



ICC0008-UF4-PR01

Ana Cascante

Practica entregable (Enunciado y entregable)

Guía para el alumno

El alumno debe de entregar la práctica enunciada en este documento antes del cierre programado en el calendario. La nota y corrección de la práctica se publicará en la plataforma en un plazo no superior a 10 días hábiles a contar desde la fecha límite de entrega.

Los entregables son:

- Este mismo documento incluyendo las respuestas solicitadas, los dibujos y las capturas de pantallas indicadas en el mismo:
 - **[CSnn]**: son capturas de pantalla que demuestran el resultado de una práctica. Para realizar la captura se utilizará la tecla "imp pant" o equivalente del teclado, y luego al final de documento y dentro de la página en blanco habilitada para cada captura, se realiza el "pegado" o "paste". Si fuera necesario se ajustará el tamaño.
 - **[DIBnn]**: Son esquemas que se solicitan en el enunciado de la práctica y pueden ser realizadas con cualquier herramienta dependiendo del tipo de dibujo, incluso escanear la imagen de un dibujo hecho a mano. También pueden ser completar tablas, escribir texto.

Utilizar los espacios habilitados al final de este documento para la inserción de las capturas y dibujos.

El documento entregado tendrá el siguiente nombre:

ICC0008-UF4-PR01-"username".pdf "username" = nombre de usuario del alumno en la plataforma Ejemplo: ICC0008-UF4-PR01-raulgarciaflores.pdf

[DIB00]: 1 punto reservado para pulcritud y correcta redacción de las explicaciones.

Puntuación: 1

Ejercicio #1 Iptables

Aplica filtros Iptables en tu servidor para que sólo puedan acceder al servicio web los clientes de cualquier IP. HTTP y HTTPS.

Aplica también un filtro para que sólo puedan acceder al puerto 8080 clientes de la red 192.168.1.0/24.

El servidor no responde PINGs.

¿Dónde has ubicado las Iptables (INPUT;OUTPUT;FORWARD)? ¿Cómo han quedado las políticas por defecto?

[DIB01...x]: Capturas y explicaciones del proceso

Listamos todas las iptables

```
root@anaserver:/home/anaserver# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
DOCKER-USER all -- anywhere              anywhere
DOCKER-ISOLATION-STAGE-1 all -- anywhere            anywhere
ACCEPT     all -- anywhere            anywhere            ctstate RELATED,ESTABLISHED
DOCKER     all -- anywhere            anywhere
ACCEPT     all -- anywhere            anywhere
ACCEPT     all -- anywhere            anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain DOCKER (1 references)
target     prot opt source                destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
target     prot opt source                destination
DOCKER-ISOLATION-STAGE-2 all -- anywhere            anywhere
RETURN     all -- anywhere            anywhere

Chain DOCKER-ISOLATION-STAGE-2 (1 references)
target     prot opt source                destination
DROP       all -- anywhere            anywhere
RETURN     all -- anywhere            anywhere

Chain DOCKER-USER (1 references)
target     prot opt source                destination
RETURN     all -- anywhere            anywhere
root@anaserver:/home/anaserver#
```

Borramos reglas de las las iptables por defecto

```

root@anaserver:/home/anaserver# iptables -F
root@anaserver:/home/anaserver# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain DOCKER (0 references)
target     prot opt source                destination

Chain DOCKER-ISOLATION-STAGE-1 (0 references)
target     prot opt source                destination

Chain DOCKER-ISOLATION-STAGE-2 (0 references)
target     prot opt source                destination

Chain DOCKER-USER (0 references)
target     prot opt source                destination
root@anaserver:/home/anaserver#

```

Ahora vuelvo a borrar las políticas con iptables -F, y limito las inputs al puerto 80 y 443 y acepto los outputs de otros puertos

```

root@anaserver:/home/anaserver# iptables -F
root@anaserver:/home/anaserver# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@anaserver:/home/anaserver# iptables -A INPUT -p tcp --dport 443 -j ACCEPT
root@anaserver:/home/anaserver# iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination
ACCEPT     tcp  --  anywhere              anywhere            tcp dpt:http
ACCEPT     tcp  --  anywhere              anywhere            tcp dpt:https

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain DOCKER (0 references)
target     prot opt source                destination

Chain DOCKER-ISOLATION-STAGE-1 (0 references)
target     prot opt source                destination

Chain DOCKER-ISOLATION-STAGE-2 (0 references)
target     prot opt source                destination

Chain DOCKER-USER (0 references)
target     prot opt source                destination
root@anaserver:/home/anaserver# _

```

Ahora, no nos conecta ni con ping ni con apache, como indica 100% de packet loss

```
anacr@anacr-VirtualBox: ~  
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.  
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.953 ms  
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.12 ms  
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1.62 ms  
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.903 ms  
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.976 ms  
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=0.901 ms  
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=0.964 ms  
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=0.916 ms  
^C  
--- 192.168.1.1 ping statistics ---  
8 packets transmitted, 8 received, 0% packet loss, time 7054ms  
rtt min/avg/max/mdev = 0.901/1.044/1.624/0.228 ms  
anacr@anacr-VirtualBox:~$ ^C  
anacr@anacr-VirtualBox:~$ ping 192.168.1.1  
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.  
^C  
--- 192.168.1.1 ping statistics ---  
16 packets transmitted, 0 received, 100% packet loss, time 17462ms  
anacr@anacr-VirtualBox:~$
```

Para limitar la ip a 192.168.1.0/24 he aplicado el siguiente comando

```
root@anaserver:/home/anaserver# iptables -A INPUT -p tcp --dport 8080 -m iprange --src-range 192.168.1.0-192.168.1.255 -j ACCEPT  
root@anaserver:/home/anaserver#
```

Y la web en la maquina servidor del puerto 8080 ya funciona



Mis políticas de la chain input han quedado de la siguiente forma

```

root@anaserver:/home/anaserver# iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination          tcp dpt:http
ACCEPT     tcp  --  anywhere              anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere              anywhere             tcp dpt:http-alt source IP range 192.1
68.1.0-192.168.1.255

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain DOCKER (0 references)
target     prot opt source                destination

Chain DOCKER-ISOLATION-STAGE-1 (0 references)
target     prot opt source                destination

Chain DOCKER-ISOLATION-STAGE-2 (0 references)
target     prot opt source                destination

Chain DOCKER-USER (0 references)
target     prot opt source                destination
root@anaserver:/home/anaserver# _

```

Puntuación: 7

Ejercicio #1 - Tarea #1

Las iptables no son persistentes. Es decir, cuando se apaga el servidor éstas se borran. Busca la forma de hacer que sean persistentes. Documenta el proceso.

[DIB02..y]: Capturas y explicaciones del proceso

He puesto el comando `iptables -P INPUT ACCEPT` , para abrir los puertos y poder instalar las iptables persistentes con el comando

```

root@anaserver:/home/anaserver# apt install -y iptables-persistent_

```

Para guardarlos, ejecuto el siguiente comando

```

root@anaserver:/home/anaserver# iptables-save > /etc/iptables/rules.v4_

```

Y las observo con un `cat`

```

root@anaserver:/home/anaserver# cat /etc/iptables/rules.v4
# Generated by iptables-save v1.8.7 on Fri Apr 26 16:00:17 2024
*filter
:INPUT ACCEPT [90:300344]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [126:11433]
:DOCKER - [0:0]
:DOCKER-ISOLATION-STAGE-1 - [0:0]
:DOCKER-ISOLATION-STAGE-2 - [0:0]
:DOCKER-USER - [0:0]
- A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
- A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
- A INPUT -p tcp -m tcp --dport 8080 -m iprange --src-range 192.168.1.0-192.168.1.255 -j ACCEPT
COMMIT
# Completed on Fri Apr 26 16:00:17 2024
# Generated by iptables-save v1.8.7 on Fri Apr 26 16:00:17 2024
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:DOCKER - [0:0]
- A PREROUTING -m addrtype --dst-type LOCAL -j DOCKER
- A OUTPUT ! -d 127.0.0.0/8 -m addrtype --dst-type LOCAL -j DOCKER
- A POSTROUTING -s 172.17.0.0/16 ! -o docker0 -j MASQUERADE
- A DOCKER -i docker0 -j RETURN
COMMIT
# Completed on Fri Apr 26 16:00:17 2024
root@anaserver:/home/anaserver#

```

Y cuando realizo un reboot, y hago un iptables -L

```

[sudo] password for anaserver:
Chain INPUT (policy ACCEPT)
target     prot opt source                destination          tcp dpt:http
ACCEPT     tcp  --  anywhere              anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere              anywhere             tcp dpt:http-alt source IP range 192.1
68.1.0-192.168.1.255

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination          anywhere
DOCKER-USER all  --  anywhere              anywhere             ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere              anywhere
DOCKER     all  --  anywhere              anywhere
ACCEPT     all  --  anywhere              anywhere
ACCEPT     all  --  anywhere              anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain DOCKER (1 references)
target     prot opt source                destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
target     prot opt source                destination          anywhere
DOCKER-ISOLATION-STAGE-2 all  --  anywhere              anywhere
RETURN     all  --  anywhere              anywhere

Chain DOCKER-ISOLATION-STAGE-2 (1 references)
target     prot opt source                destination
DROP      all  --  anywhere              anywhere
RETURN     all  --  anywhere              anywhere

Chain DOCKER-USER (1 references)
target     prot opt source                destination
RETURN     all  --  anywhere              anywhere
anaserver@anaserver:~$ _

```

Puntuación: 3