IPTABLES RULES

1.

SINTAXIS DE REGLAS

Creación de reglas

Sintaxis del comando *iptables*:

1. Comando *iptables*
2. Tabla a usar: *filter, nat, mangle*
3. Comando sobre la cadena: *insertar, modificar, eliminar reglas…*
4. Cadena a usar: *input, output, forward, prerouting o postrouting*
5. Condición: criterios que deben cumplir los campos
6. Acción a realizar (para los que cumplan la condición previa)
7. Opciones extra para ajustar la acción

2.

PARÁMETROS

Manejo de reglas

- *L :* Listar las reglas, se puede especificar la cadena

 # iptables –L [CHAIN -v] [--line-numbers]

- *A / -I i:* Agregar una regla [final o posición]

 # iptables –A CHAIN… // -I i CHAIN…

- *F / - D i :* Eliminar reglas [todas o la *i-ésima* de una cadena]

 # iptables –F CHAIN // –D CHAIN i

- *R i :* Reemplazar la regla i-ésima por otra nueva especificada

*# iptables -R CHAIN i _newRule_*

Manejo de cadenas

- *E :* Renombrar una cadena (solo cambia apariencia)

 # iptables –E old-chain new-chain

- *N name :* Crear una nueva cadena

- *X name :* Borrar una cadena (debe estar vacía)

- *R i :* Reemplazar la regla i-ésima por otra nueva especificada

*# iptables –-R CHAIN i _newRule_*

- *Z :* Pone a cero los contadores de todas las reglas de una cadena

- *P :* Cambia la política por defecto sobre una cadena, no match con las reglas, ¿qué hacer con ellos? ACCEPT / DROP

Ejecución de reglas en la cadena

- Reglas compuestas por *condición* y *acción*
- Si se cumple la condición se ejecutará la acción
- Si no se cumple la condición, se pasará a la siguiente regla
- Si no coincide ninguna regla de la cadena se ejecutará la política por defecto (ACCEPT o DROP)
- Importante tener cuidado con el *orden secuencial*
- Acciones con el parámetro *-j [acción]*

3.

OPERADORES

Operadores

- p [protocolo] : Sobre qué protocolo se realiza la comprobación, posibilidades en */etc/protocols*. **Ejemplo**: *-p tcp,udp*

- s [ip/máscara origen] : IP o subred origen del paquete.

Ejemplo: *-s 192.168.1.0/24*

- d [ip/máscara destino] : IP o subred destino del paquete.

Ejemplo: *-d 192.168.1.0/24*

- i / - o [interfaz] : Especifica la interfaz de entrada o salida, solo se puede utilizar en las tablas *nat* o *mangle*. **Ejemplo**: *-i eth0, -o eth1*

Extensiones

Protocolo extiende sus funcionalidades con distintos operadores denominados *extensiones:*

--sport, --dport: Puerto origen o destino para *tcp* o *udp*.

Ejemplos: *-p tcp --sport 0:1024 // -p tcp,udp --dport 80*

--icmp-type: Selecciona los paquetes ICMP y comprueba de qué tipo de mensaje se trata. **Ejemplo**: *-p icmp --icmp-type echo-reply // -p icmp --icmp-type time-exceded*

- Posibilidad de negación con “!”

4.

ACCIONES

Acciones

El parámetro *acción* indica lo que se hará con el paquete si se cumple la condición. Algunas acciones son comunes de todas las cadenas aunque otras son específicas.

ACCEPT: Acepta el paquete.

DROP: Rechaza el paquete.

REJECT: Rechaza el paquete, pero notifica al emisor que el paquete fue descartado.

LOG: Crea una entrada en el fichero de log.

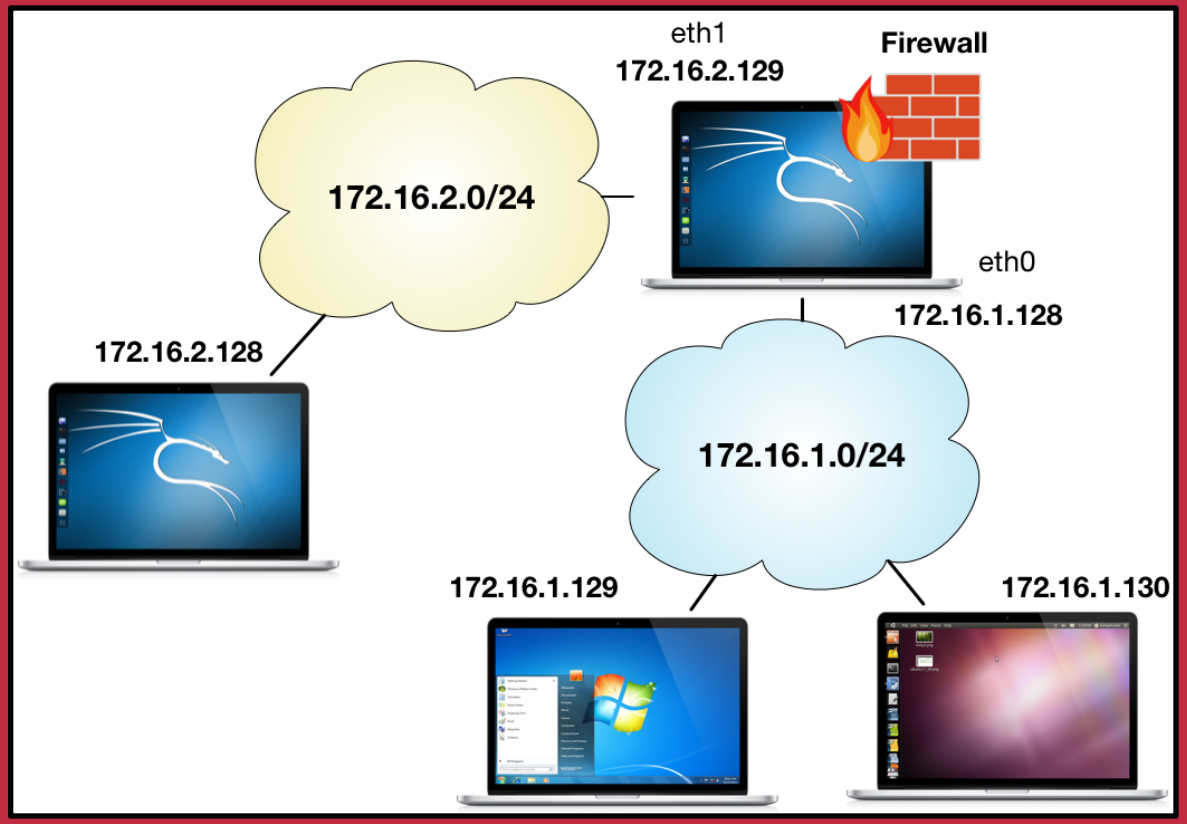
Acciones

MASQUERADE [dirección_ip]: Enmascaramiento de la dirección IP origen de forma dinámica. Solo disponible en la tabla NAT de la cadena POSTROUTING.

DNAT --to [dirección_ip][:puerto]: Enmascaramiento de la dirección destino. Re-enrutado de paquetes.

SNAT--to [dirección_ip][:puerto]: Enmascaramiento de la dirección origen. Similar al *masquerade* pero con IP fija.

- Acciones adicionales: *DENY*, *REDIRECT*, *RETURN* y *MIRROR*.



LABORATORIO