NAME

ettercap - Man page for the Ncurses GUI.

GENERAL DESCRIPTION

The curses GUI is quite simple and intuitive.
It is menu-driven. Every flag or function can be modified/called through the upper menu. All user messages are printed in the bottom window. If you want to see the old messages, you can scroll the window buffer by pressing the UP, DOWN, PPAGE, NPAGE keys. The middle part is used to display information or dialogs for the user.

The menus can be opened by pressing the relative hotkey. For the menus the hotkey is represented by the uppercase initial letter of the title (e.g. 'S' for Sniffing, 'T' for Targets). The functions within a menu can be called by pressing the hotkey depicted near the function name on the right. Hotkeys prefixed with 'C-' are to be used in conjunction with the CTRL key (e.g. 'C-f' means CTRL+f).

You can switch the focus between the objects on the screen by pressing the TAB key or by clicking on it with the mouse (if you are running ettercap within an xterm). Mouse events are supported only through the xterm. You can use the mouse to select objects, open a menu, choose a function, scroll the elevators for the scrolling windows, etc etc.

When you open multiple windows in the middle part, they will overlap. Use the TAB key to switch between them. Use CTRL+Q to close the focused window.
You can also use CTRL+Q to close the input dialog if you want to cancel the requested input. (i.e. you have selected the wrong function and you want to go back).

To have a quick help on the shortcuts you can use against a particular window press the SPACE key. A help window will be displayed with a list of shortcuts that can be used. If the window does not appear, no shortcuts are available.

HOW TO SELECT IT

To use the ncurses GUI you have to:

- compile ettercap with ncurses support (obviously)
- run it with the −C flag

Passing the −C flag is sufficient, but if you want you can pass other flags that will be automatically set for the ncurses GUI. You will be able to override them using the menu to change the options.

ONCE STARTED

As soon as ettercap is launched with the Ncurses GUI, you will be prompted with multiple choices. The first screen lets you select if you want to open a pcap file or dump the sniffed traffic to a file, if you want unified sniffing or bridged one, permits you to set a pcap file on the captured traffic and enables you to log all the sniffed data.

Once you have selected a sniffing method (from file, unified or bridged) this screen will not be reachable anymore. The only way is to restart ettercap.

Let's analyze each menu in the start screen:

File

Open... Open a pcap file and analyze it. All the functionalities available for live sniffing are in place except for those sending or forwarding packets (mitm attacks and so on...).

Dump to file...
All the traffic sniffed by the live capture will be dumped to that file. The filters, not the targets, have effects on this file, as all the packets received by pcap will be dumped. The only way to not dump a certain packet is to set a proper pcap filter (see below).

Exit
Exits from ettercap and returns to the command prompt.

Sniff

Unified sniffing...
Choosing this function you will be prompted to select the network interface to be used for sniffing. The first up and running interface is suggested in the input box. For an explanation of what unified sniffing is, refer to ettercap(8).
TIP: if you use the 'u' hotkey, this step will be skipped and the default interface is automatically selected.

Bridged sniffing...
After selecting the two interfaces to be used, you will enter the Bridged sniffing mode. For an explanation of what bridged sniffing is, refer to ettercap(8).

Set pcap filter...
Here you can insert a tcpdump-like filter for the capturing process.
IMPORTANT: if you manage to use a mitm attack, remember that if ettercap does not see a packet, it will NOT be forwarded. So be sure of what you are doing by setting a pcap filter.

Options

Unoffensive
This enable/disable the unoffensive flag. The asterisk '*' means "the option is enabled". Otherwise the option is not enabled.

Promisc mode
Enable/disable the promisc mode for the live capture on a network interface. This is an "asterisk-option" as the unoffensive one.

Set netmask
Use the specified netmask instead of the one associated with the current iface. This option is useful if you have the NIC with an associated netmask of class B and you want to scan (with the arp scan) only a C class.

THE INTERESTING PART

Once you have selected an offline sniffing or a live capture, the upper menu is modified and you can start to do the interesting things...
Some of the following menu are only available in live capture.

Start

Start sniffing
Starts the sniffing process depending on what you have selected on startup (live or from file)

Stop sniffing
Stops the sniffing thread.

Exit
Returns to your favourite shell ;)

Targets

Current Targets
Displays a list of hosts in each TARGET. You can selectively remove a host by selecting it and press 'd' or add a new host pressing 'a'. To switch between the two lists, use the ARROWS keys.

Select TARGET(s)
Lets you select the TARGET(s) as explained in ettercap(8). The syntax is the same as for the command line specification.

Protocol...
You can choose to sniff only TCP, only UDP or both (ALL).

Reverse matching
Reverse the matching of a packet. It is equivalent to a NOT before the target specification.

Wipe Targets
Restores both TARGETS to ANY/ANY/ANY

Hosts

Hosts list
Displays the list of hosts detected through an ARP scan or converted from the passive profiles. This list is used by MITM attacks when the ANY target is selected, so if you want to exclude a host from the attack, simply delete it from the list.
You can remove a host from the list by pressing 'd', add it to TARGET1 by pressing '1' or add it to TARGET2 by pressing '2'.

Scan for hosts
Perform the ARP scan of the netmask if no TARGETS are selected. If TARGETS was specified it only scans for those hosts.

Load from file...
Loads the hosts list from a file previously saved with "save to file" or hand crafted.

Save to file...
Save the current hosts list to a file.

View

Connections
Displays the connection list. To see detailed information about a connection press 'd', or press 'k' to kill it. To see the traffic for a specific connection, select it and press enter. Once the two-panel interface is displayed you can move the focus with the arrow keys. Press 'j' to switch between joined and split visualization. Press 'k' to kill the connection. Press 'y' to inject interactively and 'Y' to inject a file. Note that it is important which panel has the focus as the injected data will be sent to that address.
HINT: connections marked with an asterisk contain account(s) information.

Profiles
Diplays the passive profile hosts list. Selecting a host will display the relative details (including account with user and pass for that host).
You can convert the passive profile list into the hosts list by pressing 'c'. To purge remote hosts, press 'l'. To purge local hosts, press 'r'. You can also dump the current profile to a file by pressing 'd'; the dumped file can be opened with etterlog(8).
HINT: profiles marked with an asterisk contain account(s) information.

Statistics
Displays some statistics about the sniffing process.

Resolve IP addresses
Enables DNS resolution for all the sniffed IP address. CAUTION: this will extremely slow down ettercap. By the way the passive dns resolution is always active. It sniffs dns replies and stores them in a cache. If an ip address is present in that cache, it will be automatically resolved. It is dns resolution for free... ;)

Visualization method
Change the visualization method for the sniffed data. Available methods: ascii, hex, ebcdic, text, html.

Visualization regex
Set the visualization regular expression. Only packets matching this regex will be displayed in the connection data window.

Set the WiFi key
Set the WiFi key used to decrypt WiFi encrypted packets. See ettercap(8) for the format of the key.

Mitm

[...] For each type of attack, a menu entry is displayed. Simply select the attack you want and fill the arguments when asked. You can activate more than one attack at a time.

Stop mitm attack(s)
Stops all the mitm attacks currently active.

Filters

Load a filter...
Load a precompiled filter file. The file must be compiled with etterfilter(8) before it can be loaded.

Stop filtering
Unload the filter and stop filtering the connections.

Logging

Log all packets and infos...
Given a file name, it will create two files: filename.eci (for information about hosts) and filename.ecp (for all the interesting packets). This is the same as the –L option.

Log only infos...
This is used only to sniff information about hosts (same as the –l option).

Stop logging info
Come on... it is self explanatory.

Log user messages...
Will log all the messages appearing in the bottom window (same as −m option).

Compressed file
Asterisk-option to control whether or not the logfile should be compressed.

Plugins

Manage the plugins
Opens the plugin management window. You can select a plugin and activate it by pressing 'enter'. Plugins already active can be recognized by the [1] symbol instead of [0]. If you select an active plugin, it will be deactivated.

Load a plugin...
You can load a plugin file that is not in the default search path. (remember that you can browse directories with EC_UID permissions).

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