NAME

ipmon - monitors /dev/ipl for logged packets

SYNOPSIS

ipmon [**-abBDFhnpstvxX**] [**-B <binarylogfile>**] [**-C <configfile>**] [**-N <device>**] [**-L <facility>**] [**-o [NSI]**] [**-O [NSI]**] [**-P <pidfile>**] [**-S <device>**] [**-f <device>**] [**<filename>**]

DESCRIPTION

ipmon opens **/dev/ipl** for reading and awaits data to be saved from the packet filter. The binary data read from the device is reprinted in human readable form, however, IP#'s are not mapped back to hostnames, nor are ports mapped back to service names. The output goes to standard output by default or a filename, if given on the command line. Should the **-s** option be used, output is instead sent to **syslogd(8)**. Messages sent via syslog have the day, month and year removed from the message, but the time (including microseconds), as recorded in the log, is still included.

Messages generated by ipmon consist of whitespace separated fields. Fields common to all messages are:

1. The date of packet receipt. This is suppressed when the message is sent to syslog.

2. The time of packet receipt. This is in the form HH:MM:SS.F, for hours, minutes seconds, and fractions of a second (which can be several digits long).

3. The name of the interface the packet was processed on, e.g., **we1**.

4. The group and rule number of the rule, e.g., **@0:17**. These can be viewed with **ipfstat -n**.

5. The action: **p** for passed, **b** for blocked, for a short packet, **n** did not match any rules or **L** for a log rule.

6. The addresses. This is actually three fields: the source address and port (separated by a comma), the -> symbol, and the destination address and port. E.g.: **209.53.17.22,80 -> 198.73.220.17,1722**.

7. **PR** followed by the protocol name or number, e.g., **PR tcp**.

8. **len** followed by the header length and total length of the packet, e.g., **len 20 40**.

If the packet is a TCP packet, there will be an additional field starting with a hyphen followed by letters corresponding to any flags that were set. See the ipf.conf manual page for a list of letters and their flags.

If the packet is an ICMP packet, there will be two fields at the end, the first always being 'icmp', and the next being the ICMP message and submessage type, separated by a slash, e.g., **icmp 3/3** for a port unreachable message.

In order for **ipmon** to properly work, the kernel option **IPFILTER_LOG** must be turned on in your kernel. Please see **options(4)** for more details.

ipmon reopens its log file(s) and rereads its configuration file when it receives a SIGHUP signal.

OPTIONS

-a Open all of the device logfiles for reading log entries from. All entries are displayed to the same output 'device' (stderr or syslog).

-b For rules which log the body of a packet, generate hex output representing the packet contents after the headers.

-B <binarylogfilename>
Enable logging of the raw, unformatted binary data to the specified <*binarylogfilename*> file. This can be read, later, using **ipmon** with the **-f** option.

-C <configfilename>
This option specifies a file to be used to specify optional extra actions when it sees specific log entries from the kernel.

-D Cause ipmon to turn itself into a daemon. Using subshells or backgrounding of ipmon is not required to turn it into an orphan so it can run indefinitely.

-f <device>
specify an alternative device/file from which to read the log information for normal IP Filter log records.

-F Flush the current packet log buffer. The number of bytes flushed is displayed, even should the result be zero.

-L <facility>
Using this option allows you to change the default syslog facility that ipmon uses for syslog messages. The default is local0.

-n IP addresses and port numbers will be mapped, where possible, back into hostnames and service names.

-N <device>
Set the logfile to be opened for reading NAT log records from to <device>.

-o Specify which log files to actually read data from. N - NAT logfile, S - State logfile, I - normal IP Filter logfile. The **-a** option is equivalent to using **-o NSI**.

-O Specify which log files you do not wish to read from. This is most sensibly used with the **-a**. Letters available as parameters to this are the same as for **-o**.

-p Cause the port number in log messages to always be printed as a number and never attempt to look it up as from */etc/services*, etc.

-P <pidfile>
Write the pid of the ipmon process to a file. By default this is *//etc/opt/ipf/ipmon.pid* (Solaris), */var/run/ipmon.pid* (44BSD or later) or */etc/ipmon.pid* for all others.

-s Packet information read in will be sent through syslogd rather than saved to a file. The default facility when compiled and installed is **security**. The following levels are used:

LOG_INFO - packets logged using the "log" keyword as the action rather than pass or block.

LOG_NOTICE - packets logged which are also passed

LOG_WARNING - packets logged which are also blocked

LOG_ERR - packets which have been logged and which can be considered "short".

-S <device>
Set the logfile to be opened for reading state log records from to <device>.

-t read the input file/device in a manner akin to tail(1).

-v show tcp window, ack and sequence fields.

-x show the packet data in hex.

-X show the log header record data in hex.

DIAGNOSTICS

ipmon expects data that it reads to be consistent with how it should be saved and will abort if it fails an

assertion which detects an anomaly in the recorded data.

FILES

/dev/ipl
/dev/ipnat
/dev/ipstate
/etc/ipmon.conf
/etc/services

SEE ALSO

ipl(4), ipmon(5), ipf(8), ipfstat(8), ipnat(8)

BUGS

If you find any, please send email to me at darrenr@pobox.com