NAME

dpa - DNS Packet Analyzer. Analyze DNS packets in ip trace files

SYNOPSIS

dpa [*OPTION*] *TRACEFILE*

DESCRIPTION

dpa is used to analyze dns packets in trace files. It has 3 main options: count, filter, and count uniques (i.e. count all different occurrences).

OPTIONS

-c *expressionlist*

Count occurrences of matching expressions

-f *expression*

Filter: only process packets that match the expression

-h Show usage

-p Show the total number of correct DNS packets, and percentage of -u and -c values (of the total of matching on the -f filter. if no filter is given, percentages are on all correct dns packets)

-of *file*

Write all packets that match the -f flag to file, as pcap data.

-ofh *file*

Write all packets that match the -f flag to file, in hexadecimal format, readable by drill.

-s Show possible match names

-s *matchname*

show possible match operators and values for name

-sf Only evaluate packets (in representation format) that match the -f filter. If no -f was given, evaluate all correct dns packets.

-u *matchnamelist*
Count every occurrence of every value of the matchname (for instance, count all packetsizes, see EXAMPLES in ldns-dpa(1)).

-ua For every matchname in -u, show the average value of all matches. Behaviour for match types that do not have an integer value is undefined.

-uac
For every matchname in -u, show the average number of times this value was encountered.

-um *number*
Only show the results from -u for values that occurred more than <number> times.

-v *level*
Set verbosity to level (1-5, 5 being the highest). Mostly used for debugging.

-notip *file*
Write packets that were not recognized as IP packets to file (as pcap data).

-baddns *file*
Write dns packets that were too mangled to parse to file (as pcap data).

-version
Show version and exit

LIST AND MATCHES

A <matchnamelist> is a comma separated list of match names (use -s to see possible match names). A <expressionlist> is a comma separated list of expressions.

An expression has the following form: <expr>: (<expr>)

<expr> | <expr>

<expr> & <expr>

<match>

<match>: <matchname> <operator> <value>

<operator>: = equal to <value> != not equal to <value> > greater than <value> < lesser than <value> >= greater than or equal to <value> <= lesser than or equal to <value> ~= contains <value>

See the -s option for possible matchnames, operators and values.

EXAMPLES

ldns-dpa -u packetsize -p test.tr

Count all different packetsizes in test.tr and show the percentages.

ldns-dpa -f "edns=1&qr=0" -of edns.tr test.tr

Filter out all edns enable queries in test.tr and put them in edns.tr

ldns-dpa -f edns=1 -c tc=1 -u rcode test.tr

For all edns packets, count the number of truncated packets and all their rcodes in test.tr.

ldns-dpa -c tc=1,qr=0,qr=1,opcode=QUERY test.tr

For all packets, count the number of truncated packets, the number of packets with qr=0, the number of packets with qr=1 and the number of queries in test.tr.

ldns-dpa -u packetsize -ua test.tr

Show all packet sizes and the average packet size per packet.

ldns-dpa -u srcaddress -uac test.tr
Show all packet source addresses and the average number of packets sent from this address.

sudo tcpdump -i eth0 -s 0 -U -w - port 53 | ldns-dpa -f qr=0 -sf
Print all query packets seen on the specified interface.

AUTHOR

Written by Jelte Jansen for NLnetLabs.

REPORTING BUGS

Report bugs to <dns-team@nlnetlabs.nl>.

COPYRIGHT