Experiment No : 10

Aim: Study of security tools like Kismet and NetStumbler.

Theory:

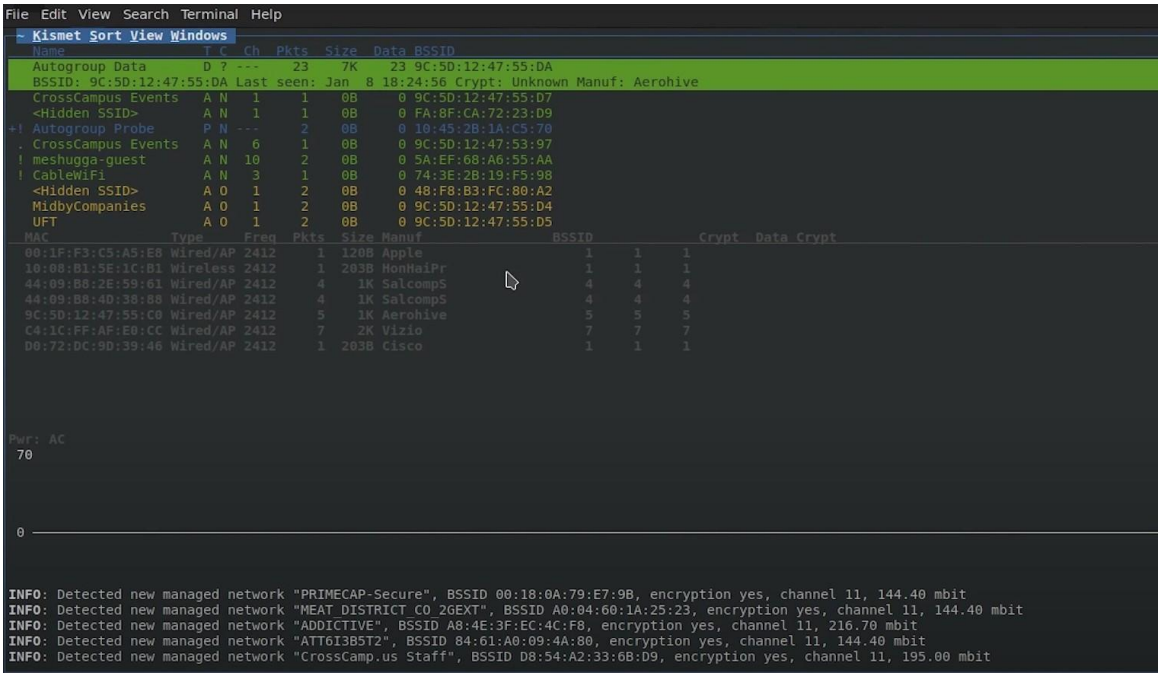
With the increasing use of wireless networks, security concerns have also risen. Unauthorized access, data breaches, and network vulnerabilities pose serious threats to individuals and organizations. To analyze and secure wireless networks, various security tools are available. Among them, **Kismet** and **NetStumbler** are widely used for detecting, analyzing, and monitoring wireless networks. These tools help security professionals, network administrators, and ethical hackers to perform audits and identify security weaknesses in Wi-Fi networks.

Kismet

Kismet is an open-source network detection and monitoring tool primarily used for analyzing wireless network traffic. It is widely used in ethical hacking, penetration testing, and security auditing.

Features of Kismet:

1. **Wireless Network Detection:** Kismet can detect Wi-Fi networks, even those with hidden SSIDs (Service Set Identifiers), by capturing network traffic.
2. **Packet Sniffing:** It captures data packets transmitted over the air, providing insights into network activity.
3. **Multiple Interface Support:** Kismet supports multiple wireless interfaces and operates in monitor mode.
4. **Passive Network Monitoring:** Unlike tools that actively probe networks, Kismet passively listens for network traffic, making it undetectable.
5. **Intrusion Detection System (IDS):** Kismet can detect rogue access points, unauthorized connections, and possible network intrusions.
6. **Cross-Platform Compatibility:** It is compatible with Linux, macOS, and Windows (with limited functionality).
7. **GPS Integration:** Kismet can be integrated with GPS tools to map network locations.



How Kismet Works:

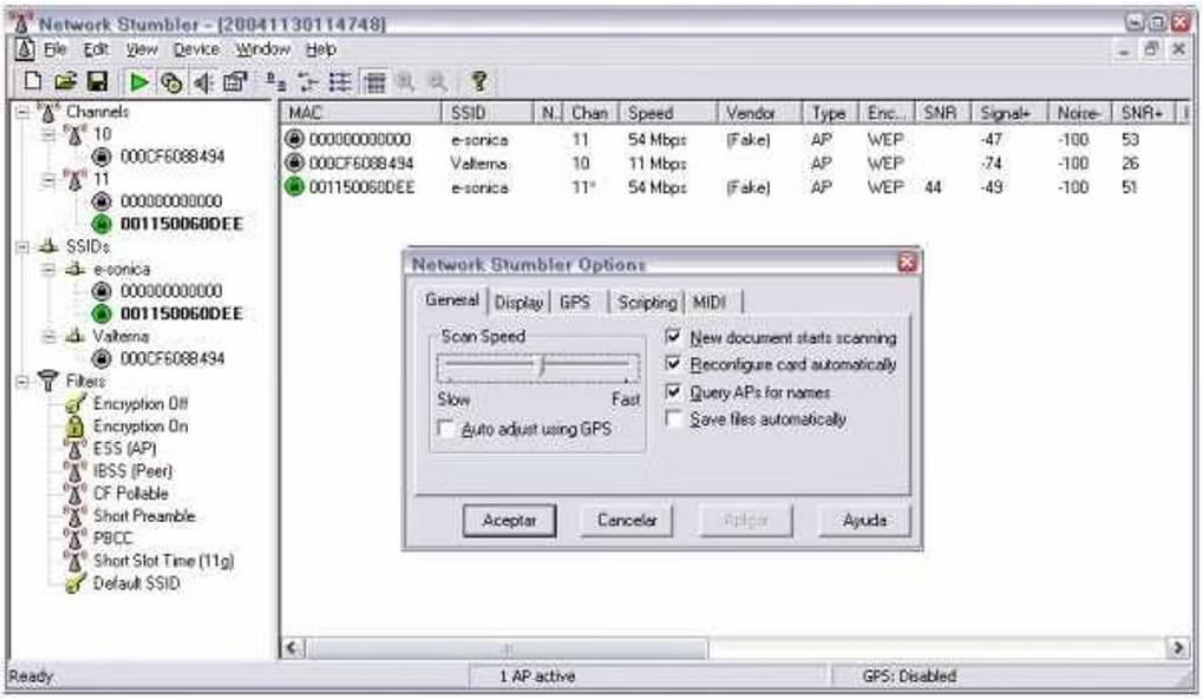
- Kismet operates by placing the wireless network interface card in monitor mode, allowing it to capture packets without connecting to any network.
- It analyzes the captured packets to identify network SSIDs, encryption types, and device details.
- Security professionals use this information to assess network vulnerabilities and implement necessary security measures

NetStumbler

NetStumbler is a Windows-based wireless network discovery tool used for detecting nearby Wi-Fi networks. It is commonly used for wardriving, network optimization, and troubleshooting.

Features of NetStumbler:

1. **Wi-Fi Network Discovery:** NetStumbler scans for available Wi-Fi networks and provides details such as SSID, signal strength, and encryption type.
2. **Graphical User Interface (GUI):** Unlike Kismet, NetStumbler provides an easy-to-use GUI for network analysis.
3. **Signal Strength Analysis:** It helps in identifying weak signals and optimizing Wi-Fi coverage.
4. **Detection of Unauthorized Access Points:** NetStumbler can identify rogue access points that might pose security risks.
5. **Simple and Lightweight:** It is easy to install and requires minimal system resources..
6. **Active Scanning:** NetStumbler actively probes networks, which means it can be detected by



How NetStumbler Works:

- It scans for Wi-Fi signals and collects network information, including SSID, encryption type, and signal strength.
- It displays the detected networks in a user-friendly interface, making it easy to analyze and troubleshoot network issues.
- Unlike Kismet, which passively monitors networks, NetStumbler actively sends probe requests, which can be detected by network administrators.

Applications of Kismet and NetStumbler:

1. **Network Security Auditing:** These tools help in identifying vulnerabilities and unauthorized access points in wireless networks.
2. **Ethical Hacking & Penetration Testing:** Security professionals use these tools to conduct penetration tests and assess network security.
3. **Wi-Fi Optimization:** NetStumbler is particularly useful for improving signal strength and optimizing network coverage.
4. **Wardriving:** Both tools are used to map and analyze wireless networks while moving through different locations.
5. **Intrusion Detection:** Kismet helps detect network intrusions and unauthorized devices.

Limitations of Kismet and NetStumbler:

- **Kismet:** Requires advanced knowledge of Linux and network security concepts; lacks a graphical interface.
- **NetStumbler:** Limited to Windows; does not support packet sniffing; easily detectable by network security systems.

Github Link:

https://github.com/ItsAbdulRehman/Mobile-Computing/tree/main/Experiment%2010/Experiment%2010

Conclusion:

The study of security tools like Kismet and NetStumbler provides insights into wireless network security and auditing techniques. **Kismet** is a powerful tool for passive network monitoring, intrusion detection, and packet sniffing, making it suitable for security professionals and ethical hackers. **NetStumbler**, on the other hand, is useful for network troubleshooting, Wi-Fi optimization, and basic security analysis, but it actively scans networks, making it detectable.