Monitoreo de red con Arpwatch

Arpwatch permite que un sistema rastree IP pares de direcciones. Mapea las MAC Addresses en una red al rastrear ARP a cada una dispositivo en LAN y registra la respuesta en una base de datos. Todas las tarjetas de red se fabrican con una dirección MAC única y esto permite que Arpwatch identifique cada dispositivo. El objetivo principal de mapear una red como esta es para que el administrador del sistema pueda realizar un seguimiento de los dispositivos en una red e identificar cuándo hay problemas de red. Arpwatch se usa comúnmente para identificar cuándo se está llevando a cabo un ARP Man in the Middle attack notificando al administrador del sistema cuando se usa una dirección MAC duplicada en el red. Arpwatch se ejecuta más comúnmente en enrutadores, pero también puede ser útil en un conmutador de red administrado.

Instalar

Arpwatch no es aparte de la distribución estándar de Slackware Linux. Se puede obtener descargando SlackBuild de SlackBuilds.org para la versión de Slackware que desee. SlackBuilds.org tiene un excelente HOWTO que trata cómo instalar un SlackBuild. Las SlackBuilds.org FAQ también son muy útiles para los usuarios de Slackware que quieren instalar un SlackBuild.

Configuración

El script de inicio incluido permite al administrador configurar Arpwatch para una o más tarjetas de red. También es donde el administrador puede configurar los ajustes del tiempo de ejecución para Arpwatch. Abra **/etc/rc.d/rc.arpwatch** en su sistema y edite la variable **OPTIONS** para su necesidades. Por defecto, la cuenta **root** recibe todos los correos electrónicos de Arpwatch. Cambie la cuenta de correo electrónico que Arpwatch usará para las notificaciones por correo electrónico. Asegúrese de utilizar una cuenta de usuario o una dirección de correo electrónico que exista o Arpwatch no le enviará notificaciones.

La línea que estás buscando es:

```
OPTIONS="-i $IFACE -f $ARPDIR/arp-$IFACE.dat -u root -e root -s root"
```

La página del manual de Arpwatch indica que el interruptor **- e** administra la cuenta de correo electrónico. Cambiemoslo al usuario **darkstar** .

```
OPTIONS="-i $IFACE -f $ARPDIR/arp-$IFACE.dat -u root -e darkstar -s root"
```

O podemos usar una dirección de correo electrónico remota si **sendmail** está configurado para hacerlo:

```
OPTIONS="-i $IFACE -f $ARPDIR/arp-$IFACE.dat -u root -e
user@randomdomain.com -s root"
```

Actualizar la base de datos de direcciones MAC

El README.ethercodes instalado con Arpwatch SlackBuild indica que la base de datos de direcciones MAC que viene con el tarball fuente puede estar desactualizada. Esta base de datos solo se actualiza cuando hay una nueva versión de Arpwatch, que no ha sucedido en mucho tiempo.

Estos pasos están cubiertos en mayor detalle si lees /usr/doc/arpwatch-$VERSION/README.ethercodes

```
su -
cd /var/lib/arpwatch
wget http://standards-oui.ieee.org/oui.txt
./massagevendor oui.txt > ethercodes.dat
rm -f oui.txt
```

Comience y pare en el arranque

El archivo **/ etc / rc.d / rc.arpwatch** controla el inicio y apagado de Arpwatch. Para utilizar este script, debe agregar algunas líneas a **/ etc / rc.d / rc.local** y **/ etc / rc.d / rc.local_shutdown** . Asegúrese de utilizar el orden adecuado si tiene otros servicios de red que comienzan o se detienen en estos scripts. Como ejemplo, debe iniciar Arpwatch antes de abrir hostapd si está ejecutando un Punto de acceso inalámbrico, y apagar Arpwatch después de que hostapd salga. El uso de tales pedidos asegura que Arpwatch identifique todas las solicitudes ARP en su red.

Continuando con el ejemplo anterior, supongamos que está ejecutando un punto de acceso inalámbrico. Agregue esto a **/ etc / rc.d / rc.local**

```
if [ -x /etc/rc.d/rc.arpwatch ]; then
  /etc/rc.d/rc.arpwatch start wlan0
fi
```

Si desea ejecutar Arpwatch en múltiples tarjetas de red, ajuste **/etc/rc.d/rc.local** de esta manera:

```
# Change eth0 and wlan0 to match your configuration
if [ -x /etc/rc.d/rc.arpwatch ]; then
  /etc/rc.d/rc.arpwatch start eth0
  /etc/rc.d/rc.arpwatch start wlan0
fi
```

Es importante que Arpwatch se detenga limpiamente cuando su sistema se apaga o se reinicia. Si aún no lo ha hecho, cree **/etc/rc.d/rc.local_shutdown** como root:

```
touch /etc/rc.d/rc.local_shutdown
```

A continuación, debe editar **rc.local_shutdown** así:

```
if [ -x /etc/rc.d/rc.arpwatch ]; then
  /etc/rc.d/rc.arpwatch stop
```

```
fi
```

Finalmente, marque **rc.local** y **rc.local_shutdown** como *ejecutable* . Esto le dice a Slackware que ejecute automáticamente estos scripts durante el proceso de arranque.

```
chmod +x /etc/rc.d/rc.local
chmod +x /etc/rc.d/rc.local_shutdown
```

Finalizando

Suponiendo que se siguieron todos los pasos, debería haber recibido un correo electrónico por cada dispositivo que Arpwatch descubrió en su red. Si optó por utilizar el usuario **root** para las notificaciones, puede verlas utilizando el comando **mail** como usuario root.

```
mail -f /var/spool/mail/root
```

Aquí hay un ejemplo de lo que puede encontrar en su bandeja de entrada:

```
           hostname: <unknown>
         ip address: 192.168.151.170
   ethernet address: XX:XX:XX:XX:XX:XX
   ethernet address: XX:XX:XX:XX:XX:XX
    ethernet vendor: <unknown>
          timestamp: Monday, April 9, 2018 12:01:39 -0600
```

Fuentes

- Arpwatch Home
- Originalmente escrito por Brenton Earl
- Traducido por Víctor 2019/08/26 13:21 (UTC)

howtos, network, monitoring, arpwatch, user mralk3