



Security Tool Review and Howto:
kismet/gkismet

By Joe Burke GSEC, MCP, Linux+
joe@localareasecurity.com

Introduction:

Kismet is an open source utility used for monitoring wireless network traffic. It is a popular choice for detecting/enumerating wireless access points and wireless clients.

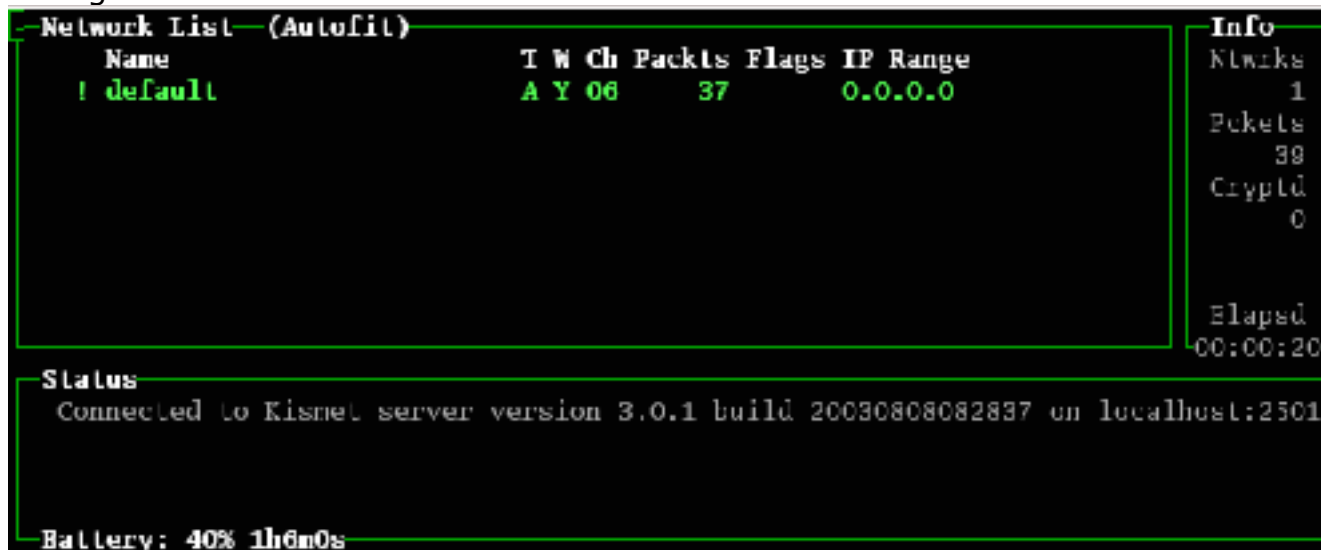
Overview:

The first step to using kismet is purchasing a compatible network card. The card's chipset must be capable of "Monitor Mode", also referred to as RFMON. Current compatible chipset choices include Lucent/Orinoco, Cisco, Prism, Atheros. There are a number of resources available online including forums, newsgroups and mailing lists to assist tracking down a compatible NIC. RFMON is also a requirement for other wireless tools including aircrack-ng.

Once you have a compatible NIC, the next step is to compile and install the correct driver and software. Consult the kismet website and accompanying documentation for assistance. The Aircrack-ng website is also a valuable resource for driver and dependency help.

Once everything is installed and your conf files are setup the way you like, you can then execute kismet from a terminal session. (You may need to su to root or the SUID account you assigned during installation before executing) If you're presented with the screen shown in figure 1, then you're in good shape.

Figure 1: Kismet panel interface - uses keyboard driven panels to navigate through available menus.



```
Network List (Autofit)
Name          T W Ch Packets Flags IP Range
! default    A Y 06      37      0.0.0.0

Info
Kiwiks      1
Packets     39
Crypto      0

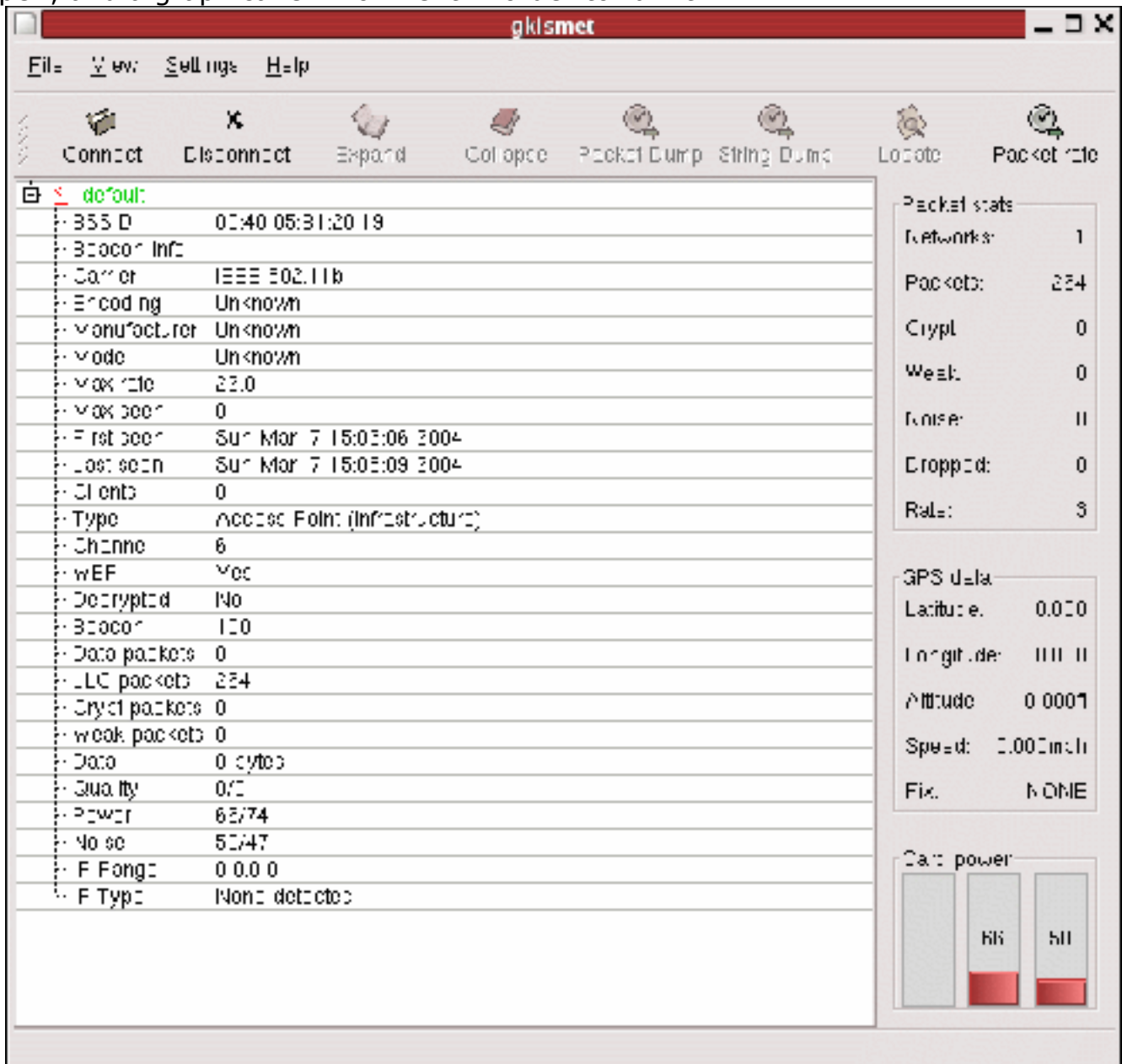
Elapsed
00:00:20

Status
Connected to Kismet server version 3.0.1 build 20030808082837 on localhost:2501

Battery: 40% 1h6m0s
```

You can use the 'h' key to display the help screen at any time. Each panel has a different help screen to assist you by listing the available hot keys.

Gkismet GUI interface – Offers the same information as the panel interface, but in a different format. This program is a front-end for the kismet tool, and cannot run independently. The program is helpful because it allows you to display more data to the screen at once, and is conveniently useful to connect to multiple instances of kismet. There are however additional system requirements such as perl, gtk-perl, and a graphical environment in order to run it.



Key features:

Kismet groups detected devices by network, and allows you to drill down into the details for more information.

Kismet can report the following interesting network attributes (among others):

- SSID
- AP MAC (BSSID)
- Client MAC(s)
- 802.11 standard and maximum data rate
- Channel used
- Quality, Signal, and Noise
- Packet counts including: data, LLC, encrypted, weak
- IP range

In addition to printing summary information to the screen, Kismet captures packets and periodically dumps them to a file. These files can later be used as input to packet analysis tools such as Aircrack-ng or ethereal.

GPS software such as GPSdrive can be used in conjunction with kismet to log and track physical locations of detected devices.

Kismet also recognizes the signatures of popular wireless attacks, and can act as an intrusion detection system. To increase your effective coverage for IDS and other configurations, multiple instances of Kismet running on different machines can be centrally managed.

Manpage:

The manpage is not overly useful considering that much of what is shown as command switches is more easily managed via conf files. It is also out of date in some sections (See note in italics below).

NAME

kismet - Wireless sniffing and monitoring

SYNOPSIS

kismet [server-options] [--] [client-options]

kismet_server [-nqs] [-t title] [-f config-file] [-c capture-source]
[-C enable-capture-sources] [-l log-types] [-d dump-type]
[-m max-packets-per-file] [-g gpshost:port] [-p listen-port]
[-a allowed-hosts] [-N server-name]

kismet_client [-qr] [-f config-file] [-s serverhost:port] [-g gui-type]
[-c display-columns]

DESCRIPTION

kismet is an 802.11b wireless network sniffer. It is capable of sniffing using almost any wireless card supported by Linux, including cards based on the Prism/2 chipset with the wlan-ng driver (Compaq, Linksys, D-Link, and more), cards based on the Lucent chipset (Orinoco) with the patched orinoco driver, cards using the Aironet chipset (Cisco) supported by the kernel Aironet drivers, and limited support for cards that do not support RF Monitoring.

kismet supports logging to the wtapfile packet format (readable by tcpdump and ethereal) and saves detected network informat as plaintext, XSV, and XML. kismet is capable of using any GPS supported by gpsd and logs and plots network data.

kismet is divided into three basic programs, kismet_server kismet_client and gpsmap

USAGE

kismet handles automatically starting kismet_server and kismet_client.

IT IS IMPERATIVE THAT YOU PLACE YOUR CARD IN RFMON MODE BEFORE STARTING

KISMET OR YOU WILL NOT SEE ANY TRAFFIC. Your card can be placed into monitor mode by configuring kismet for your card and running kismet_monitor as root.

Note: I have an Orinoco silver card using kismet v3.0.1 and setting RFMON mode prior to launching kismet is no longer required.

kismet is installed as `sudo` by default. It will drop privs to the user specified in `kismet.conf` immediately after binding to the capture source. `kismet_monitor` must be run as root, as it modifies the state of the wireless card. `kismet` can be run as any user due to the aforementioned privilege drop.

KISMET_SERVER

`kismet_server` captures, dissects, and logs packets and GPS data. It is capable of running in 'headless' mode with no display. Multiple clients (on multiple computers) can be connected to a single server.

- I Set the initial channel for a channel source (source:channel)
- x Forcibly enable the channel hopper
- X Forcibly disable the channel hopper
- t Set the title used for the %t field of the logfile template (Default: Kismet)
- n Disable all logging
- f Use an alternate config file
- c Override capture source lines (type,interface,name). Refer to `kismet.conf(5)` for more information. Multiple capture source options can be specified for multiple sources. All sources provided here are automatically enabled unless an enable list is also supplied.
- C Comma-separated list to override what capture sources are enabled.
- l Override logging types, comma separated (dump, cisco, weak, csv, xml, gps)
- m Override maximum packets logged per file
- q Override sound option and run in quiet mode
- g Override GPS host:port
- p Override port to listen on for clients
- a Override list of client IPs or network/mask blocks (comma separated) allowed to connect

- s Run in silent mode (no console status information)
- N Override server name for this instance of Kismet
- v Print version
- h Help

KISMET_CLIENT

kismet_client is a ncurses and panels interface which connects to the server and displays detected networks, statistics, network details, etc.

- f Use an alternate config file
- u Use an alternate UI config file
- q Override sound option and run in quiet mode
- s Override server host:port
- r Attempt to automatically reestablish the connection if the server terminates
- g Override UI type (curses, panel)
- c Override list of columns to display (comma separated)
- v Print version
- h Help

GPSMAP

gpsmap reads GPS and Network XML datafiles and plots networks on downloaded maps or user-supplied images (such as satellite photos).

SEE ALSO

kismet_drone(1), gpsmap(1), kismet.conf(5), kismet_ui.conf(5), kismet_drone.conf(5)

Resources

<http://airsnort.shmoo.org>
<http://prism54.org>
<http://sourceforge.net/projects/madwifi>
<http://airo-linux.sourceforge.net>
<http://kismetwireless.net>

