Vidya Vikas Education Trust's
Universal College of Engineering, Kaman Road, Vasai – 401208
Accredited A Grade by NAAC

Experiment No: 10

Aim: Study of security tools like **Kismet** and **NetStumbler**

Theory: Wireless networks are widely used in modern communication systems, but they are also vulnerable to security threats such as unauthorized access, data interception, and rogue access points. Security tools like Kismet and NetStumbler help network administrators, cybersecurity professionals, and ethical hackers analyze, secure, and troubleshoot wireless networks.

1. Kismet

Kismet is a passive wireless network sniffer and intrusion detection system (IDS) that works by capturing network packets without actively probing the network.

Features of Kismet:

- Packet Sniffing: Captures raw data packets from the air without connecting to networks.
- Hidden SSID Detection: Identifies wireless networks that do not broadcast their SSID.
- Intrusion Detection: Helps in finding unauthorized access points and security threats.

- GPS Integration: Can be used for wardriving to map wireless networks with location data.
- Multiple Wireless Card Support: Works with various Wi-Fi interfaces to capture more data.

Use Cases of Kismet:

- Penetration Testing: Identifying vulnerabilities in wireless networks.
- Network Security Auditing: Monitoring for unauthorized Wi-Fi activity.
- Forensic Investigations: Analyzing captured network packets for security incidents.

Limitations of Kismet:

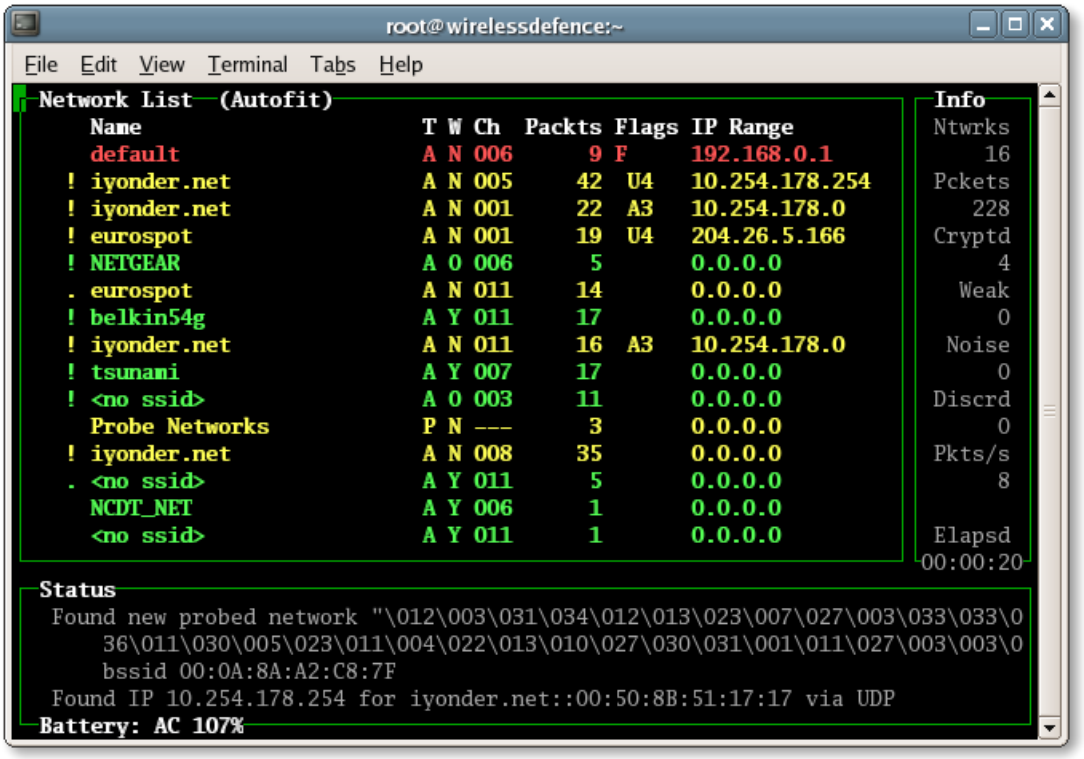
- Requires compatible wireless network cards that support monitor mode.
- Command-line interface (CLI) can be challenging for beginners.

Platform Support:

- Linux, macOS, Windows (limited support)

2. NetStumbler

NetStumbler is an active wireless network discovery tool that scans for available networks and gathers information such as signal strength, security type, and access point details.



Features of NetStumbler:

- Wi-Fi Network Discovery: Identifies all nearby wireless networks.
- Signal Strength Analysis: Helps in optimizing the placement of Wi-Fi routers.
- Rogue Access Point Detection: Detects unauthorized or misconfigured access points.
- Graphical User Interface (GUI): Easy to use for beginners.
- GPS Support: Used for wardriving to map Wi-Fi networks.

Use Cases of NetStumbler:

- Network Optimization: Finding the best placement for Wi-Fi access points.
- Troubleshooting Connectivity Issues: Identifying interference and weak signal areas.
- Wireless Security Audits: Detecting unauthorized networks in an organization.

Limitations of NetStumbler:

- Does not support hidden SSID detection.
- Not effective on modern Windows versions (last updated for Windows XP).
- Cannot capture network packets like Kismet.

Platform Support:

- Windows

GitHubLink:

https://github.com/Jatan2004/Mc-experiments/tree/main/MC%20EXP%2010%20Case%20study

Conclusion: The study of security tools like Kismet and NetStumbler is essential for understanding wireless network security, network monitoring, and intrusion detection.

- Kismet is a passive tool used for packet sniffing, hidden SSID detection, and intrusion detection, making it ideal for network security auditing and penetration testing.
- NetStumbler is an active tool used for Wi-Fi network discovery, signal strength analysis, and rogue AP detection, making it useful for network optimization and troubleshooting.