arpwatch

arpwatch – демон, который отслеживает соответствие между IP и MAC-адресами, и при обнаружении аномалий, сообщающий об этом в Syslog. Используется как один из инструментов для борьбы с ARP-spoofing'ом.

Демон анализирует ARP-ответы на сетевом интерфейсе, к которому он привязан, и запоминает соответствие IP-адресов и MAC-адресов. Как только он видит, что соответствие нарушено, или обнаруживает появление новых адресов в сети, он сообщает об этом в системный журнал (syslog).

```
# yum install arpwatch
```

Конфигурируем:

```
$ cat /etc/sysconfig/arpwatch
OPTIONS="-i enp5s0 -f arp.dat -u arpwatch -e admin@example.com
-s 'root (Arpwatch)'"
```

```
$ sudo systemctl start arpwatch
$ sudo systemctl enable arpwatch
```

```
/var/lib/arpwatch - default directory
          arp.dat - ethernet/ip address database
   ethercodes.dat - vendor ethernet block list
```

По умолчанию, демон пишет логи в /var/log/messages, что бы не мусорить в этот файл перенаправим в отдельный лог. Для этого создаем файл логов и файл конфигурации для rsyslog

```
# touch /var/log/arpwatch.log
```

```
# vi /etc/rsyslog.d/arpwatch.conf
if ( $programname startswith "arpwatch" ) then {
action(type="omfile" file="/var/log/arpwatch.log")
stop
}
```

Проверяем и перезапускаем:

```
# rsyslogd -N 1
# systemctl restart rsyslog
```

Так как в первых трех октетах MAC-адреса кодируется производитель оборудования, нам желательно иметь обновленную локальную базу MAC/Производитель. Обновляем базу MAC адресов:

```
# vi arpwatch_update_mac.sh

#!/bin/bash
# update_mac_addresses.sh
# This script downloads the currect mac address data from the IEEE and parses it for nmap and arpwatch.
# nmap-mac-prefixes is for nmap.
# ethercodes.dat is arpwatch.

# Download the current data

wget http://standards-oui.ieee.org/oui/oui.txt

# Divide the data into Manufacturer and Address files
cat oui.txt | grep '(base 16)' | cut -f3 > mac.manufacturer
cat oui.txt | grep '(base 16)' | cut -f1 -d' ' > mac.address

# Paste them back together for nmap data
paste mac.address mac.manufacturer > nmap-mac-prefixes

# Parse the address data for arpwatch
cat mac.address | perl -pe 's/^(([^0].)|0(.))(([^0].)|0(.))(([^0].)|0(.))/\2\3:\5\6:\8\9/' > tmp.address
cat tmp.address | tr [A-Z] [a-z] > mac.address

# Paste the parsed data into the arpwatch file
paste mac.address mac.manufacturer > /var/lib/arpwatch/ethercodes.dat

# Clean up intermediary files
rm tmp.address
rm mac.address
rm mac.manufacturer
rm oui.txt
```

Делаем файл исполняемым и прописываем в cron для ежемесячного обновления:

```
# chmod +x arpwatch_update_mac.sh

# crontab -e
@monthly                /home/svm/bin/arpwatch_update_mac.sh
```

ARPWatch рассылает четыре вида сообщений.

- **new activity** – связка ethernet/ip-адресов снова проявила активность спустя шесть месяцев или больше
- **new station** – ethernet-адрес зафиксирован впервые
- **flip flop** – ethernet-адрес изменился с одного известного адреса на другой известный адрес
- **changed ethernet address** – хост перешёл на использование нового ethernet-адреса

ARPWatch также пишет события в **messages/syslog**.

В **syslog** могут писаться следующие типы уведомлений:

- **ethernet broadcast** – MAC-адрес хоста является широковещательным.
- **ip broadcast** – IP-адрес хоста является широковещательным.
- **bogon** – адрес отправителя IP-пакета не входит в непосредственно подключённую сеть (directly connected network) для заданного интерфейса.
- **ethernet broadcast** – MAC-адрес отправителя состоит из одних нулей или одних единиц.
- **ethernet mismatch** – MAC-адрес отправителя пакета не соответствует MAC-адресу, указанному внутри ARP-запроса.
- **reused old ethernet address** – ethernet-адрес изменился с известного адреса на адрес, который был замечен ранее, но не только что. (Похоже на flip flop, но чуть-чуть другое.)
- **suppressed DECnet flip flop** – сообщение “flip flop” подавлено в связи с тем, что как минимум один из двух адресов является адресом DECnet.

Если в логах появляются сообщения вида

```
Aug  2  06:52:09  ring  arpwatch:  bogon  10.90.90.91
1c:af:f7:e1:b6:71
Aug  2  06:52:10  ring  arpwatch:  bogon  10.90.90.91
1c:af:f7:e1:b6:71
Aug  2  06:52:35  ring  arpwatch:  bogon  10.90.90.91
1c:af:f7:e1:b6:71
Aug  2  06:52:36  ring  arpwatch:  bogon  10.90.90.91
1c:af:f7:e1:b6:71
Aug  2  06:52:37  ring  arpwatch:  bogon  10.90.90.91
1c:af:f7:e1:b6:71
```

где 10.90.90.91 – IP из другой сети, отличной от той, что сконфигурирована на слушающимся интерфейсе (например, для доступа к комуникатору), то можно добавить эту сеть в настройках **/etc/sysconfig/arpwatch**, что бы не мусорило в логах и перегрузить сервис:

```
-n 10.90.90.0/24
```

Источники:

- https://blog.trebacz.com/2015/12/update-arpwatch-ethercodes-dat-file-ubuntu.html
- http://muff.kiev.ua/content/arpwatch-sledim-za-novymi-ustroistvami-v-seti