Installation arpwatch

MAC watcher

19th of October 2000

Document name:	Installation-arpwatch-V1.0.pdf
Version:	V 1.0
Author:	Ivan Buetler, Compass Security AG
	ivan.buetler@csnc.ch
	http://www.csnc.ch/
References:	README distribution
Date of delivery:	19th of October 2000
Document state:	PUBLIC

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

CONTENT

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

1 Installation

1.1 Introduction

Arpwatch watches for MAC addresses within your ip segment. The very first time you start Arpwatch, it will collect all arp packets from your network in arp.dat. If there appear any new MAC addresses within your local ip segment, arpwatch will send root an e-mail. Arpwatche helps you to monitor network interfaces within the DMZ. MAC spoofing attacks are also detectable by arpwatch.

1.2 Version control

Version	Author	Description	Filename
1.0	Ivan Buetler ivan.buetler@csnc.ch	Initial version saved on http://www.csnc.ch/download/	Installation-arpwatch-V1.0.pdf

[Ivan] If you feel like having something you would like to see in this document, pls. Let me know. I will leave the version control chapter in the future. So everybody can see who did what on this document.

1.3 Download source

Download tripwire from:

ftp://ftp.ee.lbl.gov/arpwatch.tar.Z

1.4 Software requirements

For successful compilation of arpwatch, libpcap is needed. Checkout README at 2.1.

1.5 Copy the source to /opt/download

Compass recommends to copy or move all sources to the /opt/download directory. After the successfully compilation and installation, the sources goes to /opt/installed directory. If the Solaris Administrator wants to check weather a package is already installed or not, he can use the traditional pkginfo (Solaris packages) and the list of /opt/installed to check versions of installed packages.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

1.6 Unpack the source

gzip -d arpwatch.tar.Z
tar –xvf arpwatch.tar

This will untar the sources into /opt/download/arpwatch directory

1.7 Who will get the e-mails

Configure addresses.h.in for your needs. In its default configuration you have:

```
#define WATCHER "root"
#define WATCHEE "arpwatch (Arpwatch)"
```

This will send the mails to the local root account. You can specify whatever you want to send e-mails to, as far as sendmail is able to transport the e-mail.

1.8 Configure software

Cd /opt/download/arpwatch
./configure
./make
./make install

```
quala:arpwatch-2.1a6# ./configure
loading cache ./config.cache
checking host system type... sparc-sun-solaris2.6
checking target system type... sparc-sun-solaris2.6
checking build system type... sparc-sun-solaris2.6
checking for gcc... (cached) gcc
checking whether the C compiler (gcc  ) works... yes
checking whether the C compiler (gcc  ) is a cross-compiler... no
checking whether we are using GNU C... (cached) yes
checking whether gcc accepts -g... (cached) yes
checking how to run the C preprocessor... (cached) gcc -E
checking for fcntl.h... (cached) yes
checking for memory.h... (cached) yes
checking whether time.h and sys/time.h may both be included... (cached) yes
checking for dn_skipname... (cached) no
checking for bcopy... (cached) yes
checking for strerror... (cached) yes
checking whether byte ordering is bigendian... (cached) yes
checking return type of signal handlers... (cached) void
checking for sigset... (cached) yes
checking if union wait is used... (cached) no
checking for _res... (cached) no
checking for _res in -lresolv... (cached) yes
checking for gethostbyname... (cached) no
checking for gethostbyname in -lnsl... (cached) yes
checking for socket... (cached) no
checking for socket in -lsocket... (cached) yes
checking for putmsg in -lstr... (cached) no
checking for local pcap library... ../libpcap-0.4/libpcap.a
checking for sendmail... (cached) /usr/lib/sendmail
checking for ANSI C header files... (cached) no
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

```
checking for int32_t... (cached) yes
checking for u_int32_t... (cached) no
checking if ether_header uses ether_addr structs... (cached) yes
checking if ether_arp uses ether_addr structs... (cached) no
checking if ether_arp uses erp_xsha member... (cached) no
checking for a BSD compatible install... ./install-sh -c
creating ./config.status
creating Makefile
quala:arpwatch-2.1a6# make
gcc -O -DDEBUG  -DHAVE_FCNTL_H=1 -DHAVE_MEMORY_H=1 -DTIME_WITH_SYS_TIME=1 -DHAVE_BCOPY=1 -
DHAVE_STRERROR=1 -DWORDS_BIGENDIAN=1 -DRETSIGTYPE=void -DRETSIGVAL= -DHAVE_SIGSET=1 -
Dsignal=sigset -DDECLWAITSTATUS=int -DHAVE_LIBRESOLV=1 -DHAVE_LIBNSL=1 -DHAVE_LIBSOCKET=1 -
Du_int32_t=u_int -DETHER_HEADER_HAS_EA=1  -DARPDIR=\"/usr/local/arpwatch\" -
DPATH_SENDMAIL=\"/usr/lib/sendmail\" -I. -I../libpcap-0.4  -c ./arpwatch.c
gcc -O -DDEBUG  -DHAVE_FCNTL_H=1 -DHAVE_MEMORY_H=1 -DTIME_WITH_SYS_TIME=1 -DHAVE_BCOPY=1 -
DHAVE_STRERROR=1 -DWORDS_BIGENDIAN=1 -DRETSIGTYPE=void -DRETSIGVAL= -DHAVE_SIGSET=1 -
Dsignal=sigset -DDECLWAITSTATUS=int -DHAVE_LIBRESOLV=1 -DHAVE_LIBNSL=1 -DHAVE_LIBSOCKET=1 -
Du_int32_t=u_int -DETHER_HEADER_HAS_EA=1  -DARPDIR=\"/usr/local/arpwatch\" -
DPATH_SENDMAIL=\"/usr/lib/sendmail\" -I. -I../libpcap-0.4  -c ./db.c
gcc -O -DDEBUG  -DHAVE_FCNTL_H=1 -DHAVE_MEMORY_H=1 -DTIME_WITH_SYS_TIME=1 -DHAVE_BCOPY=1 -
DHAVE_STRERROR=1 -DWORDS_BIGENDIAN=1 -DRETSIGTYPE=void -DRETSIGVAL= -DHAVE_SIGSET=1 -
Dsignal=sigset -DDECLWAITSTATUS=int -DHAVE_LIBRESOLV=1 -DHAVE_LIBNSL=1 -DHAVE_LIBSOCKET=1 -
Du_int32_t=u_int -DETHER_HEADER_HAS_EA=1  -DARPDIR=\"/usr/local/arpwatch\" -
DPATH_SENDMAIL=\"/usr/lib/sendmail\" -I. -I../libpcap-0.4  -c ./dns.c
gcc -O -DDEBUG  -DHAVE_FCNTL_H=1 -DHAVE_MEMORY_H=1 -DTIME_WITH_SYS_TIME=1 -DHAVE_BCOPY=1 -
DHAVE_STRERROR=1 -DWORDS_BIGENDIAN=1 -DRETSIGTYPE=void -DRETSIGVAL= -DHAVE_SIGSET=1 -
Dsignal=sigset -DDECLWAITSTATUS=int -DHAVE_LIBRESOLV=1 -DHAVE_LIBNSL=1 -DHAVE_LIBSOCKET=1 -
Du_int32_t=u_int -DETHER_HEADER_HAS_EA=1  -DARPDIR=\"/usr/local/arpwatch\" -
DPATH_SENDMAIL=\"/usr/lib/sendmail\" -I. -I../libpcap-0.4  -c ./ec.c
gcc -O -DDEBUG  -DHAVE_FCNTL_H=1 -DHAVE_MEMORY_H=1 -DTIME_WITH_SYS_TIME=1 -DHAVE_BCOPY=1 -
DHAVE_STRERROR=1 -DWORDS_BIGENDIAN=1 -DRETSIGTYPE=void -DRETSIGVAL= -DHAVE_SIGSET=1 -
Dsignal=sigset -DDECLWAITSTATUS=int -DHAVE_LIBRESOLV=1 -DHAVE_LIBNSL=1 -DHAVE_LIBSOCKET=1 -
Du_int32_t=u_int -DETHER_HEADER_HAS_EA=1  -DARPDIR=\"/usr/local/arpwatch\" -
DPATH_SENDMAIL=\"/usr/lib/sendmail\" -I. -I../libpcap-0.4  -c ./file.c
gcc -O -DDEBUG  -DHAVE_FCNTL_H=1 -DHAVE_MEMORY_H=1 -DTIME_WITH_SYS_TIME=1 -DHAVE_BCOPY=1 -
DHAVE_STRERROR=1 -DWORDS_BIGENDIAN=1 -DRETSIGTYPE=void -DRETSIGVAL= -DHAVE_SIGSET=1 -
Dsignal=sigset -DDECLWAITSTATUS=int -DHAVE_LIBRESOLV=1 -DHAVE_LIBNSL=1 -DHAVE_LIBSOCKET=1 -
Du_int32_t=u_int -DETHER_HEADER_HAS_EA=1  -DARPDIR=\"/usr/local/arpwatch\" -
DPATH_SENDMAIL=\"/usr/lib/sendmail\" -I. -I../libpcap-0.4  -c ./intoa.c
gcc -O -DDEBUG  -DHAVE_FCNTL_H=1 -DHAVE_MEMORY_H=1 -DTIME_WITH_SYS_TIME=1 -DHAVE_BCOPY=1 -
DHAVE_STRERROR=1 -DWORDS_BIGENDIAN=1 -DRETSIGTYPE=void -DRETSIGVAL= -DHAVE_SIGSET=1 -
Dsignal=sigset -DDECLWAITSTATUS=int -DHAVE_LIBRESOLV=1 -DHAVE_LIBNSL=1 -DHAVE_LIBSOCKET=1 -
Du_int32_t=u_int -DETHER_HEADER_HAS_EA=1  -DARPDIR=\"/usr/local/arpwatch\" -
DPATH_SENDMAIL=\"/usr/lib/sendmail\" -I. -I../libpcap-0.4  -c ./machdep.c
gcc -O -DDEBUG  -DHAVE_FCNTL_H=1 -DHAVE_MEMORY_H=1 -DTIME_WITH_SYS_TIME=1 -DHAVE_BCOPY=1 -
DHAVE_STRERROR=1 -DWORDS_BIGENDIAN=1 -DRETSIGTYPE=void -DRETSIGVAL= -DHAVE_SIGSET=1 -
Dsignal=sigset -DDECLWAITSTATUS=int -DHAVE_LIBRESOLV=1 -DHAVE_LIBNSL=1 -DHAVE_LIBSOCKET=1 -
Du_int32_t=u_int -DETHER_HEADER_HAS_EA=1  -DARPDIR=\"/usr/local/arpwatch\" -
DPATH_SENDMAIL=\"/usr/lib/sendmail\" -I. -I../libpcap-0.4  -c ./util.c
gcc -O -DDEBUG  -DHAVE_FCNTL_H=1 -DHAVE_MEMORY_H=1 -DTIME_WITH_SYS_TIME=1 -DHAVE_BCOPY=1 -
DHAVE_STRERROR=1 -DWORDS_BIGENDIAN=1 -DRETSIGTYPE=void -DRETSIGVAL= -DHAVE_SIGSET=1 -
Dsignal=sigset -DDECLWAITSTATUS=int -DHAVE_LIBRESOLV=1 -DHAVE_LIBNSL=1 -DHAVE_LIBSOCKET=1 -
Du_int32_t=u_int -DETHER_HEADER_HAS_EA=1  -DARPDIR=\"/usr/local/arpwatch\" -
DPATH_SENDMAIL=\"/usr/lib/sendmail\" -I. -I../libpcap-0.4  -c ./report.c
gcc -O -DDEBUG  -DHAVE_FCNTL_H=1 -DHAVE_MEMORY_H=1 -DTIME_WITH_SYS_TIME=1 -DHAVE_BCOPY=1 -
DHAVE_STRERROR=1 -DWORDS_BIGENDIAN=1 -DRETSIGTYPE=void -DRETSIGVAL= -DHAVE_SIGSET=1 -
Dsignal=sigset -DDECLWAITSTATUS=int -DHAVE_LIBRESOLV=1 -DHAVE_LIBNSL=1 -DHAVE_LIBSOCKET=1 -
Du_int32_t=u_int -DETHER_HEADER_HAS_EA=1  -DARPDIR=\"/usr/local/arpwatch\" -
DPATH_SENDMAIL=\"/usr/lib/sendmail\" -I. -I../libpcap-0.4  -c ./setsignal.c
sed -e 's/.*/char version[] = "&";/' ./VERSION > version.c
gcc -O -DDEBUG  -DHAVE_FCNTL_H=1 -DHAVE_MEMORY_H=1 -DTIME_WITH_SYS_TIME=1 -DHAVE_BCOPY=1 -
DHAVE_STRERROR=1 -DWORDS_BIGENDIAN=1 -DRETSIGTYPE=void -DRETSIGVAL= -DHAVE_SIGSET=1 -
Dsignal=sigset -DDECLWAITSTATUS=int -DHAVE_LIBRESOLV=1 -DHAVE_LIBNSL=1 -DHAVE_LIBSOCKET=1 -
Du_int32_t=u_int -DETHER_HEADER_HAS_EA=1  -DARPDIR=\"/usr/local/arpwatch\" -
DPATH_SENDMAIL=\"/usr/lib/sendmail\" -I. -I../libpcap-0.4  -c ./version.c
gcc -O -DDEBUG  -DHAVE_FCNTL_H=1 -DHAVE_MEMORY_H=1 -DTIME_WITH_SYS_TIME=1 -DHAVE_BCOPY=1 -
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

```
DHAVE_STRERROR=1 -DWORDS_BIGENDIAN=1 -DRETSIGTYPE=void -DRETSIGVAL= -DHAVE_SIGSET=1 -
Dsignal=sigset -DDECLWAITSTATUS=int -DHAVE_LIBRESOLV=1 -DHAVE_LIBNSL=1 -DHAVE_LIBSOCKET=1 -
Du_int32_t=u_int -DETHER_HEADER_HAS_EA=1  -DARPDIR=\"/usr/local/arpwatch\" -
DPATH_SENDMAIL=\"/usr/lib/sendmail\" -I. -I../libpcap-0.4  -o arpwatch arpwatch.o db.o dns.o ec.o file.o intoa.o machdep.o
util.o report.o setsignal.o version.o  ../libpcap-0.4/libpcap.a -lsocket -lnsl -lresolv
gcc -O -DDEBUG  -DHAVE_FCNTL_H=1 -DHAVE_MEMORY_H=1 -DTIME_WITH_SYS_TIME=1 -DHAVE_BCOPY=1 -
DHAVE_STRERROR=1 -DWORDS_BIGENDIAN=1 -DRETSIGTYPE=void -DRETSIGVAL= -DHAVE_SIGSET=1 -
Dsignal=sigset -DDECLWAITSTATUS=int -DHAVE_LIBRESOLV=1 -DHAVE_LIBNSL=1 -DHAVE_LIBSOCKET=1 -
Du_int32_t=u_int -DETHER_HEADER_HAS_EA=1  -DARPDIR=\"/usr/local/arpwatch\" -
DPATH_SENDMAIL=\"/usr/lib/sendmail\" -I. -I../libpcap-0.4  -c ./arpsnmp.c
gcc -O -DDEBUG  -DHAVE_FCNTL_H=1 -DHAVE_MEMORY_H=1 -DTIME_WITH_SYS_TIME=1 -DHAVE_BCOPY=1 -
DHAVE_STRERROR=1 -DWORDS_BIGENDIAN=1 -DRETSIGTYPE=void -DRETSIGVAL= -DHAVE_SIGSET=1 -
Dsignal=sigset -DDECLWAITSTATUS=int -DHAVE_LIBRESOLV=1 -DHAVE_LIBNSL=1 -DHAVE_LIBSOCKET=1 -
Du_int32_t=u_int -DETHER_HEADER_HAS_EA=1  -DARPDIR=\"/usr/local/arpwatch\" -
DPATH_SENDMAIL=\"/usr/lib/sendmail\" -I. -I../libpcap-0.4  -o arpsnmp arpsnmp.o db.o dns.o ec.o file.o intoa.o machdep.o
util.o report.o setsignal.o version.o  -lsocket -lnsl -lresolv
quala:arpwatch-2.1a6# make install
./install-sh -c -m 555 -o bin -g bin arpwatch /usr/local/sbin
./install-sh -c -m 555 -o bin -g bin arpsnmp /usr/local/sbin
quala:arpwatch-2.1a6#
```

1.9 ARPWATCH example-email

```
quala:arpwatch-2.1a6# mailx
mailx version 5.0 Tue Jul 15 21:29:48 PDT 1997  Type ? for help.
"/var/mail/root": 94 messages 3 new 94 unread
 U 91 Super-User         Tue Sep 12 16:03 3758/397594
>N 92 Super-User          Wed Sep 13 06:03 3762/397832
 N 93 Arpwatch           Wed Sep 13 08:00   17/509   new station (quala)
 N 94 Super-User         Wed Sep 13 09:48   14/367   Message from Swatch
? 93
Message 93:
From root Wed Sep 13 08:00:58 2000
Date: Wed, 13 Sep 2000 08:00:58 +0200
From: arpwatch (Arpwatch)
To: root
Subject: new station (quala)

          hostname: quala
        ip address: 192.168.100.202
   ethernet address: 8:0:20:f2:7d:7b
    ethernet vendor: <unknown>
         timestamp: Wednesday, September 13, 2000 8:00:57 +0200

?
```

1.10 Good to know

arpwatch has a mac reference database. You will be able to identify vendors according to the mac addresses. Check out the file:

ethercodes.dat

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

1.11 Start arpwatch at boot-time

```
quala:rc3.d# ls -al
total 24
drwxrwxr-x   2 root     sys          512 Sep  7 14:47 .
drwxr-xr-x  27 root     sys         3584 Sep 13 20:25 ..
-rw-r--r--   1 root     sys         1708 Jul 16  1997 README
lrwxrwxrwx   1 root     other         20 Sep  7 11:48 S00umask.sh -> /etc/init.d/umask.sh
-rwxr--r--   5 root     sys         1738 Jul 16  1997 S15nfs.server
-rwxr-xr-x   1 root     other        320 Sep  6 13:28 S26arpwatch
-rwxr-xr-x   3 root     sys          677 Jul 16  1997 S76snmpdx
quala:rc3.d#
```

```
quala:rc3.d# cat S26arpwatch
#!/bin/sh
# ident @(#)netra.postboot      1.3     96/02/02 SMI
# Copyright 1995 Sun Microsystems, Inc. All Rights Reserved

#
# Script to be run when system finishes booting, recommended at level S99.
#
if [ "$1" = "stop" ]; then
        exit
fi

CMD=/usr/local/sbin/arpwatch

if [ -x $CMD ]; then
        $CMD -f /var/adm/arpwatch/arp.dat
fi
quala:rc3.d#
```

1.12 Clean-up Installation

Compass recommends to tar the already running distribution and move it to /opt/installed directory.

cd /opt/download/arpwatch
tar –cvpf arpwatch-compiled.tar *
mv ./arpwatch-compiled.tar /opt/installed

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

2 Appendix

2.1 README

quala:arpwatch-2.1a6# more README
@(#) $Header: README,v 1.20 97/09/30 14:46:55 leres Exp $ (LBL)

ARPWATCH 2.1
Lawrence Berkeley National Laboratory
Network Research Group
arpwatch@ee.lbl.gov
ftp://ftp.ee.lbl.gov/arpwatch.tar.Z

This directory contains source code for arpwatch and arpsnmp, tools that monitors ethernet or fddi activity and maintain a database of ethernet/ip address pairings. It also reports certain changes via email.

Arpwatch uses libpcap, a system-independent interface for user-level packet capture. Before building arpwatch, you must first retrieve and build libpcap, also from LBL, in:

ftp://ftp.ee.lbl.gov/libpcap.tar.Z.

Once libpcap is built (either install it or make sure arpwatch and libpcap share the same parent directory), you can build arpwatch using the procedure in the INSTALL file.

Arpsnmp has the same database features of arpwatch but relies on an external agent to collect the arp data. This distribution contains a script, arpfetch, that uses snmpwalk from the CMU SNMP package. This package is available from:

ftp://ftp.net.cmu.edu/pub/snmp-dist/cmu-snmp*.tar.Z

It should be trivial to adaptive the output of any snmp query program for use with arpsnmp.

The ethernet vendor codes come from:

ftp://ftp.cavebear.com/pub/Ethernet.txt
http://www.cavebear.com/CaveBear/Ethernet/vendor.html

Another source of ethernet vendor code data is:

http://standards.ieee.org/db/oui/

However that version is copyrighted.

Please send bugs and comments to arpwatch@ee.lbl.gov.