NAME

etterlog – Log analyzer for ettercap log files

SYNOPSIS

etterlog [*OPTIONS*] *FILE*

DESCRIPTION

Etterlog is the log analyzer for logfiles created by ettercap. It can handle both compressed (created with –Lc) or uncompressed logfiles. With this tool you can manipulate binary files as you like and you can print data in different ways all the times you want (in contrast with the previous logging system which was used to dump in a single static manner).
You will be able to dump traffic from only one connection of your choice, from only one or more hosts, print data in hex, ascii, binary etc...

TIP: All non-useful messages are printed to stderr, so you can save the output from etterlog with the following command:

etterlog [options] logfile > outfile

Thus you can dump for example a binary file from an ftp connection if you print the data in binary mode, without headers and selecting only the ftp server as the source of the communication.

GENERAL OPTIONS

–a, **––analyze**

Analyze a log file and display some interesting statistics.

–c, **––connections**

Parse the log file and print a table of unique connections (port to port). This option can be used only on LOG_PACKET logfiles. On LOG_INFO logfiles it is useless.

TIP: you can search for a particular host by using the following command:

etterlog –c logfile.ecp | grep 10.0.0.1

–f, **––filter <TARGET>**

Print only packets coming from or going to TARGET. The TARGET specification is the same as in ettercap.
TARGET is in the form *MAC/IPs/PORTs*. With IPv6 support enabled, *TARGET* is in the form *MAC/IPs/IPv6/PORTs*. Omitting one or more of its parts will be equivalent to set them to ANY. IPs and IPv6 will be treated as one part so that it's only set to ANY if both IPs and IPv6 is omitted. This concludes in a result most users would expect.

If the log type is LOG_INFO the target is used to display hosts matching the mac, ip and having the specified port(s) open. For example the target //80 will display only information about hosts with a running web server.

–r, **––reverse**

Reverse the matching in the TARGET selection. It means not(TARGET). All but the selected TARGET.

–t, **––proto <PROTO>**

Sniff only PROTO packets (default is TCP + UDP). This option is only useful in "simple" mode. If you start ettercap in interactive mode both TCP and UDP are sniffed.

PROTO can be "tcp", "udp" or "all" for both.

–F, ––filcon <CONNECTION>
Print packets belonging only to this CONNECTION.
CONNECTION is in the form PROTO:SOURCE:DEST. SOURCE and DEST are in the form IP:PORT.

example:

etterlog –F TCP:10.0.0.23:3318:198.182.196.56:80

–s, ––only–source
Display only packets that are sent by the source of the selected CONNECTION. This option makes sense only in conjunction with the –F option.

TIP: if you want to save a file transferred in an HTTP or FTP connection, you can use the following command:

etterlog –B –s –n –F TCP:10.0.0.1:20:10.0.0.2:35426 logfile.ecp > example.tar.gz

–d, ––only–dest
Same as ––only–source but it filters on the destination host.

–n, ––no–headers
Do not print the header of each packet. This option is useful if you want to save a file in binary format (–B option). Without the headers you can redirect the output to a file and you will get the original stream.

NOTE: the time stamp in the header is in the form: Thu Mar 27 23:03:31 2003 [169396], the value in the square brackets is expressed in microseconds

–m, ––show–mac
In the headers show also the mac addresses corresponding to the ip addresses.

–k, ––color
If used in conjunction with –F it displays the source and dest of the connection using different colors. If used with a LOG_INFO file it prints LAN hosts in green, REMOTE hosts in blue and GATEWAYS in red.

–l, ––only–local
Used displaying an INFO file, it displays information only about local hosts.

–L, ––only–remote
Used displaying an INFO file, it displays information only about remote hosts.

SEARCH OPTIONS

–e, ––regex <REGEX>
Display only packets matching the regex <REGEX>.
If this option is used agains a LOG_PACKET logfile, the regex is executed on the payload of the

packet. If the type is LOG_INFO, the regex is executed on all the fields of the host profile (OS, banners, service and ethernet adapter).
NOTE: the regex is compiled with the REG_ICASE flag (case insensitive).

−u, −−user <USER>
Display information about this user. The search is performed over all the user/pass couples collected across all hosts.

−p, −−passwords
Print only the collected account information for each host. This prevents the huge profile output. It can be used in conjunction with the −u option to filter the users. An asterisk '*' used in front of an account represents a failed login attempt.

−i, −−show−client
Show the client ip address when displaying the collected users and passwords. It may be useful when ACLs are in place.

−I, −−client <IP>
Show passwords only coming from a specific <IP>. This is useful to view all the usernames and passwords of a client.

EDITING OPTIONS

−C, −−concat
Use this option to concatenate two (or more) files into one single file. This is useful if you have collected ettercap log files from multiple sources and want to have an unified report. The output file must be specified with the −o option and the input files are listed as normal arguments.

example:
etterlog −C −o outfile input1 input2 input3

−o, −−outfile <FILE>
specifies the output file for a concatenation.

VISUALIZATION METHOD

−B, −−binary
Print data as they are, in binary form. Useful to dump binary data to a file (as described above).

−X, −−hex
Print the packets in hex format.

example:

the string "HTTP/1.1 304 Not Modified" becomes:

```
0000: 4854 5450 2f31 2e31 2033 3034 204e 6f74  HTTP/1.1 304 Not
0010: 204d 6f64 6966 6965 64                   Modified
```

–A, **––ascii**
Print only "printable" characters, the others are displayed as dots '.'

–T, **––text**
Print only the "printable" characters and skip the others.

–E, **––ebcdic**
Convert an EBCDIC text to ASCII.

–H, **––html**
Strip all html tags from the text. A tag is every string between '<' and '>'.

example:

<title>This is the title</title>, but the following <string> will not be displayed.

This is the title, but the following will not be displayed.

–U, **––utf8 <encoding>**
Print the packets in UTF-8 format. The <encoding> parameter specifies the encoding to be used while performing the conversion. Use the 'iconv ––list' command to obtain a list of all supported encodings.

–Z, **––zero**
Print always the void string. i.e. print only header information and no packet content will be printed.

–x, **––xml**
Print the host information in xml form, so you can parse it with your favourite program.

The DTD associated with the xml output is in share/etterlog.dtd

STANDARD OPTIONS

–v, **––version**
Print the version and exit.

–h, **––help**
Print the help screen with a short summary of the available options.

EXAMPLES

Here are some examples of using etterlog.

etterlog –k –l dump.eci

Displays information about local hosts in different colors.

etterlog –X dump.ecp

Prints packets in HEX mode with full headers.

etterlog –c dump.ecp

Displays the list of connections logged in the file.

etterlog –Akn –F TCP:10.0.0.1:13423:213.203.143.52:6666 dump.ecp

Displays the IRC traffic made by 10.0.0.1 in ASCII mode, without headers information and in colored mode.

etterlog –H –t tcp –f //80 dump.ecp

Dumps all HTTP traffic and strips html tags.

etterlog –Z –r –f /10.0.0.2/22 dump.ecp

Displays only the headers of all connections except ssh on host 10.0.0.2

etterlog –A –e 'user' –f //110 dump.ecp

Displays only POP packets containing the 'user' regexp (case insensitive).

etterlog –u root dump.eci

Displays information about all the accounts of the user 'root'.

etterlog –e Apache dump.eci

Displays information about all the hosts running 'Apache'.

etterlog –e Linux dump.eci

Displays information about all the hosts with the 'Linux' operating system.

etterlog –t tcp –f //110 dump.eci

Displays information about all the hosts with the tcp port 110 open.

etterlog –t udp dump.eci

Displays information about all the hosts with at least one UDP port open.

etterlog –B –s –n –F TCP:10.0.0.1:20:10.0.0.2:35426 logfile.ecp > example.tar.gz

Dumps in binary form the data sent by 10.0.0.1 over the data port of FTP. Since the headers are omitted, you will get the file as it was.

ORIGINAL AUTHORS

Alberto Ornaghi (ALoR) <alor@users.sf.net>
Marco Valleri (NaGA) <naga@antifork.org>

PROJECT STEWARDS

Emilio Escobar (exfil) <eescobar@gmail.com>
Eric Milam (Brav0Hax) <jbrav.hax@gmail.com>

OFFICIAL DEVELOPERS

Mike Ryan (justfalter) <falter@gmail.com>
Gianfranco Costamagna (LocutusOfBorg) <costamagnagianfranco@yahoo.it>
Antonio Collarino (sniper) <anto.collarino@gmail.com>
Ryan Linn <sussuro@happypacket.net>
Jacob Baines <baines.jacob@gmail.com>

CONTRIBUTORS

Dhiru Kholia (kholia) <dhiru@openwall.com>
Alexander Koeppe (koeppea) <format_c@online.de>
Martin Bos (PureHate) <purehate@backtrack.com>
Enrique Sanchez
Gisle Vanem <giva@bgnett.no>
Johannes Bauer <JohannesBauer@gmx.de>
Daten (Bryan Schneiders) <daten@dnetc.org>

SEE ALSO

ettercap(8) etterfilter(8) etter.conf(5) ettercap_curses(8) ettercap_plugins(8) ettercap−pkexec(8)