

03 Laboratorio de Firewalls

CC50P, Taller de Redes de Datos

Profesor: Sebastián Castro A.

Introducción

Una herramienta clave dentro de la definición de una política de seguridad es el firewall, que permite autorizar o restringir ciertos servicios de red basados en reglas de filtraje. Con ello se define los accesos autorizados, estableciendo una base para la seguridad.

Existen diversas herramientas para obtener lo mismo, pero todas se basan en los mismos fundamentos: analizar los datagramas IP circulantes y tomar la decisión de permitir su tránsito o rechazarlos en base a la inspección de reglas.

Para ejercitar la definición de éstos elementos, vamos a utilizar la implementación de firewall de Linux, basada en una herramienta llamada IPTables. Ésta combina una verificación de reglas que residen en el kernel del S.O. más un conjunto de herramientas para manipular las reglas que opera a nivel de usuario.

Herramientas a utilizar

Linux

Comandos Necesarios

- **ifconfig:** permite configurar y chequear el estado de las interfaces de red, en particular la interfaz eth0 es normalmente la interfaz real de red existente, algunos ejemplos:
 - **ifconfig -a**, despliega el estado y configuración de todas las interfaces existentes para el sistema.
 - **ifconfig eth0 inet 192.168.88.3 netmask 255.255.255.240 broadcast 192.168.88.15 mtu 1496 up**, configura la interfaz eth0 con el número ip 192.168.88.3, define la mtu en 1496 y activa la interfaz si esta estuviera desactivada.
- **vconfig:** permite configurar y chequear el estado de las vlan agregadas al sistema, una vez que se agrega una vlan al sistema esta aparece como interfaz de red. Los comandos típicos son:
 - **vconfig add eth0 37**, agrega la interfaz “eth0” a la vlan con TAG 37, creando la interfaz virtual “eth0.37”. Dicha interfaz queda “administrativamente desactivada” al momento de definirla.
- **tcpdump:** permite mirar los paquetes que llegan o salen por la interfaz de red seleccionada, por ejemplo: **tcpdump -qn -i eth0**.
- **modprobe:** permite agregar en forma dinámica módulos al sistema operativo mediante lo cual este adquiere nuevas funcionalidades, por ejemplo: “**modprobe 8021q**”, agrega la capacidad al sistema de manejar vlan.

- Iptables: permite agregar/modificar/eliminar reglas del kernel. Cada comando tiene la estructura `iptables -t tabla cadena comando definici3n_regla -j objetivo`.

Donde los valores posibles son:

Tabla	Cadena	Objetivo
Filter	INPUT, OUTPUT, FORWARD	ACCEPT, REJECT, DROP
Mangle	INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING	TTL, TOS, MARK
NAT	PREROUTING, POSTROUTING, FORWARD	DNAT, SNAT, MASQUERADE

Comandos 3tiles para IPTables son:

- `iptables -t tabla -F`: borra todas las reglas asociadas a una tabla.
- `Iptables -t tabla -L -n`: lista todas las reglas de una tabla. La opci3n “-n” evita que se resuelva v3a DNS los elementos de cada regla.
- `Iptables -t tabla -A cadena definici3n_regla -j objetivo`: agrega una regla a la cadena de la tabla especificada. Si un datagrama coincide con la regla, se realiza “objetivo”.
- `Iptables -t tabla -D cadena n3mero`: borra la regla n3mero “n3mero” de la *cadena* de la *tabla* especificada.

Switch Cisco Catalyst 2950XL

Este switch tiene implementado en hardware la capacidad de direccionar los paquetes entre las distintas interfaces. Adem3s de esto permite el manejo del protocolo 8021q en cada interfaz.

A este se accede mediante un cable serial que sirve como consola o mediante telnet/ssh, una vez dentro del switch presionando el tabulador sale la lista de opciones v3lidas.

Comandos 3tiles

Creando una VLAN

```
switch> enable
switch# vlan database
switch(vlan)# vlan <vlan-id> name <vlan-name>
switch(vlan)# end
switch#
```

Configurando una puerta como miembro de una VLAN

```
switch> enable
switch# configure terminal
switch(config)# interface <interface-id>
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan <vlan-id>
switch(config-if)# end
switch(config)# end
switch#
```

Configurando una puerta como troncal para una VLAN

```
switch> enable
switch# configure terminal
switch(config)# interface <interface-id>
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk encapsulation dot1q
switch(config-if)# end
switch(config)# end
```

Agregando más VLAN a una puerta troncal

```
switch> enable
switch# configure terminal
switch(config)# interface <interface-id>
switch(config-if)# switchport trunk allowed vlan add <vlan-id>,<vlan-id>
switch(config-if)# end
switch(config)# end
switch#
```

Infraestructura de trabajo

Para realizar las diferentes experiencias de este laboratorio, contaremos con un switch “Cisco Catalyst 2950”, 20 computadores tipo PC corriendo Linux Knoppix, 1 notebook con Linux, conectado al switch mediante un cable serial (para tener acceso a la consola de administración).

Cada alumno estará a cargo de dos computadores, uno de los cuales configurará con 2 interfaces tipo “vlan” y el otro operará como un computador “normal”. El computador con interfaces VLAN será llamado **externo** y el otro será **interno** con el fin de diferenciarlos para las experiencias.

Experiencia 1

Objetivo: Instalar el software para administración de VLAN en una de las máquinas.

Datos:

- Red 192.168.0.0/25 (máscara 255.255.255.128)
- Dirección 192.168.0.126 será la dirección IP del servidor del profesor.

Procedimiento

1. Configure la interfaz eth0 de su computador, utilizando una dirección del rango especificado. Para evitar conflictos, utilice su número de grupo como último número de la dirección IP.
2. Verifique conectividad con el profesor, ejecutando “ping 192.168.0.126”
3. Descargue el archivo con las herramientas para VLAN en Linux, mediante wget. El archivo está en el computador del profesor, en la URL <http://192.168.0.126/vlan.1.8.tar.gz>. Guarde el archivo en el directorio “/ramdisk”.
4. Descomprima el contenido del archivo usando `tar xvfz vlan.1.8.tar.gz`, entre la directorio recién creado y ejecute “make”.

Experiencia 2

Datos

- VLAN 4 para todos los **externos**.
- VLAN 1X para el **interno** y el **externo**.
- Redes entre **externos**: 172.16.10.0/24 (utilice el número .X0 para su computador).
- Redes entre **interno** y **externo**: 10.0.X.0/25 (utilice .1 para **externo** y .2 para **interno**).

Instrucciones

1. Configure las puertas que esté usando de modo que la puerta conectada a su **externo** sea troncal y que transporte las VLAN 4 y 1X. Configure la puerta conectada a su **interno** de modo que sea “untag” perteneciente a la VLAN 1X.
2. Cree una interfaz en la VLAN 4 en **externo** y asígnele la dirección que corresponda.
3. Cree una interfaz en la VLAN 1X en **externo** y asígnele la dirección que corresponda.
4. Asígnele dirección a su **interno** en la red que corresponda.
5. Verifique conectividad usando ping entre su **interno** y **externo**, y entre su **externo** y otros **externos**.

Experiencia 3 (Configuración de SNAT)

Instrucciones

1. Primera parte
 - a. Habilite el IP forwarding en su externo, usando `sysctl -w net.ipv4.ip_forward=1`.
 - b. Ejecute ping desde su máquina **interna** a cualquier máquina **externa**.
 - c. Verifique que el tráfico se está generando correctamente usando `tcpdump` en ambas interfaces VLAN (eth0.4 y eth0.1x).
 - d. Comunique sus conclusiones al profesor.
2. Segunda parte
 - a. Habilite el SNAT, con el comando “`iptables -t nat -A POSTROUTING -s 10.0.X.0/24 -d 172.16.10.0/24 -j SNAT --to-source 172.16.10.X1`”. La dirección “172.16.10.X1” no debiere existir y la instrucción es deliberada.
 - b. Ejecute ping como en la primera parte y verifique el tráfico utilizando `tcpdump`.
 - c. Comunique sus conclusiones al profesor.
3. Tercera parte
 - a. Elimine la regla anotada anteriormente.
 - b. Habilite el SNAT, con el comando “`iptables -t nat -A POSTROUTING -s 10.0.X.0/24 -d 172.16.10.0/24 -j SNAT --to-source 172.16.10.X0`”.
 - c. Ejecute ping como en la primera parte y verifique el tráfico utilizando `tcpdump`.
 - d. Comunique sus conclusiones al profesor.

Experiencia 4 (Configuración de DNAT)

Instrucciones

1. Habilite en la máquina **interna** algún servicio TCP como SSH, http, etc.
2. Habilite el DNAT en la máquina externa, de modo que el servicio habilitado en la máquina interna sea visto desde el “exterior”. Para ello, utilice el comando `“iptables -t nat -A PREROUTING -d 172.16.10.X0 -p tcp -dport 8080 -j DNAT --to-destination 10.0.X.2:YY”`, donde YY es el puerto donde opera el servicio habilitado (22 para SSH, 80 para http, etc).
3. Para verificar el correcto funcionamiento, pida al profesor que pruebe el servicio recién habilitado. Podrá monitorear su correcta operación usando tcpdump en ambas interfaces de red.

Experiencia 5 (Configuración de limit)

Instrucciones

1. Restrinja la tasa de entrada de ICMP a 2 por segundo, originada en su máquina interna. Para ello, utilice los siguientes comandos: `“iptables -A INPUT -p icmp -m limit -limit 2/s -j ACCEPT”` y `“iptables -A INPUT -p icmp -j DROP”`.
2. Verifique el correcto funcionamiento de la regla usando ping desde su máquina interna. Para ello, abra tres ventanas y ejecute el comando `“ping -i 1 10.0.X.1”`. Dos de las tres máquinas deberían recibir respuesta.
3. Sin cortar el ping, elimine las reglas definidas en el punto 1, usando `“iptables -F”`.
4. Restrinja la tasa de entrada de ICMP a 2 por segundo, originada en su máquina interna. Para ello, utilice los siguientes comandos: `“iptables -A INPUT -p icmp -m limit -limit 2/s -j ACCEPT”` y `“iptables -A INPUT -p icmp -j REJECT”`.
5. Comente las diferencias de comportamiento entre reglas con el profesor. Para mayor información, puede utilizar tcpdump.

Experiencia 6 (Restricción de entrada/salida)

Instrucciones

1. Bloquee la salida de http hacia el computador del profesor (172.16.10.126), utilizando `“iptables -A OUTPUT -d 172.16.10.126 --dport 80 -j DROP”`. Verifique utilizando telnet.
2. Cambie la definición anterior (eliminándola e insertando una nueva), utilizando el comando `“iptables -A OUTPUT -d 172.16.10.126 --dport 80 -j REJECT”`. Verifique utilizando telnet.
3. Bloquee la entrada al servicio habilitado en la experiencia 4, desde el computador del profesor. Para ello, ejecute `“iptables -A INPUT -s 172.16.10.126 -dport 8080 -j DROP”`. Pida al profesor que verifique la correcta operación de la regla.