

UNIT 11.COMPUTER NETWORKS

Iptables. Examples

Computer Systems
CFGS DAW

Autor: Vicent Bosch
vicente.bosch@ceedcv.es

2020/2021
Versión:210325.1614

Licencia



original.

Reconocimiento - NoComercial - CompartirIgual (by-nc-sa): No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra

Nomenclatura

A lo largo de este tema se utilizarán distintos símbolos para distinguir elementos importantes dentro del contenido. Estos símbolos son:

🔔 Actividad opcional. Normalmente hace referencia a un contenido que se ha comentado en la documentación por encima o que no se ha hecho, pero es interesante que le alumno investigue y practique. Son tipos de actividades que no entran para examen

👁️ Atención. Hace referencia a un tipo de actividad donde los alumnos suelen cometer equivocaciones.

UD11. COMPUTER NETWORKS

Iptables. Examples

1.1 Example 1

```
profesor@profesor-VirtualBox: ~  
Archivo Acciones Editar Vista Ayuda  
profesor@profesor-VirtualBox: ~  
profesor@profesor-virtualbox:~$ ssh profesor@192.168.1.50  
ssh: connect to host 192.168.1.50 port 22: Connection timed out  
profesor@profesor-virtualbox:~$ ssh profesor@192.168.1.50  
profesor@192.168.1.50's password:  
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.8.0-45-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
29 actualizaciones se pueden instalar inmediatamente.  
0 de estas actualizaciones son una actualización de seguridad.  
Para ver estas actualizaciones adicionales ejecute: apt list --upgradable  
  
Your Hardware Enablement Stack (HWE) is supported until April 2021.  
Last login: Mon Mar 22 17:53:46 2021 from 192.168.1.48  
profesor@profesor-VirtualBox:~$  
profesor@profesor-VirtualBox:~$ sudo iptables -P INPUT DROP  
profesor@profesor-VirtualBox:~$ sudo iptables -L  
Chain INPUT (policy DROP)  
target     prot opt source                destination  
  
Chain FORWARD (policy ACCEPT)  
target     prot opt source                destination  
  
Chain OUTPUT (policy ACCEPT)  
target     prot opt source                destination  
profesor@profesor-VirtualBox:~$ sudo iptables -P INPUT ACCEPT  
profesor@profesor-VirtualBox:~$
```

1. Server (right) (in red): the incoming connections are blocked.
2. Client (left) (in red) tries to connect using ssh, and it gets a timeout.
3. Server (right) (in blue) the incoming connections are allowed.
4. Client (left) (in blue) can connect using ssh.

1.2 Example 2

The image shows two terminal windows from an Oracle VM VirtualBox. The left window is titled 'profesor@profesor-VirtualBox: ~' and shows the configuration of iptables. The right window is titled 'profesor@profesor-VirtualBox: ~' and shows an SSH connection from a client.

Left Terminal (Server Configuration):

```
profesor@profesor-VirtualBox:~$ sudo iptables -P INPUT DROP
[sudo] contraseña para profesor:
profesor@profesor-VirtualBox:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
profesor@profesor-VirtualBox:~$ sudo iptables -nvl
iptables v1.8.4 (legacy)
profesor@profesor-VirtualBox:~$ sudo iptables -nvl
Chain INPUT (policy DROP 7 packets, 663 bytes)
pkts bytes target      prot opt in      out     source
0      0 ACCEPT     tcp  --  *      *       0.0.0.0/0
tcp dpt:22

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

Chain OUTPUT (policy ACCEPT 4 packets, 307 bytes)
pkts bytes target      prot opt in      out     source

profesor@profesor-VirtualBox:~$ who
profesor :0                2021-03-22 09:59 (:0)
profesor pts/2            2021-03-22 18:51 (192.168.1.48)
profesor@profesor-VirtualBox:~$
```

Right Terminal (Client Connection):

```
profesor@profesor-VirtualBox:~$ ssh profesor@ssh-server
profesor@ssh-server's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.8.0-45-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

29 actualizaciones se pueden instalar inmediatamente.
0 de estas actualizaciones son una actualización de seguridad.
Para ver estas actualizaciones adicionales ejecute: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Mar 22 18:26:35 2021 from 192.168.1.48
profesor@profesor-VirtualBox:~$
```

1. Server (left) (in red): the incoming policy is changed to DROP.
2. Server (left) (in blue): add a new rule to accept incoming connections to port 22 (ssh) using protocol (tcp)
3. Server (left) (in blue): check the new network security configuration.
4. Client (left) (in blue) can connect using ssh.
5. The command who shows the users connected: remote client (192.168.1.48).

1.3 Example 3

- Blocking http and https protocols so that the user cannot access websites.

```
sudo iptables -A OUTPUT -p tcp --dport 80 -j DROP
sudo iptables -A OUTPUT -p tcp --dport 443 -j DROP
```

- Using **wget** command (like using a web browser) to connect. *Had to CTRL+C to stop after a couple of minutes.*

```
profesor@profesor-VirtualBox:~$ wget http://www.google.es
--2021-03-23 11:23:16-- http://www.google.es/
Resolviendo www.google.es (www.google.es)... 142.250.200.131, 2a00:1450:4003:800::2003
Conectando con www.google.es (www.google.es)[142.250.200.131]:80... ^C
profesor@profesor-VirtualBox:~$ wget https://www.google.es
--2021-03-23 11:24:32-- https://www.google.es/
Resolviendo www.google.es (www.google.es)... 142.250.200.131, 2a00:1450:4003:800::2003
Conectando con www.google.es (www.google.es)[142.250.200.131]:443... ^C
```

- Deleting rule that blocks outgoing connections to port 443 (https). First, you must get the rule number and the delete it.

```
profesor@profesor-VirtualBox:~$ sudo iptables -L OUTPUT --line-numbers
Chain OUTPUT (policy ACCEPT)
num target      prot opt source                destination            tcp dpt:http
1  DROP          tcp  --  anywhere              anywhere               tcp dpt:https
2  DROP          tcp  --  anywhere              anywhere               tcp dpt:https
profesor@profesor-VirtualBox:~$ sudo iptables -D OUTPUT 2
profesor@profesor-VirtualBox:~$ wget https://www.google.es
--2021-03-23 11:29:28-- https://www.google.es/
Resolviendo www.google.es (www.google.es)... 142.250.200.131, 2a00:1450:4003:808::2003
Conectando con www.google.es (www.google.es)[142.250.200.131]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: no especificado [text/html]
Guardando como: "index.html"

index.html          [ <=> ] 13,54K --.-KB/s en 0s

2021-03-23 11:29:28 (55,2 MB/s) - "index.html" guardado [13861]
```

1.4 Example 4

- Deleting all rules and verifying.

```
profesor@profesor-VirtualBox:~$ sudo iptables -F
[sudo] contraseña para profesor:
profesor@profesor-VirtualBox:~$ sudo iptables -nvL
Chain INPUT (policy ACCEPT 4 packets, 128 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 2 packets, 64 bytes)
 pkts bytes target    prot opt in     out     source destination
```

1.5 Activities

- How would you block a ping connection to your computer?
- First, add a rule to drop all incoming connections to the port 22. Then, add another rule that accepts all incoming connections from an IP to that port (22).