GUIA DE IPTABLES

Comandos	Descripción	Ejemplo
-A	Insertar una regla al final de una cadena	`iptables -A INPUT <especificación de regla>`
-I	Insertar una regla en una posición específica de una cadena	`iptables -I INPUT 1 <especificación de regla>`
-D	Eliminar una regla específica	`iptables -D INPUT <número de regla>` `iptables -D INPUT <especificación de regla>`
-F	Eliminar todas las reglas de un firewall	`iptables -F` `iptables -F -t nat`
-L	Lista todas las reglas de la cadena	`iptables -L` `iptables -L --line-numbers`
-R	Reemplazar una regla en la cadena seleccionada	`iptables -L (OUTPUT|INPUT) <número de regla> (estado)`

PATRON DE RECONOCIMIENTOS MAS COMUNES

Comando	**Descripción**	**Ejemplo**
-j	objetivo de salto Esto especifica el objetivo de la regla; es decir, qué hacer si el paquete coincide.	`iptables -A INPUT -s 192.168.0.0/24 -j DROP`
-s, --source, --src	indica un dominio o IP (rango de Ips) de origen sobre el que se evalúa la condición de la regla	`iptables -A INPUT --source 12.168.120.15 -j ACCEPT` `iptables -A INPUT --src 12.168.120.15 -j ACCEPT`
-d,-- destination, --dst	igual anterior, solo que sobre dirección destino	`iptables -A INPUT --destination 32.112.0.31/24 -j ACCEPT` `iptables -A INPUT --dst 32.112.0.31/24 -j ACCEPT`
-i	interfaz entrada para aplicar regla	`iptables -A INPUT -i eth1 -j ACCEPT`
-o	interfaz salida para aplicar regla	`iptables -A INPUT -o eth0 -j ACCEPT`
-p	especifica el protocolo del	`iptables -A OUTPUT --protocol tcp -j ACCEPT`

Realizado por: Univ. Heidy Soliz Santos

	datagrama a analizar valores válidos: tcp, udp o icmp, o un número	
--sport	Puerto de Origen	`iptables -A OUTPUT --protocol tcp --source-port 21232 -j DROP`
--dport	Puerto de destino	`iptables -A INPUT --protocol tcp -- destination-port 22:12 -j LOG`

ACCIONES MAS COMUNES

Comando	**Descripción**	**Ejemplo**
ACCEPT	dejar el paquete pasar	`iptables -A INPUT -source 192.168.0.1 -j ACCEPT`
DROP	tirar el paquete	`iptables -A INPUT -source 192.168.0.1 -j DROP`

iptables-save > fire.txt	Guardar las configuraciones que hicimos
iptables-restore < fire.txt	Restablecer la configuración
iptables -P INPUT DROP	Denegar todo el tráfico de entrada
iptables -P ONPUT DROP	Denegar todo el tráfico de salida
iptables -t nat -L	Para ver la tabla de nat

Referencias

https://www.acens.com/wp-content/images/2014/07/wp-acens-iptables.pdf

https://linux.die.net/man/8/iptables

http://index-of.co.uk/INFOSEC/iptables.pdf

https://www.acens.com/wp-content/images/2014/07/wp-acens-iptables.pdf

Realizado por: Univ. Heidy Soliz Santos

Realizado por: Univ. Heidy Soliz Santos