**Tarea 6**

|  |  |
| --- | --- |
| **Nombre:** Univ. Mamani Chavez Carla Vanesa | **CI:** 9124602 LP  **Paralelo:** Martes |
| **Docente :** Lic. Gallardo Portanda Franz Ramiro | **Fecha :** 04/03/2020 |

1. **Explicar las reglas que se crean si se ejecutan los siguientes comandos:**

|  |
| --- |
| 1. iptables -A INPUT -p tcp -m iprange –src-range 10.0.100.2-10.0.100.50   El comando iptables se utiliza para el para el filtrado de paquetes   * –A es utilizado para añadir una nueva regla a la cadena especifica * INPUT: es para filtrar paquetes que vienen hacia nuestra máquina * -p Configura el protocolo IP para la regla, el cual puede ser icmp, tcp, udp, o all   Por lo tanto esta regla nos permite bloquear el tráfico que se origina en una ip |
| 1. iptables -A INPUT -m mac –mac-source 00:00:00:00:00:01   El comando iptables se utiliza para el para el filtrado de paquetes   * –A es utilizado para añadir una nueva regla a la cadena especifica * INPUT: es para filtrar paquetes que vienen hacia nuestra máquina * -m mac –mac-source es la dirección MAC de hardware como único medio para tomar decisiones de firewall   Por lo tanto permite bloquear por la dirección mac de un host o de una computadora |
| 1. iptables -A INPUT -p icmp –icmp-type echo-reply -j ACCEPT   El comando iptables se utiliza para el para el filtrado de paquetes   * –A es utilizado para añadir una nueva regla a la cadena especifica * INPUT: es para filtrar paquetes que vienen hacia nuestra máquina * -p Configura el protocolo IP para la regla, el cual puede ser icmp, tcp, udp, o all * -icmp para habilitar la solicitud del cliente entrante de ping * -j especifica el objetivo de la cadena de reglas, o sea una acción * ACCEPT paquete aceptado   Por lo tanto nos permite hacer ping a otros servidores , por defecto el ping esta deshabilitado , y para habilitarlo ponemos ACCEPT |
| 1. iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT   El comando iptables se utiliza para el para el filtrado de paquetes   * –A es utilizado para añadir una nueva regla a la cadena especifica * FORWARD permite el paso de paquetes a otra dirección del firewall * -i eth0 interfaz de entrada * -j especifica el objetivo de la cadena de reglas, o sea una acción * ACCEPT paquete aceptado   Por lo tanto cuando se tiene dos tarjetas red conectadas a internet , podemos configurarlo para que reenvié el tráfico de la red local a través de la internet |
| * iptables −A INPUT −s 80.37.45.194 −p tcp −dport 20:21 −j ACCEPT   El comando iptables se utiliza para el para el filtrado de paquetes     * –A es utilizado para añadir una nueva regla a la cadena especifica * INPUT: es para filtrar paquetes que vienen hacia nuestra máquina * -s Se utiliza para coincidir con la dirección de origen del paquete * -p Configura el protocolo IP para la regla, el cual puede ser icmp, tcp, udp, o all * -dport puerto destino * -j especifica el objetivo de la cadena de reglas, o sea una acción * ACCEPT paquete aceptado   Por lo tanto nos permite la conexión a los puertos 20 al 21de una ip de origen |
| 1. iptables -A OUTPUT -o eth0 -p tcp –sport 80 -m state –state ESTABLISHED -j ACCEPT   El comando iptables se utiliza para el para el filtrado de paquetes   * –A es utilizado para añadir una nueva regla a la cadena especifica * OUTPUT es el filtrado de paquetes de salida * -o eth0 interfaz de salida * -p Configura el protocolo IP para la regla, el cual puede ser icmp, tcp, udp, o all * -sport es el puerto de origen * ESTABLISHED establecido * -j especifica el objetivo de la cadena de reglas, o sea una acción * ACCEPT paquete aceptado   Por lo tanto nos permite el trafico saliente (OUTPUT) hacia las demás páginas web |
| * sudo iptables -A INPUT -p tcp -s 15.15.15.0/24 --dport 3306 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT   El comando iptables se utiliza para el para el filtrado de paquetes   * –A es utilizado para añadir una nueva regla a la cadena especifica * INPUT: es para filtrar paquetes que vienen hacia nuestra máquina * - p Configura el protocolo IP para la regla, el cual puede ser icmp, tcp, udp, o all * -s Se utiliza para coincidir con la dirección de origen del paquete * -dport puerto destino * -m comntrack es un alias * -j especifica el objetivo de la cadena de reglas, o sea una acción * ACCEPT paquete aceptado   Por lo tanto esto nos va permitir y mantener activas las conexiones tanto de entrada como de salida, que tiene origen una ip en el puerto 3306. |
| 1. sudo iptables -A INPUT -i eth1 -p tcp --dport 5432 -m conntrack –ctstate NEW,ESTABLISHED -j ACCEPT  * sudo Permiten ejecutar los programas con los privilegios de administrador * El comando iptables se utiliza para el para el filtrado de paquetes * –A es utilizado para añadir una nueva regla a la cadena especifica * INPUT: es para filtrar paquetes que vienen hacia nuestra máquina * -p Configura el protocolo IP para la regla, el cual puede ser icmp, tcp, udp, o all * -dport puerto destino * -m comntrack es un alias * --ctstate Reemplaza contrack * -j especifica el objetivo de la cadena de reglas, o sea una acción * ACCEPT paquete aceptado   Por lo tanto nos permite crear y establecer una conexión mediante la interfaz eth1 hacia el puerto 5432 tanto de entrada como de salida |
| 1. sudo iptables -A INPUT -p tcp --dport 143 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT  * sudo Permiten ejecutar los programas con los privilegios de administrador * El comando iptables se utiliza para el para el filtrado de paquetes * –A es utilizado para añadir una nueva regla a la cadena especifica * INPUT: es para filtrar paquetes que vienen hacia nuestra máquina * -p Configura el protocolo IP para la regla, el cual puede ser icmp, tcp, udp, o all * -dport puerto destino * -m comntrack es un alias * --ctstate Reemplaza contrack * -j especifica el objetivo de la cadena de reglas, o sea una acción * ACCEPT paquete aceptado   Por lo tanto nos permite crear y establecer una conexión mediante la interfaz eth1 hacia el puerto 143 tanto de entrada como de salida |
| 1. iptables -A INPUT -p tcp –dport 80 -m limit –limit 25/minute –limit-burst 100 -j ACCEPT  * El comando iptables se utiliza para el para el filtrado de paquetes * –A es utilizado para añadir una nueva regla a la cadena especifica * INPUT: es para filtrar paquetes que vienen hacia nuestra máquina * -p Configura el protocolo IP para la regla, el cual puede ser icmp, tcp, udp, o all * -dport puerto destino * -m limit – limit Se usa para restringir la tasa de coincidencias. * -j especifica el objetivo de la cadena de reglas, o sea una acción * ACCEPT paquete aceptado   Por lo tanto nos permite prevenir y bloquear ataques DDos |
| 1. iptables -A FORWARD -p TCP -i eth0 -s 192.168.9.0/24 -d 0/0 --dport 22 -j ACCEPT   El comando iptables se utiliza para el para el filtrado de paquetes   * –A es utilizado para añadir una nueva regla a la cadena especifica * FORWARD permite el paso de paquetes a otra dirección del firewall * -p Configura el protocolo IP para la regla, el cual puede ser icmp, tcp, udp, o all * -i eth0 interfaz de entrada * -s Se utiliza para coincidir con la dirección de origen del paquete * -d Direcciones ip de destino. * -dport Puerta de destino * -j especifica el objetivo de la cadena de reglas, o sea una acción * ACCEPT paquete aceptado   Por lo tanto nos permite la conexión del puerto 22 desde una interfaz en este caso es eth0 del ip origen 192.168.9.0/24 |

1. **Escribir los respectivos comandos para crear las siguientes reglas (donde sea necesario, completar con una dirección IP):**

|  |
| --- |
| 1. Permitir tráfico DNS saliente   Bloquear la URL www.twitter.com  iptables -A INPUT -p tcp --dport www.twitter.com -j DROP |
| 1. Permitir el tráfico saliente de todas las conexiones establecidas en respuesta a legítimas conexiones de entrada   iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT |
| 1. Permitir todas las conexiones entrantes de SSH   iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT |
| 1. Bloquear el tráfico saliente de SMTP   iptables -A INPUT -p tcp --dport 25 -j DROP |
| 1. Permitir todo el tráfico saliente HTTPS  * iptables -A INPUT -I eth0 -p tcp --dport 80 -m state --state new,ESTABLISHED -j ACCEPT * iptables -A INPUT -I eth0 -p tcp --dport 443 -m state --state new,ESTABLISHED -j ACCEPT |
| 1. Bloquear todo el tráfico de una dirección IP independientemente del servicio solicitado  * iptables -A INPUT -p tcp –dport 192.168.0.4 -j DROP * iptables -A OUTPUT -p tcp –dport 192.168.0.4 -j DROP * iptables -A FORWARD -p tcp –dport 192.168.0.4 -j DROP |
| 1. Permitir al servidor responder a todas las conexiones POP3.   iptables -A INPUT -p tcp –dport 110 -j ACCEPT |
| 1. Permitir las conexiones entrantes desde una página web  * iptables -A INPUT -i eth0 -p tcp –dport 80 -m state –state NEW,ESTABLISHED -j ACCEPT * iptables -A INPUT -i eth0 -p tcp –dport 443 -m state –state NEW,ESTABLISHED -j ACCEPT |
| 1. Bloquear las conexiones entrantes por el puerto 1234   iptables -A INPUT -p icmp -s 192.168.0.4 --dport 1234 -j DROP |
| 1. Bloquear peticiones ping   iptables -A INPUT -p icmp –icmp-type echo-request -j DROP |
| 1. Permitir tráfico SSH de 192.168.9.0/24 a donde sea   iptables -A INPUT -s 192.168.9.0/24 –i eth0 –p TCP –destinatation –port ssh –j ACCEPT |
| 1. Permitir POP3 y POP3S  * iptables -A INPUT -i eth0 -p tcp --dport 110 -m state --state NEW,ESTABLISHED -j ACCEPT * iptables -A OUTPUT -o eth0 -p tcp --sport 110 -m state --state ESTABLISHED -j ACCEPT * iptables -A INPUT -i eth0 -p tcp --dport 995 -m state --state NEW,ESTABLISHED -j ACCEPT * iptables -A OUTPUT -o eth0 -p tcp --sport 995 -m state --state ESTABLISHED -j ACCEPT |