Fecha límite para la entrega: 28 de diciembre de 2024

1. OBJETIVO

En esta práctica se aborda el filtrado de paquetes, procedimiento básico para la construcción de cortafuegos (*firewals*). Para establecer las reglas de filtrado utilizaremos el módulo *NetFilter*, integrado en el kernel de Linux y accesible a través del interfaz de comandos *iptables.* También trabajaremos con *UFW* y *shorewall*, dos herramientas de alto nivel que permiten configurar NetFilter.

Cubriremos los siguientes objetivos:

- Filtros de paquetes sin estado y con estado
- Translación de direcciones (NAT), redirección y enmascaramiento
- Administración de cortafuegos personal con UFW
- Administración de cortafuegos de red con *shorewall*

2. TAREAS A REALIZAR

Cortafuegos personal

1. Establecer distintas reglas de filtrado sin estado sobre las cadenas INPUT y OUTPUT. Filtraremos ambos sentidos de la conexión, con reglas complementarias. Fijar en primer lugar la política DROP para el tráfico entrante y saliente del equipo, y habilitar a continuación el intercambio ICMP con el resto de los equipos de nuestra subred. Permitir el tráfico saliente hacia los puertos 80/tcp, 443/tcp y 53/udp (nuestro equipo actúa como cliente). Habilitar el tráfico entrante al puerto 22/tcp y 80/tcp (nuestro equipo actúa como servidor).
2. Comprobar el efecto que tiene el orden de las reglas de filtrado. Partiendo de una configuración sin filtros, bloquear todo el tráfico TCP saliente salvo el dirigido a una dirección IP concreta de nuestra subred, viendo el efecto del orden en la entrada de las dos reglas necesarias.
3. Definir una regla que redirija todo el tráfico SSH saliente que va hacia una dirección IP concreta (por ejemplo, 1.2.3.4) para que se redirija a la IP de un servidor real que tenga el servicio SSH activo. Para probar su funcionamiento, abrir una sesión SSH contra 1.2.3.4.
4. Desde una máquina remota, utilizar **nmap** para identificar el sistema operativo de nuestra máquina virtual Linux. A continuación, aplicar una regla con estado para impedir conexiones TCP inválidas (las que no se inician con el segmento SYN). Volver a utilizar la herramienta nmap para identificar el SO y comentar los nuevos resultados obtenidos.

   Nota1. Para detectar el SO de un equipo es necesario que tenga abierto algún puerto TCP.
5. Partir nuevamente de una configuración sin filtros y bloquear todo el tráfico entrante y saliente. A continuación, definir reglas con estado que permitan iniciar conexiones TCP o UDP hacia el exterior, así como el tráfico ICMP siempre que sea iniciado por nosotros o relacionado con nuestras conexiones. Comprobarlo iniciando conexiones exteriores, intentando conectar desde el exterior (por ejemplo, al servidor SSH) y lanzando o recibiendo mensajes de alcanzabilidad (ping).
6. Considere la siguiente situación: Se están produciendo accesos continuos a nuestro servidor OpenSSH para intentar descubrir mediante fuerza bruta usuarios y contraseñas válidas del sistema. Nos gustaría limitar el número de accesos desde una única dirección IP origen (por ejemplo, un máximo de 2 conexiones cada 180 segundos desde cada IP), para minimizar el riesgo este tipo de intentos sin afectar a los usuarios legítimos. Busque una solución para este problema mediante iptables, e indique la secuencia de reglas que habría que aplicar para implantar esta política y la función que cumple cada de ellas. Para acotar más aún estos intentos de acceso es posible limitar también el número máximo de

reintentos de autentificación en cada sesión (por ejemplo, a dos). ¿Cómo podríamos configurar esta nueva restricción?

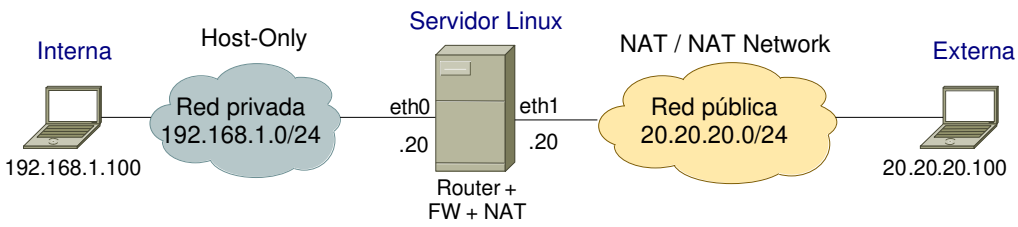
Cortafuegos personal con UFW

7. UFW (*Uncomplicated Firewall*) es una aplicación desarrollada por Canonical (Ubuntu) para activar reglas iptables y mantener un cortafuegos personal de manera sencilla. Para realizar este apartado se recomienda usar una máquina Ubuntu, que tienen ya instalado UFW. Llevar a cabo las siguientes tareas:
   a. Verificar el estado del cortafuegos personal y si ya existen reglas iptables
   b. Arrancar algún servicio en el equipo para realizar las pruebas posteriores (Apache2, OpenSSH Server, …)
   c. Arrancar UWF y configurar su arranque automático. Iniciar el cortafuegos (ufw enable)
   d. Comprobar el estado de UFW (ufw status). También es posible ver información extendida (ufw status verbose) que incluye la política definida, y las reglas iptables generadas (iptables -L -n | more). Con este último comando podemos ver las nuevas reglas y cadenas generadas por UFW.
   e. Usar el comando ufw default allow|deny incoming|outgoing para definir la configuración por defecto del cortafuegos personal. Comprobar el efecto de estos comandos intentando conexiones hacia o desde el equipo.
   f. Establecer una política por defecto que permita conexiones salientes e impida conexiones entrantes.
   g. Sobre la configuración anterior permitir conexiones entrantes a los servicios arrancados en el apartado b) (ufw allow …)
   h. También es posible limitar las conexiones realizadas desde una IP origen (ufw limit …), para mitigar los ataques de diccionario. Activar el acceso limitado al servidor SSH de nuestro equipo. ¿Qué límite se ha establecido para las conexiones SSH entrantes?

Router con función de cortafuegos y NAT

8. Vamos a preparar una maqueta como la reflejada en el gráfico adjunto. Añadiremos dos nuevas máquinas virtuales (interna y externa) y asociaremos un segundo interface (eth1) a la máquina que actúa como cortafuegos. La red exterior (puede usar el modo NAT en *VMWare* o NAT Network en *VirtualBox*) tendrá un direccionamiento público (20.20.20.0/24) y la privada (en modo Host-Only) tendrá direccionamiento privado (192.168.1.0/24). Las nuevas máquinas tendrán como *router* por defecto al equipo que actúa como firewall.

   NOTA: Verificar el nombre de los interfaces asignados, y la red a la que están conectados.



9. Reiniciar el servicio de red y comprobar que somos capaces de alcanzar las máquinas interna y externa desde el cortafuegos (fw). Habilitar el encaminamiento en el cortafuegos (añadir net.ipv4.ip_forward=1 en el archivo /etc/sysctl.conf y a continuación ejecutar sysctl -p; puede comprobarse el nuevo valor con sysctl net.ipv4.ip_forward). Verificar que es posible comunicar las máquinas interna y externa.

10. Instalar la herramienta shorewall (los paquetes rpm se encuentran en el directorio /usr/local/src/shorewall).
11. Describir unas políticas básicas en el cortafuegos: se acepta el tráfico desde la red interna al exterior (saliente), se impide tráfico entrante desde el exterior, se acepta tráfico saliente desde el cortafuegos hacia cualquier sitio. Se acepta tráfico entrante al cortafuegos desde la red interna. Activar las reglas (systemctl start shorewall) y verificar su correcto funcionamiento.
12. Habilitar el enmascaramiento de direcciones desde la red interior hacia la red exterior. Verificar que todo el tráfico saliente se enmascara (puede usar el sniffer tcpdump)
13. Implantar una política más restrictiva para el tráfico que atraviesa el FW (todo el tráfico será rechazado). A continuación, se habilitará la salida a servicios concretos (http, https, SMTP, …). Configurar algún servicio de *port forwarding* que será visible desde el exterior y ofrecido por la máquina de la red interna. Configurar un acceso al cortafuegos por SSH desde una dirección externa concreta. Establecer el redireccionamiento de todo el tráfico DNS saliente para que se reenvíe a un servidor de DNS externo concreto.

    Para realizar este apartado se recomienda estudiar los ejemplos de reglas shorewall presentes en el manual de esta aplicación (man shorewall-rules)

Parte OPCIONAL

14. Vamos a trabajar con la sintaxis nativa del módulo **Nftables** (nft). Para ello realizaremos las siguientes tareas
    a) Habilitar el uso de nftables. Normalmente ya contamos con el módulo y el interface de comandos (este último, de no existir, se instala con el paquete nftables). La activación de nftables se realiza como si fuera un nuevo servicio (systemctl enable nftables && systemctl start nftables). Ojo: si previamente están activos otros servicios de filtrado (ufw, firewalld, …), deben desactivarse.
    b) Identificar la tabla predefinida (inet filter), con sus cadenas, políticas y posibles reglas (nft list ruleset). Identificar también dónde se encuentra el archivo de esta tabla nftables (el que se activa al iniciar el servicio).
    c) Establecer una política de drop para todo el tráfico entrante y saliente.
    d) Añadir reglas para permitir la entrada y salida al interface de loopback (lo).
    e) Añadir reglas para permitir conexiones HTTP y HTTPS salientes (iniciades desde el equipo hacia cualquier iP externa).
    f) Añadir reglas para permitir la conexión a nuestro servidor SSH desde cualquier equipo que se encuentre en la misma red el nuestro.
    g) Verificar la política definida y salvar la nueva política para que se active en el arranque.

3. FORMA DE ENTREGA

Una vez finalizada la práctica, se entregará una memoria justificativa en formato PDF. Deberá incluir los pasos seguidos para la realización de cada tarea planteada, comandos utilizados y dificultades encontradas.

La memoria será ordenada, clara y legible, e irá encabezada con el nombre del autor. Se deberán evitar los “listados” innecesarios. Si se considera de interés, podrán incorporarse como anexos a la memoria, debidamente reseñados.

El resultado será un documento único denominado **practica4-SPD.pdf** que se enviará antes de la fecha de cierre a la dirección de correo electrónico **teo.rojo@ceu.es**.

Se podrá requerir la defensa individual de la práctica. Se deberá guardar una copia del entorno virtual utilizado en el desarrollo de la práctica, para poder verificar, si fuera necesario, su correcto funcionamiento.

4. REFERENCIAS

https://netfilter.org/

https://launchpad.net/ufw

https://shorewall.org/

https://netfilter.org/projects/nftables/