Gestión e Implantación
de Redes de Computadores

Práctica 4

Cortafuegos (Firewalls) - iptables

Objetivo

Cuando se conecta un sistema a una red, una de las tareas que debe realizar el administrador del sistema es garantizar un mínimo de seguridad en su sistema. Una de las tareas que en esta práctica se pretende desarrollar, es que el alumno implemente filtros de paquetes para controlar el tráfico.

Conocimientos previos

Conectar un sistema a una red supone exponerlo al peligro de ser atacado por los distintos sistemas que cohabitan con el nuestro y por todos aquellos que pueden alcanzar dicha red. Es por ello que un administrador de un sistema debe, como una de sus principales tareas, diseñar, implementar y configurar una política de seguridad que le dé unos niveles de fiabilidad aceptables.

Los mecanismos mínimos que todo administrador debe introducir en su sistema son los llamados preventivos y que, básicamente, consistirán en configurar adecuadamente tanto el núcleo y el sistema operativo que ejecuta nuestro equipo como los servicios y programas que están ejecutándose en él.

Otra característica que todo administrador debe introducir, y que es en la que nos centraremos en esta práctica, es la de filtrar los paquetes que llegan y salen de nuestro sistema. Para ello, en las versiones de los núcleos de Linux, se dispone de la utilidad **iptables** que nos permite configurar reglas de filtrado de paquetes.

El filtrado de IP es simplemente un mecanismo que decide qué tipos de datagramas IP serán procesados normalmente y cuáles serán descartados. Se pueden aplicar muchos

criterios y en diferentes ordenamientos para determinar qué datagramas se desean filtrar; como por ejemplo:

Tipo de protocolo: TCP, UDP, ICMP, etc.

Tipo de datagrama: SYN/ACK, datos, petición de eco de ICMP, etc.

Dirección de origen del datagrama: de dónde proviene

Dirección de destino del datagrama: a dónde se dirige

El filtrado IP es una utilidad en la capa de red. Esto significa que este mecanismo no entiende nada acerca de la aplicación que utiliza las conexiones de red, sólo sabe acerca de las conexiones mismas. Por ejemplo, se puede denegar el acceso a usuarios a la red interna por el puerto predeterminado de telnet, pero si se apoya únicamente en el filtrado de IP, no se podrá evitar que se utilice el programa de telnet en un puerto por el que sí se permite el paso a través del cortafuegos implementado. El conjunto de reglas de filtrado de IP se construye a partir de combinaciones de los criterios enumerados anteriormente.

Sintaxis

La sintaxis se ha analizado en clase de teoría mostrando varios ejemplos relacionados con las tablas y cadenas más comunes.

iptables [–t tabla] –A cadena opciones –j objetivo

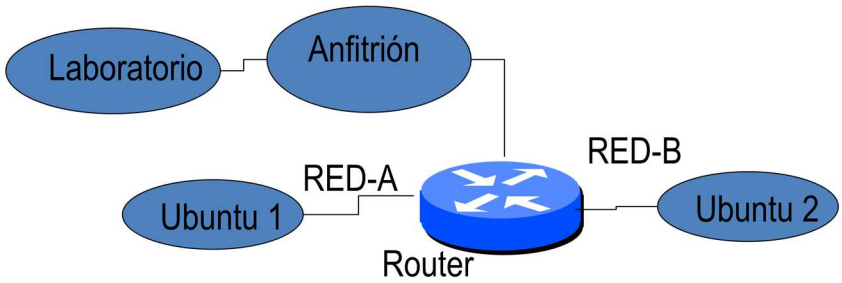
Ejemplo

Vamos a suponer que queremos denegar todo el tráfico de reenvío (si nuestro equipo no es un router, no debería tener permitido esta opción) y que sólo va a admitir que se use el servicio ssh desde la dirección 192.168.10.130, el resto estará denegado. La dirección local será 192.168.10.129. Además, mostraremos todos los paquetes TCP rechazados.

```
# iptables -F
# iptables -P FORWARD DROP
# iptables -P INPUT DROP
# iptables -P OUTPUT DROP
# iptables -A INPUT  -p tcp  -s 192.168.10.130  --dport 22  –j ACCEPT
# iptables -A OUTPUT  -p tcp  --sport 22  -d 192.168.10.130  –j ACCEPT
#iptables -A INPUT -p tcp -j LOG
#iptables -A OUTPUT -p tcp -j LOG
#iptables –A FORWARD -p tcp -j LOG
```

Enunciado

- Iniciar y configurar con el entorno gráfico de virtualización VirtualBox las máquinas Ubuntu1, Ubuntu2 y Router según esquema de red descrito en prácticas anteriores.



- Para configurar en el equipo Router un firewall que controle el flujo de paquetes que entra, sale y atraviesa nuestro sistema de acuerdo a una política preasignada. Daremos solución a los siguientes requerimientos o restricciones:

1. Borrar cualquier regla existente en las tablas nat y filter.

2. Establecer como política por defecto DROP en las reglas de la tabla filter.

3. Permitir realizar consultas DNS sólo a los equipos de la red A. Suponer que el servidor DNS es el configurado en la práctica anterior y que se encuentra corriendo en Router.

4. Permitir acceso desde Router al puerto 53 TCP y UDP del servidor DNS externo. Considerar que las consultas DNS que se realizan a dicho servidor son hechas por nuestro servidor DNS (corriendo en Router) para resolver las direcciones que él no es capaz de resolver.

5. Permitir las peticiones HTTP provenientes de los equipos tanto de la red A como de la red B que vayan dirigidas a cualquier equipo del exterior.

6. Permitir la comunicación desde el Router y desde el nodo de la red b con un servidor Web escuchando en el Nodo A (Ubuntu 1). Permitir la comunicación también desde el nodo anfitrión.

7. El administrador de nuestra red estará en un nodo de la red A. Permitir la conexión desde su IP a cualquier puerto administrativo del Router y denegar la conexión a puertos administrativos en cualquier otro caso.

8. Permitir el acceso mediante “ping” desde las redes A y B al router y viceversa.

9. Permitir el acceso mediante “ping” desde la red A a la red B y denegar el acceso en sentido contrario.

10. Registrar en el log del sistema cualquier tráfico que contenga la cadena ‘/etc/passwd’ indicando como prefijo de salida la cadena ‘***** GIRC 2018: GET /ETC/PASSWD *****’

11. Guardar los logs del tráfico desechado indicando como prefijo de la salida la cadena ‘***** GIRC 2018: PRACTICA 4 - DESECHADO *****’.

- Comprobar el correcto funcionamiento de la configuración realizada en cada paso.

Para la realización de la práctica se dispone de **4 sesiones** de laboratorio.