Experiment No: 10

Aim: Study of security tools (like Kismet, Netstumbler)

Theory:

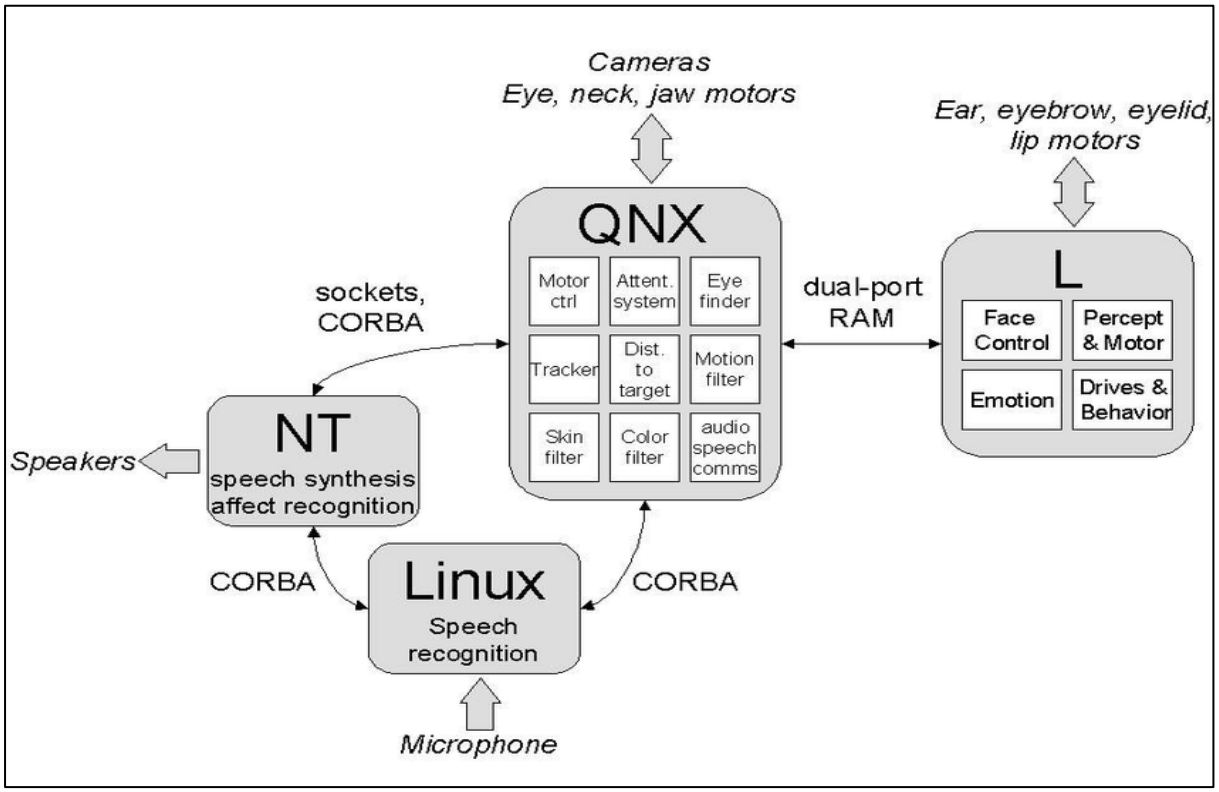
Security tools like Kismet and NetStumbler are used primarily in wireless network monitoring, auditing, and penetration testing. Both tools are designed to help security professionals and network administrators detect and analyze wireless networks, identify vulnerabilities, and ensure proper configurations. Below is an explanation of both tools, their functionalities, and how they contribute to network security.

1. Kismet

- **Kismet** is a powerful wireless network detector, sniffer, and intrusion detection system (IDS) for 802.11 wireless LANs. It supports various wireless devices and allows users to capture packets, detect hidden networks, and analyze wireless traffic.
- **Key Features of Kismet:**
  - **Wireless Network Detection**: Kismet detects wireless networks even if they are hidden (non-broadcast SSIDs).
  - **Packet Sniffing**: It captures raw packets over the air, which can be analyzed for weaknesses in encryption and other security issues.
  - **Intrusion Detection**: Kismet can identify potentially malicious activity, such as unauthorized devices trying to connect to the network.
  - **Geolocation**: Using GPS, Kismet can also map out the physical location of access points and devices.
  - **Alerts**: Users can set up alerts to notify when certain types of activity are detected.
- **Working of Kismet:**
  - Kismet runs on Linux and uses wireless network interfaces in monitor mode to capture all wireless traffic. It can capture and log data about all visible networks, even those using encryption like WPA2.
  - The tool works in passive mode, meaning it does not actively send out packets, so it's not easily detected by the monitored networks.

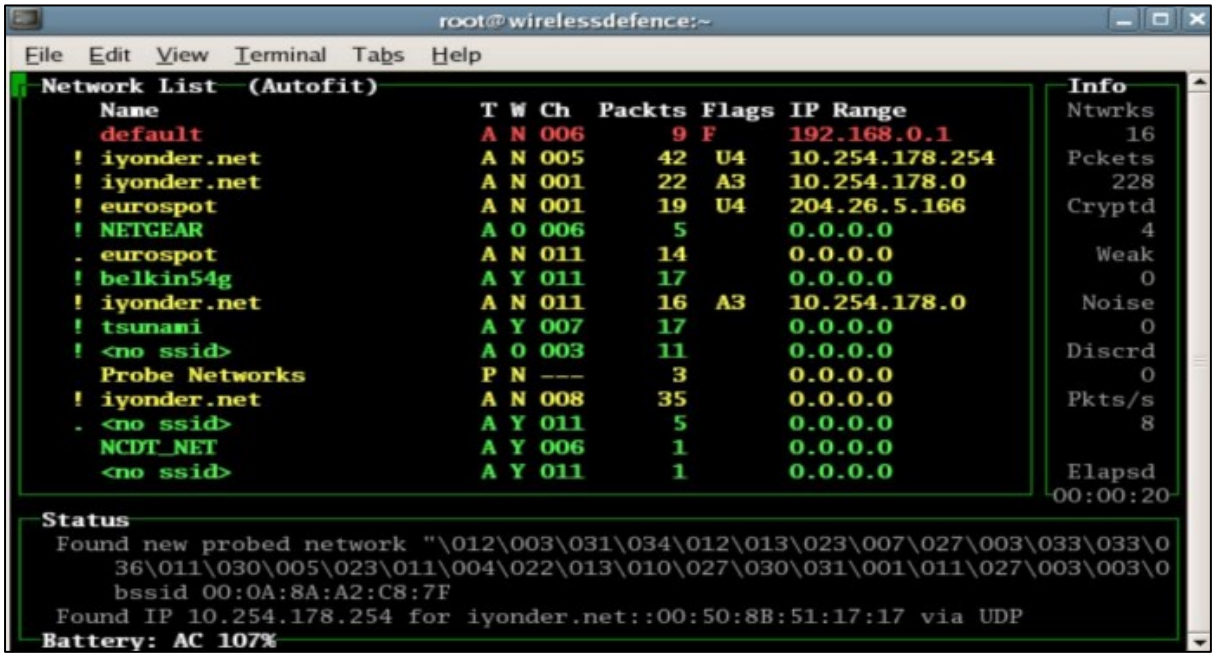
System architecture for Kismet.

The motivation system runs on four Motorola 68332 microprocessors running L, a multi-threaded Lisp developed in our lab. Vision processing and eye/neck control is performed by nine networked PCs running QNX, a real-time operating system similar to Linux.



2. NetStumbler

- **NetStumbler** is a Windows-based tool that is used for scanning wireless networks. It can help users find and diagnose network issues, such as weak signals, misconfigurations, or security flaws.
- **Key Features of NetStumbler:**
  - **Network Discovery**: It can detect open or insecure networks, making it useful for security assessments and troubleshooting.
  - **Signal Strength Visualization**: NetStumbler provides signal strength graphs that help users visualize network coverage and signal quality.
  - **SSID Detection**: It can identify and list available wireless networks, including hidden SSIDs.
  - **Location Tracking**: Similar to Kismet, it also supports GPS-based mapping of wireless networks.
- **Working of NetStumbler:**
  - NetStumbler runs on Windows and relies on standard wireless cards to detect available wireless networks.
  - It can detect various types of wireless encryption and provide detailed information on network configurations, such as SSID, encryption type, and signal strength.
  - Unlike Kismet, NetStumbler works in an active mode, meaning it actively sends probes and can be detected by network administrators.



Comparing Kismet and NetStumbler

Feature	Kismet	NetStumbler
Platform	Linux	Windows
Network Detection	Supports detecting both open and hidden networks	Detects open and hidden networks
Security Focus	Intrusion detection, packet sniffing	Wireless network scanning and troubleshooting
Packet Sniffing	Yes	No
Signal Strength	Yes (with GPS)	Yes (graphical representation)
Intrusion Detection	Yes	No
Mode of Operation	Passive (non-intrusive)	Active (can be detected)

- ## Conclusion

  Both Kismet and NetStumbler are essential tools for network security professionals. Kismet is more focused on passive monitoring and packet sniffing, making it ideal for network auditing and intrusion detection in wireless environments. NetStumbler, on the other hand, is a simpler tool for Windows users, suitable for basic wireless network detection, diagnosis, and troubleshooting. While both tools have different strengths, together they offer a powerful suite for wireless network security, vulnerability assessment, and troubleshooting.