PRACTICAL ASSESSMENT SHEET

Experiment number: - 9

Title of experiment: - Study of security tool - KISMET

Name of Student: - Niraj Nitin Surve

Roll number: - 68

Date of performance: -

Date of submission: -

Attendance 03 marks	Submission 03 marks	Performance 03 marks	Oral 03 marks	Result 03 marks	Total 15 marks

Faculty Signature with date

Practical No. 09

TITLE: STUDY OF SECURITY TOOL - KISMET

AIM: TO STUDY SECURITY TOOL - KISMET

THEORY:

What is KISMET?

- Kismet is a network detector, packet sniffer, and intrusion detection system for 802:1 1 wireless LANs.
- It was developed by Mike Kershaw.
- Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.1 1 a, 802.1 1b, and 802.1 In traffic.
- The program runs under Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X.

What is Packet Sniffing?

- Packet sniffing is the act of capturing packets of data flowing across a computer network.
- The software or device used to do this is called a packet sniffer, such as Kismet.
- It can be used to troubleshoot network problems, as well as to extract sensitive information.

Packet Sniffer components

- **Hardware :** These are standard network adaptors.
- **Capture Filters :** Captures the network traffic from the wire & filters it for the particular traffic & then stores the data in a buffer.
- **Buffer :** Used to store the frames captured by the Capture Filter.
- **Real Time Analyzer:** Used for traffic analysis.
- **Decoder :** Used for Protocol Analysis.

KISMET

- Kismet application is an open source wireless network analyzer running on Linux, UNIX and Mac OS X.
- And previously not supported by windows os.
- Kismet is a passive sniffer used to detect any wireless 802.11 a/b/g protocol complaint networks.

- Kismet can discover, log the IP range of any detected wireless network and report its signal and noise levels.
- Kismet can be used to locate, troubleshoot and optimize signal strength for access points and clients, as well as detect network intrusions.
- It can sniff all management data packets from detected networks.
- Kismet passively monitors wireless networks -
  - Cannot be detected.
  - Can see non-beaconing networks if they are in use.
  - Recovers cloaked SSIDs by listening to connection handshakes.

KISMET as a Client Infrastructure

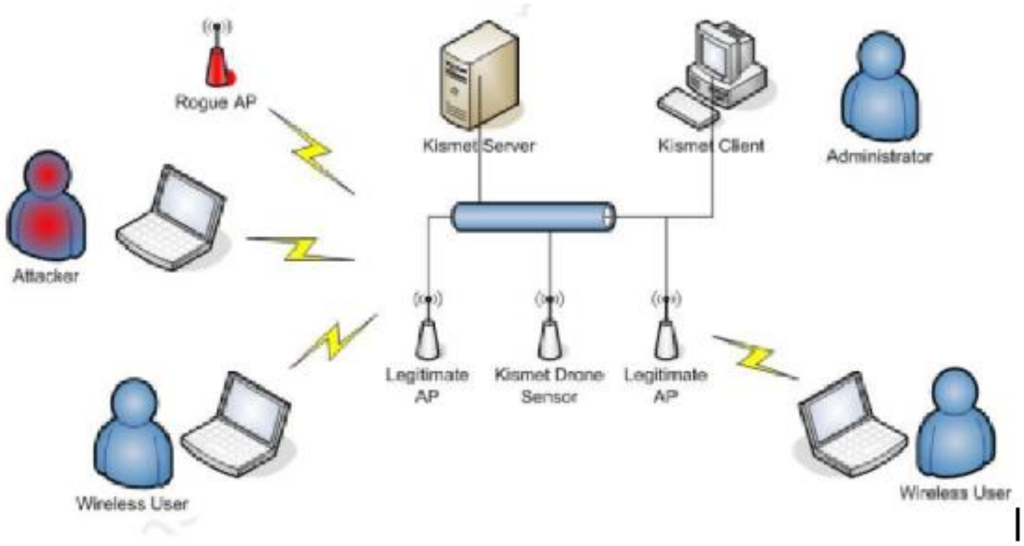
Basically there are three separate parts in Kismet Architecture.

1. Drone
2. Server
3. Client

1. KISMET Drone -
   The drone collects the information packets from the network which it has to display.

2. KISMET Server -
   Server accepts the information packets from the drone for interpretation. The server works in conjunction with a drone or works on its own. It interprets the packet data and extrapolates the wireless information and organizes it.

3. KISMET Client -
   The client communicates with the server and displays the information the server collects.



Features of KISMET -

- Kismet differs from other wireless network detectors in working passively.
- without sending any loggable packets, it is able to detect the presence of both wireless access points and wireless clients, and to associate them with each other.
- It is also the most widely used and up to date open source wireless monitoring tool.
- Kismet is licensed under the GNU GPL (General Public License).
- The GNU General Public License (GNU GPL or CPL) is the most widely used free software license, which guarantees end users (individuals, organizations, companies) the freedoms to use, study, share (copy), and modify the software.
- It is officially distributed as a source package which you can compile for a variety of platforms.
- Kismet also includes basic wireless IDS features such as detecting active wireless sniffing programs including NetStumbIer, as well as a number of wireless network attacks.

Supported Hardware -

- Kismet functions only with network cards with drivers that support RF monitoring mode.
- This includes wireless cards based on the PRISM 2, 2.5, 3, and GT chipsets; older ORiNOCO cards without the Hermesll chipset, such as the Orinoco Gold; and Atheros a/b/g chipsets.

Installing KISMET

- Kismet is officially distributed as a source package which you can compile for a variety of platforms, from Linux to OS X to BSD.
- The Kismet Web site also distributes pre-compiled binaries for Arm and MIPS platforms. These binaries allow you to run Kismet on small devices such as WRT54G routers.
- Initially the Kismet was made for Linux os, so it works best for Linux platform.
- Hence Linux users don't want to compile Kismet from source. They are only required to check repositories for their distribution.

  For eg : On my Ubuntu Linux I will simply launch 'Synaptic Package Manager' and I can easily get Kismet and click install.

Steps to install KISMET

1. Open the terminal as root user in Ubuntu and download the kismet binaries from www.kismetwireless.net: into the tmp folder. Requires root privileges: Eg: root@stephen - laptop:/home/stephen#
2. The kismet file is automatically downloaded to the kismet folder in the etc directory also.
3. To make all the kismet files executable:

   ```
   Eg: stephen@stephen-laptop:/tmp/kismet$ 1 root
   ```
4. KISMET DRONE INSTALLATION

   ```
   Eg: root@OpenWrt:~/kismet-2006-04-Rl -wrt54# scp
   kismet_drone /usr/bin/kismet_drone
   root@OpenWrt:~ /kismet-2006-04-Rl -wrt54/conf# scp
   Kismet-drone.conf    /etc/kismet-drone.conf
   ```
5. KISMET CLIENT AND KISMET SERVER INSTALLATION

   ```
   Eg: root@OpenWrt: /# ssh 192.168.1.107 root@stephen-laptop:~#
   root@stephen-laptop:~# apt-get install ascii
   ```

KISMET GUI and KISMET LAUNCH

- Before the kismet GUI is launched, it is important that the following scripts be written into the /tmp folder of the WRT.
- Using vi editor: This „rundrone.sh" script with a „wl passive" command is included so that the router does not start an active scan immediately and generating packets instead of gathering packets.

  ```
  w/ ap O
  w/ diassoc
  w/ passive 1
  w/ promisc
  chmod 777 /usr/bin/kismet*
  /usr/bin/./kismet_drone -f /etc/kismet_drone.conf
  ```

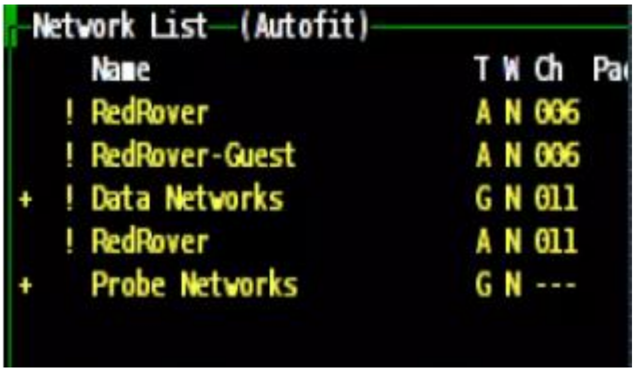
chmod 777 will make the kismet_drone.conf and the kismet_drone files executable.

Configuration of KISMET

- Kismet is designed as a client-server application, but it can be run as a standalone application.
- Run standalone means, you simply use the built-in client. But there are also a number of third-party clients available for Kismet.
- Most users run both the client and server on the same machine and simply use Kismet as a local application.
- In a typical Linux install, the Kismet configuration files are found in letc/kismet. Depending on your platform or distribution, this location may vary.
- Before you can run Kismet for the first time, you may need to edit the primary configuration file, kismet.conf. Inside, you will find the line
  :suiduser=your_username_here
- You also need to tell Kismet which "source" or wireless adapter,
  to use. The basic syntax used in kismet.conf is: source=type.interface.name
  Eg:source=prism,wlan0,hostap

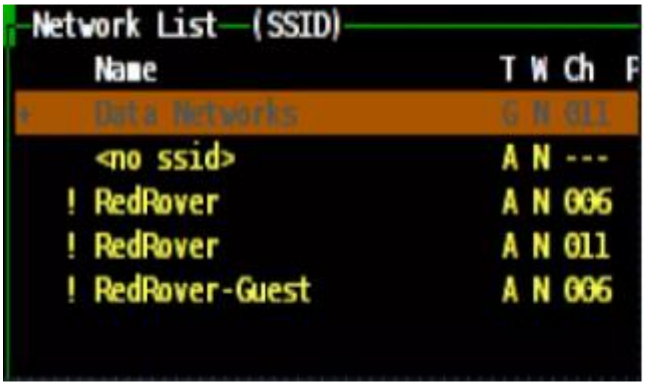
Running KISMET

- Unless you install a window-based GUI for Kismet such as KisMAC or GKismet, this is a text-based application. On Linux system, open a terminal window and launch Kismet as root:
  sudo kismet
- Kismet shows the list of detected wireless networks. They are initially sorted in "Autofit" mode. Press "s" to bring up the sort menu, where you can order the SSID's by name, chronology, and other criteria.
  - Before pressing ‘S’



```
Network List—(Autofit)
       Name                        T W Ch  Pa
     ! RedRover                    A N 006
     ! RedRover-Guest              A N 006
 +   ! Data Networks               G N 011
     ! RedRover                    A N 011
 +     Probe Networks              G N ---
```

- After pressing ‘S’



```
Network List—(SSID)
          Name                          T W Ch  F
        Data Networks                   G N 011
          <no ssid>                     A N ---
        ! RedRover                      A N 006
        ! RedRover                      A N 011
        ! RedRover-Guest                A N 006
```

What KISMET Shows?

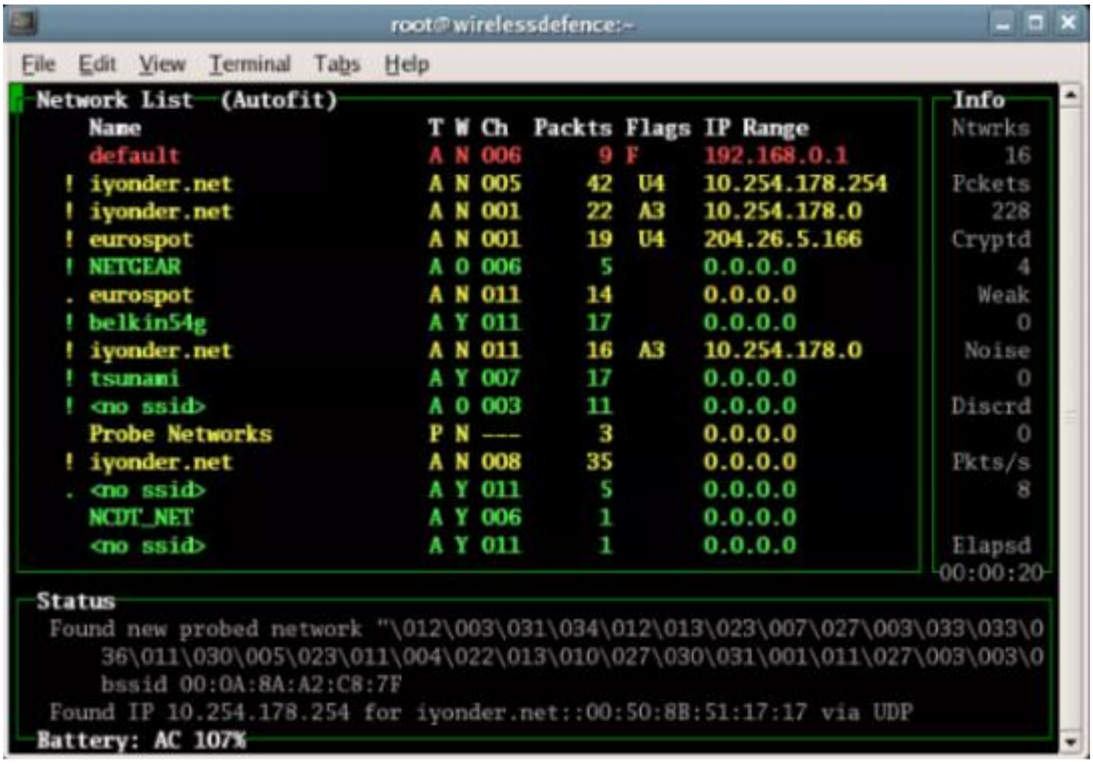
1. List of SSIDs.
2. T = Type
   a. P: Probe request - no associated connection yet
   b. A: Access point - standard wireless network
   c. H: Ad-hoc - point to point wireless network
   d. T : Turbocell - Turbocell aka Karlnet or Lucent Router
   e. G : Group - Group of wireless networks
   f. D: Data - Data only network with no control packets
3. W = Encryption
4. Colour = Network/Client Type:

   Yellow Unencrypted Network

   Red Factory default settings in use!

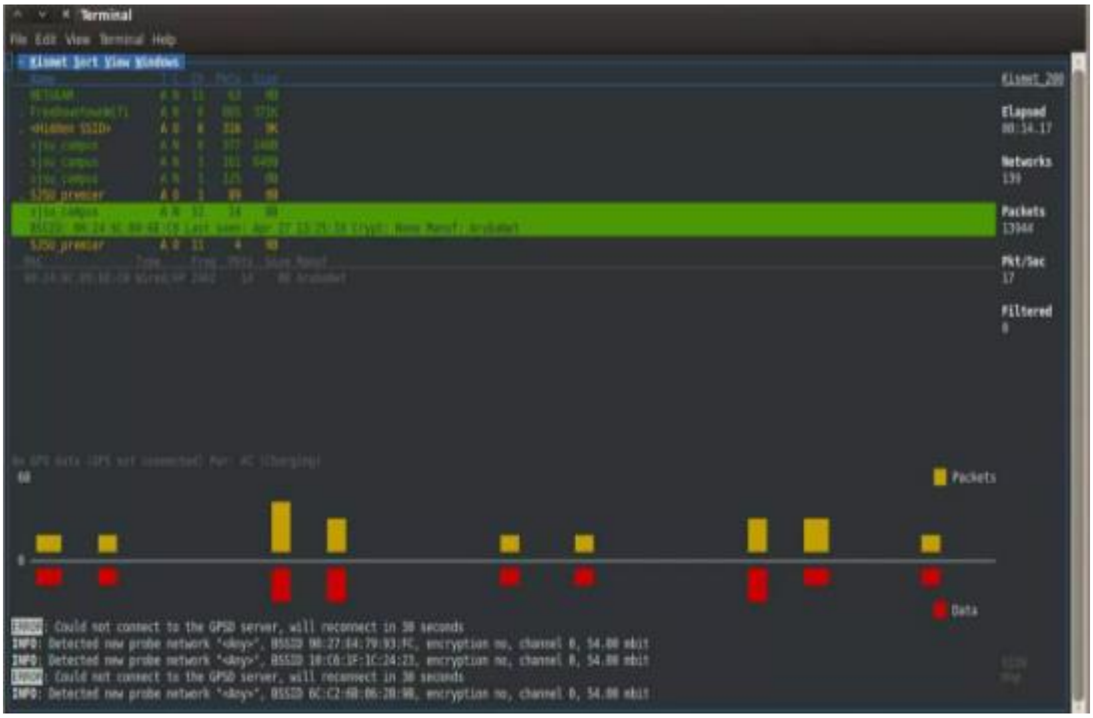
   Green Secure Networks (WEP, WPA etc.)

   Blue SSID cloaking on / Broadcast SSID disabled



```
Network List (Autofit)                                          Info
     Name                  T W Ch  Packts Flags IP Range        Ntwrks
     default               A N 006      9 F     192.168.0.1         16
   ! iyonder.net           A N 005     42 U4    10.254.178.254  Pckets
   ! iyonder.net           A N 001     22 A3    10.254.178.0       228
   ! eurospot              A N 001     19 U4    204.26.5.166    Cryptd
   ! NETGEAR               A 0 006      5       0.0.0.0              4
   . eurospot              A N 011     14       0.0.0.0           Weak
   ! belkin54g             A Y 011     17       0.0.0.0              0
   ! iyonder.net           A N 011     16 A3    10.254.178.0     Noise
   ! tsunami               A Y 007     17       0.0.0.0              0
   ! <no ssid>             A 0 003     11       0.0.0.0         Discrd
     Probe Networks        P N ---      3       0.0.0.0              0
   ! iyonder.net           A N 008     35       0.0.0.0         Pkts/s
   . <no ssid>             A Y 011      5       0.0.0.0              8
     NCDT_NET              A Y 006      1       0.0.0.0
     <no ssid>             A Y 011      1       0.0.0.0         Elapsd
                                                                00:00:20
Status
 Found new probed network "\012\003\031\034\012\013\023\007\027\003\033\033\0
     36\011\030\005\023\011\004\022\013\010\027\030\031\001\011\027\003\003\0
     bssid 00:0A:8A:A2:C8:7F
 Found IP 10.254.178.254 for iyonder.net::00:50:8B:51:17:17 via UDP
Battery: AC 107%
```

Packet Capturing in KISMET GUI



```
Kismet_2[illegible]
Elapsed
00:14.17
Networks
139
Packets
13944
Pkt/Sec
17
Filtered
0

ERROR: Could not connect to the GPSD server, will reconnect in 30 seconds
INFO: Detected new probe network "<Any>", BSSID 00:27:E4:79:93:FC, encryption no, channel 0, 54.00 mbit
INFO: Detected new probe network "<Any>", BSSID 10:C6:1F:1C:24:23, encryption no, channel 0, 54.00 mbit
ERROR: Could not connect to the GPSD server, will reconnect in 30 seconds
INFO: Detected new probe network "<Any>", BSSID 6C:C2:6B:06:28:98, encryption no, channel 0, 54.00 mbit
```

Capturing packets & decrypting traffic with KISMET

- By default, packet captures are created every time you run Kismet.
- Kismet has a unique feature that can cut down the time between wireless reconnaissance & wireless intrusion.
- Whenever kismet detects a data packet vulnerable to a related key attack it stores it in a. weak log file.
- These files can be used to speed up cracking wireless encryption & supported by major WEP cracking tools.

Main benefits of KISMET

- It puts the card into a monitoring mode which is not attached to any network.
- It scans all the wireless networks passively so it remains undetected.
- It can scan the entire spectrum and all the wireless networks nearby.
- It generates different types of logs thus giving full information about the network.

Why is KISMET better than others?

- Network IP range detection & XML output.
- Graphical mapping of networks & Distributed remote drone sniffing.
- Detection of known default access point configurations.
- Over 20 supported card types & Client/Server architecture allows multiple clients to view a single.
- Runtime decoding of WEP packets for known networks.

Conclusion- Thus we understand the implementation of bluetooth file transfer.