Guía de Estudio: iptables
Introducción a iptables

iptables es una herramienta de filtrado de paquetes para sistemas Linux que permite definir reglas para gestionar el tráfico de red. Puedes utilizar iptables para permitir o bloquear paquetes basados en diversos criterios.

Conceptos Básicos

Tablas de iptables:

1. filter: Tabla predeterminada para filtrado de paquetes.
2. nat: Traducción de direcciones de red.
3. mangle: Modificación de paquetes.
4. raw: Manejo previo al procesamiento de paquetes.

Cadenas:

1. INPUT: Tráfico dirigido al sistema.
2. OUTPUT: Tráfico generado por el sistema.
3. FORWARD: Tráfico que pasa a través del sistema.
4. PREROUTING: Modificación previa al enrutamiento.
5. POSTROUTING: Modificación posterior al enrutamiento.

Acciones: ACCEPT, DROP, REJECT, entre otras.

Comandos Básicos

Ver Reglas:
iptables -L -v -n

Agregar una Regla:
iptables -A <cadena> -p <protocolo> --dport <puerto> -j <acción>

Eliminar una Regla:
iptables -D <cadena> -p <protocolo> --dport <puerto> -j <acción>

Guardar Configuración:

Debian/Ubuntu:
iptables-save > /etc/iptables/rules.v4

Red Hat/CentOS:
service iptables save

Restaurar Configuración:

Debian/Ubuntu:
iptables-restore < /etc/iptables/rules.v4

Ejemplos de Reglas por Categoría

1. Reglas Básicas

Permitir tráfico HTTP:
iptables -A INPUT -p tcp --dport 80 -j ACCEPT

Bloquear tráfico desde una IP específica:
iptables -A INPUT -s <IP> -j DROP

2. Seguridad Avanzada

Permitir tráfico SSH (puerto 22) solo desde una IP confiable:
iptables -A INPUT -p tcp --dport 22 -s <IP_confiable> -j ACCEPT

Bloquear tráfico no solicitado en el puerto 22:
iptables -A INPUT -p tcp --dport 22 -j DROP

3. Mitigación de Ataques

Proteger contra ataques DoS (Denegación de Servicio):
Limitar la tasa de conexiones SYN:
iptables -A INPUT -p tcp --syn -m limit --limit 1/s --limit-burst 4 -j ACCEPT
iptables -A INPUT -p tcp --syn -j DROP

Detener escaneos con nmap:
Limitar la tasa de conexiones SYN para prevenir escaneos:

iptables -A INPUT -p tcp --syn -m limit --limit 10/min --limit-burst 20 -j ACCEPT

#iptables -A INPUT -p tcp --syn -j DROP

Proteger contra ataques de fuerza bruta a SSH:

Bloquear IPs sospechosas manualmente:
#iptables -A INPUT -s <IP_sospechosa> -j DROP

Limitar la tasa de intentos de conexión:
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --set
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 60 --hitcount 5 -j DROP

4. Registro y Auditoría

Registrar tráfico SSH:
iptables -A INPUT -p tcp --dport 22 -j LOG --log-prefix "SSH Attempt: "

Administración de iptables
Verificar y Monitorear Reglas:

Ver reglas con detalles:
iptables -L -v

Contar paquetes y bytes:
iptables -L -v -n --line-numbers

Establecer Políticas Predeterminadas:

Bloquear todo el tráfico entrante por defecto:

iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT