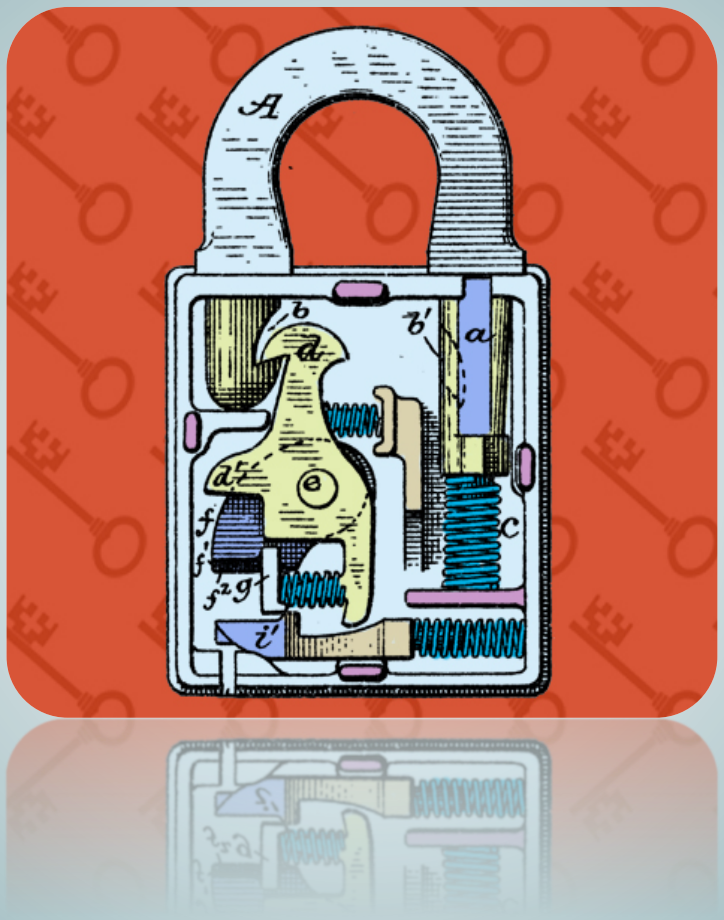
Garantía y Seguridad en Sistemas y Redes

Práctica 9. Prevención de Intrusión



Esteban Stafford

Departamento de Ingeniería
Informática y Electrónica

Práctica 9

Prevención de Intrusión

1. Introducción

Para reducir las posibilidades de ataque o infiltración, las organizaciones suelen recurrir a cortafuegos. Estos dispositivos de red permiten establecer controles de acceso al tráfico, tanto entrante como saliente. En esta práctica se aprende a utilizar el cortafuegos de Linux en el supuesto de una pequeña organización o empresa con un servidor WEB, uno o varios equipos de sobremesa dentro de una red privada, con un único acceso al exterior.

2. Objetivos

El objetivo fundamental que persigue esta práctica es prender a manejar el cortafuegos de Linux `iptables`.

3. Material

En esta práctica se usará exclusivamente el cortafuegos de Linux `iptables`. Existe una gran cantidad de información y ejemplos de uso en Internet.

4. Desarrollo

4.1. Creación de un entorno de trabajo

Para esta práctica necesitamos disponer de varios equipos. En lugar de equipos físicos utilizaremos varias máquinas virtuales dentro de VirtualBox, además de la máquina anfitrión. Esta es la configuración de cada una de las máquinas virtuales.

- Servidor GSSR
  - Es la máquina que hemos usado en otras prácticas. Asegúrate de que no está activado el IDS.
  - El primer interfaz de red está configurado como NAT.
  - El segundo esta conectado a `vboxnet0`.
- Cortafuegos
  - Clon del servidor GSSR, también con el IDS desactivado.
  - Es conveniente cambiar el nombre de la máquina para no confundirla con el servidor.

- El primer interfaz de red debe ponerse en modo *bridge*.
- El segundo esta conectado a `vboxnet0`.

- Equipo de sobremesa
  - Máquina sin disco que arranca con una ditro live. Por ejemplo
    http://cdimage.kali.org/kali-2.0/kali-linux-light-2.0-i386.iso
  - El interfaz de red debe estar conectado a `vboxnet0`.

De esta manera tenemos un cortafuegos que hace de puente entre la red física de nuestra máquina y una red virtual interna, con un equipo servidor y otro de sobremesa.

4.2. Toma de contacto con `iptables`

En este apartado usaremos solo la máquina física y el cortafuegos. Toma nota de las direcciones IP de cada uno y comprueba que se pueden abrir conexiones de la física al cortafuegos. Primero con `ping` y luego con `nmap`. Deberías tener abiertos los puertos de `ssh`, `http` y `https`.

Crea una regla de `iptables` para que el cortafuegos tire todos los paquetes ICMP. Comprueba que ya no se puede hacer `ping` desde la máquina anfitrión. ¿Se puede hacer `ping` desde el cortafuegos? ¿Que regla habría que poner para evitarlo también?

Familiarizate con la manera de eliminar reglas, bien usando el número de regla, o la especificación de la misma. Para terminar limpia todas las cadenas.

4.3. Cortafuegos local

Configura las políticas de cortafuegos para que tiren todos los paquetes. Luego pon reglas para que se permita el acceso a los puertos `http` y `https` desde cualquier IP, y al `ssh` sólo desde la máquina física. Desde el ordenador de un compañero comprueba que no puedes acceder a `ssh` pero sí a `http` y `https`.

Si no lo has hecho ya, configura la política de salida en `DROP`. ¿Que reglas hay que poner para permitir las conexiones anteriores? Es posible que necesites usar el módulo `state` de `iptables`.

4.4. Router NAT y cortafuegos

Ahora vamos a configurar el cortafuegos como bastión de nuestra red `vboxnet0`. Para empezar limpia las cadenas de `tables` y abre las políticas. Este equipo va a tener que procesar paquetes que no están dirigidos a las IPs de sus interfaces. Por ello hay que hablilitar `/proc/sys/net/ipv4/ip_forward`. Se puede hacer directamente con un `echo`, pero para que sea un cambio permanente hay que modificarlo en `/etc/sysctl.conf` y ejecutar `sysctl -p /etc/sysctl.conf`.

Para las pruebas de este apartado, arranca la máquina virtual del equipo de sobremesa. Para que use el router como enlace de salida, hay que configurar este como *gateway*.

Comprueba que se puede hacer `ping` desde el equipo de sobremesa a otro en la red del laboratorio, como por ejemplo el *gateway*, 172.31.16.1. Puedes ver los paquetes que pasan por el router con `ngrep`.

`iptables` tiene una tabla llamada `nat` que sirve para reescribir cabeceras de paquetes. Puedes crear una regla en la cadena `POSTROUTING` con el destino `MASQUERADE` para activar la reescritura.

Cuando hagas `ping` al gateway de la red del laboratorio, observa la diferencia entre los paquetes que entran por el interfaz `eth1` y los que salen por el `eth0`.

Ahora pon la política de la cadena `FORWARD` a `DROP`, y configura `iptables` de manera que permita navegar desde el equipo de sobremesa solo a través de `http`.

4.5. Acceso al servidor GSSR

Con la anterior configuración un equipo externo a la red `vboxnet0` no puede acceder al servidor GSSR. En la tabla `nat` existe una cadena llamada `PREROUTING` en la que saltando a `DNAT` se pueden reescribir paquetes de entrada. Escribe una regla que permita redirigir el tráfico destinado a los puertos `http` y `https` hacia el servidor GSSR.

4.6. Resumen

Para concluir, escribe un script, llamado `/etc/firewall` que configure el firewall de manera que se combinen las reglas necesarias para satisfacer los siguientes requisitos

- El cortafuegos no puede ni enviar ni recibir nada, excepto `ssh`.
- El cortafuegos redirige el tráfico de puerto `http` y `https` entrante a su interface externo al servidor.
- El equipo servidor no puede hacer conexiones hacia el exterior.
- Se puede navegar desde la red interna hacia fuera desde el equipo de sobremesa.

Configura la máquina cortafuegos para que ejecute el script en el arranque. Tras reiniciar la máquina, asegúrate de que se cumplen los requisitos anteriores.