EXPERIMENT NO. 5

AIM: Study working of security tools like Kismet, Netstumbler.

Case Study: Understanding the Functionality and Effectiveness of Kismet Wireless Security Tool.

Introduction to Kismet:

Kismet is an open-source wireless network detector, sniffer, and intrusion detection system. It works with any wireless card that supports raw monitoring mode and can sniff 802.11b, 802.11a, and 802.11g traffic. Kismet is designed to work with Linux operating systems and can be used for wireless network troubleshooting, monitoring, and security assessment.

Objective:

The objective of this case study is to explore the functionality and effectiveness of Kismet as a security tool in identifying and analyzing wireless network threats.

Methodology:

1. **Installation and Setup:** Kismet was installed on a Linux-based system with compatible wireless network interface cards (WNICs) that support monitor mode.

2. **Configuration:** The Kismet configuration file was modified to specify the WNIC to be used and any additional settings required for the analysis.

3. **Data Collection:** Kismet was run in monitoring mode to capture wireless network traffic in the vicinity. Various parameters such as channel hopping interval, packet capture filters, and log verbosity were adjusted based on the specific requirements of the analysis.

4. **Analysis**: The captured data was analyzed using Kismet's built-in features such as packet decoding, signal strength visualization, and network identification. The tool was utilized to identify active wireless networks, rogue access points, unauthorized devices, and potential security threats.

5. **Reporting:** A comprehensive report was generated based on the analysis findings, including details of identified networks, devices, and security vulnerabilities. Recommendations for mitigation strategies were also provided based on the observed threats.

Results:

1. **Network Discovery:** Kismet successfully detected all active wireless networks in the vicinity, including both infrastructure and ad-hoc networks. It provided detailed information such as SSID, BSSID, channel, signal strength, and encryption type for each network.

2. **Rogue Access Point Identification:** Kismet identified several rogue access points operating within the monitored area. These unauthorized access points were flagged for further investigation, as they posed potential security risks to the network infrastructure.

3. **Client Device Tracking:** Kismet tracked the movement of client devices within the wireless network range. It identified devices connecting to multiple access points and detected any unusual behaviour, such as MAC address spoofing or unauthorized network connections.
4. **Security Threats Detection:** Various security threats were identified during the analysis, including rogue access points, unauthorized device connections, weak encryption, and denial-of-service attacks. Kismet's logging and alerting capabilities helped in promptly identifying and mitigating these threats.

Applications of Kismet:

Some common application kismet is used for are:

Wardriving: Mobile detection of wireless networks, logging and mapping of network location, WEP, network name, IP-Range etc.

Site Survey: Monitoring and graphing signal strength and location.

Distributed IDS: Multiple Remote Drone sniffers distributed throughout an installation monitored by a single server and could be combined with a layer 3 IDS like snort.

Rogue Access Point Detection: Stationary or mobile sniffers to enforce site policy against rogue access points.

Conclusion:

Kismet proved to be an effective tool for wireless network security assessment and monitoring. Its ability to detect and analyze wireless network traffic allowed for the identification of security threats and vulnerabilities, enabling proactive measures to safeguard the network infrastructure. By leveraging Kismet's features, organizations can enhance their wireless network security posture and mitigate potential risks effectively.