ADMINISTRACIÓN DE REDES Y SISTEMAS

PRÁCTICAS DE LABORATORIO

Traducción de direcciones y puertos (NAPT)

En la mayoría de las organizaciones los equipos de la red corporativa (o red interna) se configuran con direcciones IP privadas (RFC 1918) y es necesario hacer traducción de direcciones (NAT) para utilizar un número reducido de direcciones públicas externas para la conectividad a Internet de dichos equipos.

Cada infraestructura de alumno (en adelante, su organización) se dispone de una única dirección pública (asignada a la interfaz "eth0" del equipo "01"), y direcciones privadas en el rango 172.21.XX.0/24 correspondiendo XX al sufijo "arsXX".

NAPT en FreeBSD:

Manual de FreeBSD, capítulo "Firewalls", apartado "IPFW".

Existen diversas maneras de implementar NAPT en FreeBSD. En las prácticas del laboratorio se utiliza la opción de "Userspace NAT" (apartado 31.4.4.3) bajo IPFW.

Tarea 1: Configure el demonio `natd` para que realice traducción de direcciones y puertos automática del tráfico saliente. Para ello, cree un fichero de configuración `/etc/natd.conf` (vacío, de momento) y configure que el demonio se lance automáticamente al iniciar.

Tarea 2: Prepare el filtro cortafuegos *ipfw* para que funcione en configuración básica, sin filtrado alguno, pero establezca una regla *divert* a fin de que todos los paquetes IP se envíen al demonio `natd` para que este, si fuera necesario, altere su contenido. Recuerde que, en su organización, como es habitual, solo debería aplicar NATP al tráfico en la interfaz pública. Verifique que las máquinas internas pueden enviar/recibir tráfico a/desde equipos externos a su organización.

NOTA: En el laboratorio se describe cómo se realizan estas tareas. Una secuencia de pasos está descrita en el manual referenciado.

Tarea 3: Redirecciones puertos, de forma que la dirección y puerto IP-pública de su organización:22005/tcp permita alcanzar el servicio SSH en su máquina "05" (en la red interna). Repita lo mismo para los puertos 22006/tcp (a su máquina "06") a 22009/tcp a su máquina "09". Verifique, usando un cliente SSH, que puede acceder a las mismas.

Filtro cortafuegos

El cortafuegos es un filtro que inspecciona cada paquete presente en las interfaces de red donde actúe y, en base a unas reglas preestablecidas (que señalan qué campos del

paquete inspeccionar), realiza alguna acción (deja pasar o descarta, principalmente) con el paquete.

A veces permiten añadir alguna acción intermedia, tal como derivar (*divert*) el paquete a algún servicio y continuar su procesado con lo que este devuelva (se ha hecho así para el servicio *natd*).

En consecuencia, la dificultad de configuración de un cortafuegos reside, fundamentalmente, en el conocimiento detallado de los diferentes protocolos (y, en concreto de cómo las diferentes funcionalidades y estados se reflejan en sus formatos de trama) para definir adecuadamente las reglas de filtrado.

Cortafuegos en FreeBSD:

Conceptos:

https://docs.freebsd.org/en_US.ISO8859-1/books/handbook/firewalls-concepts.html

IPFW

https://docs.freebsd.org/en_US.ISO8859-1/books/handbook/firewalls-ipfw.html

Tarea 4: Cree un fichero de configuración `/usr/local/etc/ipfw.conf` y añada en el mismo un conjunto de reglas para el cortafuegos `ipfw`. Seguiremos una política restrictiva (todo el tráfico se descarta excepto el explícitamente permitido). A través de estas reglas se pretende que:

- La comunicación local entre clientes y servidores en ejecución en el propio cortafuegos debe estar permitida.
- Las máquinas de su organización pueden establecer las conexiones TCP habilitadas, o iniciar comunicaciones sobre UDP a servicios habilitados, hacia cualquier equipo en la red IPv4 pública. Pero este tráfico solo se permite si quien inició la comunicación (sesión) fue el equipo de su organización. Es decir, se desea un cortafuegos *con estado*.
- Las máquinas de la red externa (pública) no pueden iniciar conexiones ni enviar tráfico alguno a las máquinas de su organización, salvo las excepciones expresamente contempladas.
- Se contempla permitir el acceso desde todas las máquinas de su organización, incluido el cortafuegos, a los servicios NTP, DNS, SSH, HTTP y HTTPS ubicados en la red pública.
- Se permite todo el tráfico ICMP.
- Continúa operativo el mecanismo NAPT.
- Se activan reglas preventivas que eviten usos malintencionados. **IMPORTANTE**: En nuestro laboratorio, la red 10.48.0.0/23 simula ser la red "pública" (la dirección "pública" de su organización se incluye en dicho rango de direccionamiento) y alberga a *lamarr* y otros servicios, por lo que debe permitirse este tráfico en la interfaz externa (a pesar de tratarse de un direccionamiento privado).
- Se realiza *log* del tráfico relevante (establecimientos de conexión, …).

- Se permite el acceso desde la red pública, y el propio cortafuegos, al servicio SSH de todas las máquinas de su organización, incluido el cortafuegos.

Tarea 5: **Opcional**. Amplíe la capacidad de filtrado en el cortafuegos de su organización para (puede realizar alguna, varias o todas las siguientes):

- No permita que fragmento IPv4 alguno alcance a los equipos de su organización. Para ello, podría impedir completamente el tráfico IP fragmentado o, como alternativa más conveniente que no descarta tráfico que podría ser legítimo, reensamblar los fragmentos IPv4 en el cortafuegos.
- Utilice el mecanismo *nat* incorporado en el propio cortafuegos ipfw, en sustitución del servicio *natd* externo al cortafuegos.
- Permita solo el tráfico ICMP correspondiente a ping y redirecciones. Mejor, de forma controlada o limitada (ratios por segundo,…).
- Se habilita una ratio máxima por segundo (p.ej en cierto tráfico ICMP, o en cantidad de establecimientos de conexión a ciertos servicios de su organización,…).