Seguridad en Redes

Topologías Seguras

Sergio Jiménez del Coso
Eduardo Eiroa Ballester

1. Servicios utilizados

- Herramienta de monitorización bmon: Monitorización de Red (Web-Server)
- Herramienta de monitorización Netdata: Monitorización de Red e iptables (Router)
- Servidor dnsmasq: DNS y DHCP (Router)
- Servidor NTP: Protocolo de Tiempo de Red (Web-Server)
- Servidor Web: Apache2 (Web-Server)

2. Políticas de Seguridad

- Los usuarios de la MZ y DMZ podrán enviar paquetes ICMP (ping) a todos los demás nodos incluidos a los nodos en Internet tipo www.google.es.
- El servicio web alojado en el nodo Web-Server de la DMZ será accesible tanto a los usuarios de la red MZ como a los usuarios en Internet, conociendo la IP el router (IP pública de nuestra topología).
- Solo los usuarios de la red MZ podrán utilizar el servicio de NTP para sincronizar sus relojes.
- El servidor DNS proporciona servicio DNS a cada uno de los clientes alojados en la MZ.
- El servicio de DHCP proporcionará una IP a cada uno de los clientes alojados en la MZ.
- El nodo router proporcionará la salida de Internet al nodo PC1.
- Todos los nodos tendrán conexión a Internet con el objetivo de poder actualizar cada uno de los nodos y contener los repositorios actualizados.
- Para la correcta utilización de NetData, el router debe permitir el paso del tráfico del puerto correspondiente al servicio, el 19999.
- Todo el tráfico no especificado en este apartado será eliminado ya que hemos integrado una política restrictiva.

2.1 Mecanismos de Seguridad

- Firewall basado en iptables

3. Tests

- Hacer ping en cada uno de los nodos procedentes de Internet, MZ, Router y DMZ.
- DNS: Cada uno de los nodos deberán resolver **www.google.es**.
- Servidor web: los nodos de la MZ y aquellos usuarios que proceden de Internet puedan acceder al servicio web y obtener el archivo correspondiente del servidor Web (index.html) indicando la ip del router.
- NTP: solo los nodos de la MZ podrán hacer uso del servicio NTP para actualizar la fecha que corresponde al servidor. Primero se cambiará la fecha del nodo y finalmente, el nodo ejecutará el comando "`ntpdate <ip del servidor>`" con el objetivo de actualizar el tiempo del sistema: Día, hora, minutos, segundos...etc.

4. Contenidos adicionales.

a) Tanto el servidor Web y el servidor NTP estarán alojados en el mismo nodo.
b) Para los usuarios procedentes de Internet, el nodo Router redirigirá los paquetes procedentes de los usuarios de Internet para acceder al servicio Web alojado en la DMZ.

c) La configuración de todos los servicios alojados en los diferentes nodos se realizará de forma automática, excepto la instalación de la herramienta de monitorización **Net-Data.**

5. Registro de iptables.

Registramos los paquetes rechazados (DROP) desde nuestro firewall mediante unas reglas de iptables, que escriben en **/var/log/messages** los paquetes que han sido descartados.

6. Monitorización de Red

Disponemos de dos servicios para monitorizar la red:

- BMON (Instalado en el Web-Server)
- NetData (Instalación en el Router)

Recomendamos usar **NetData** ya que contiene una gran variedad de opciones con el objetivo de visualizar la gestión de nuestro nodo Router. Para usarlo, debemos acceder desde el navegador por la interfaz eth1 del router en el puerto 19999.
En el caso del **bmon**, se trata de una herramienta de monitorización algo mucho más sencillo de manejar y de visualizar. Como está indicado en el README.md, para poder visualizar la herramienta de monitorización, se debe añadir una regla en el archivo iptables:

-A PREROUTING -i eth1 -p tcp --dport 19999 -j DNAT --to-destination <IP-Router>:19999

Esta regla especifica que la tabla NAT utiliza la cadena incorporada PREROUTING para reenviar las peticiones del puerto 19999 entrantes exclusivamente a la dirección IP del nodo router. Para ello ejecutaremos **vagrant provison router**.

7. Esquema de Red