regras da firewall obtivemos a seguinte iptable. Podemos observar que agora podemos aceitar tráfego http e ftp vindos de fora e rejeitamos pedidos de echo, ou seja, pedidos de ping.

```
[jpvs@jpvs ~]$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
    0      0 ACCEPT    all  --  any    any     anywhere  anywhere
    0      0 REJECT    icmp --  any    any     anywhere  anywhere
state RELATED,ESTABLISHED
reject-with icmp-host-prohibited
st-prohibited
    0      0 ACCEPT    icmp --  any    any     anywhere  anywhere
    0      0 ACCEPT    all  --  lo     any     anywhere  anywhere
    0      0 ACCEPT    tcp  --  any    any     anywhere  anywhere
    0      0 ACCEPT    tcp  --  any    any     anywhere  anywhere
    0      0 ACCEPT    tcp  --  any    any     anywhere  anywhere
    0      0 REJECT    all  --  any    any     anywhere  anywhere
state NEW tcp dpt:ssh
state NEW tcp dpt:http
state NEW tcp dpt:ftp
reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
    0      0 REJECT    all  --  any    any     anywhere  anywhere
reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
```

3. Uma vez que os pedidos de ping são rejeitados podemos dizer que o resultado obtido foi dentro do esperado.

```
core@XubunCORE:~$ ping 172.16.1.2
PING 172.16.1.2 (172.16.1.2) 56(84) bytes of data.
From 172.16.1.2 icmp_seq=1 Destination Host Prohibited
From 172.16.1.2 icmp_seq=2 Destination Host Prohibited
From 172.16.1.2 icmp_seq=3 Destination Host Prohibited
From 172.16.1.2 icmp_seq=4 Destination Host Prohibited
From 172.16.1.2 icmp_seq=5 Destination Host Prohibited
^C
--- 172.16.1.2 ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 3997ms
```

4. Como visto na tarefa 2 com o comando w3m não conseguimos observar nenhuma página, pelo que agora obtivemos a seguinte página:

Apache 2 Test Page
powered by CentOS

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the images below on Apache and CentOS Linux powered HTTP servers. Thanks for using Apache and CentOS!

[Powered by Apache] [Powered by CentOS Linux]

About CentOS:

The Community ENTERprise Operating System (CentOS) Linux is a community-supported enterprise distribution derived from sources freely provided to the public by Red Hat. As such, CentOS Linux aims to be functionally compatible with Red Hat Enterprise Linux.

<< ↑ ↓ Viewing <Apache HTTP Server Test Page powered by CentOS>

5. Com o user anonymous foi possível entrar em comunicação ftp

```
core@XubunCORE:~$ ftp 172.16.1.2
Connected to 172.16.1.2.
220 (vsFTPd 2.2.2)
Name (172.16.1.2:core): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 0          0              4096 Mar 22  2017 pub
226 Directory send OK.
```

6. Podemos observar que os serviços de ftp e http estão ativos. Uma vez com o ftp o nível de segurança diminuiu, pois qualquer IP consegue enviar pedidos FTP sem autenticação.


```

core@XubunCORE:~$ sudo nmap -sS 172.16.1.2

Starting Nmap 5.21 ( http://nmap.org ) at 2017-12-23 16:11 WET
Nmap scan report for 172.16.1.2
Host is up (0.00029s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:90:7C:D6 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 5.00 seconds

```

7. Podemos observar que o número de pacotes que chegaram ao servidor aumentou. Conforme os pedidos realizados ao longo desta tarefa podemos observar que filtrou 54 pedidos de ping e que para o ssh, http e ftp foram chegado pacotes devido às tarefas realizadas.

```

[jpvs@jpvs ~]$ sudo iptables -A INPUT -j LOG
[jpvs@jpvs ~]$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
 25  8200 LOG      all  --  any    any     anywhere  anywhere
3528 2560K ACCEPT   all  --  any    any     anywhere  anywhere
 54  4536 REJECT   icmp --  any    any     anywhere  anywhere
st-prohibited
 0      0 ACCEPT   icmp --  any    any     anywhere  anywhere
 4    218 ACCEPT   all  --  lo     any     anywhere  anywhere
 1     44 ACCEPT   tcp  --  any    any     anywhere  anywhere
 2    104 ACCEPT   tcp  --  any    any     anywhere  anywhere
 6     344 ACCEPT   tcp  --  any    any     anywhere  anywhere
2482 235K REJECT   all  --  any    any     anywhere  anywhere
 0      0 LOG      all  --  any    any     anywhere  anywhere
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
 0      0 REJECT   all  --  any    any     anywhere  anywhere
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination

```

Conclusão

Ativando a função de log do iptables para o input ficamos com a seguinte iptable. O comando utilizado foi iptables -A INPUT -j LOG, porque queremos que seja feito para todas regras de input.

```
[jpvvs@jpvvs ~]$ sudo iptables -A INPUT -j LOG
[jpvvs@jpvvs ~]$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
  25  8200 LOG      all  --  any    any     anywhere  anywhere
 3528 2560K ACCEPT   all  --  any    any     anywhere  anywhere
  54  4536 REJECT   icmp --  any    any     anywhere  anywhere
st-prohibited
  0    0 ACCEPT   icmp --  any    any     anywhere  anywhere
  4   218 ACCEPT   all  --  lo     any     anywhere  anywhere
  1    44 ACCEPT   tcp  --  any    any     anywhere  anywhere
  2   104 ACCEPT   tcp  --  any    any     anywhere  anywhere
  6   344 ACCEPT   tcp  --  any    any     anywhere  anywhere
2482 235K REJECT   all  --  any    any     anywhere  anywhere
  0    0 LOG      all  --  any    any     anywhere  anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
  0    0 REJECT   all  --  any    any     anywhere  anywhere
                                     reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
```