Vidyavardhini's College of Engineering and Technology, Vasai

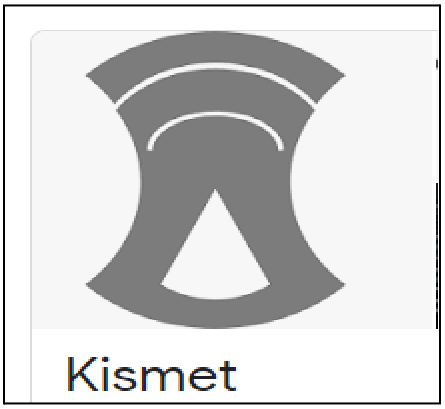
Department of Computer Science & Engineering (Data Science)

Experiment 5

Aim: Exploring wireless security tools like Kismet, NetStumbler etc.

Theory:

Kismet



Introduction:

Kismet is a very powerful wireless sniffing tool that is found in Kali Linux, an operating system designed for ethical hacking and penetration testing.

Kismet's ability to facilitate RFMON (radio frequency monitoring) means that it can monitor traffic and identify wireless networks without having to associate with an access point, unlike other packet-sniffing tools.

Kismet can also detect hidden SSIDs, rogue access points, and spoofed MAC addresses, making it a useful tool for wireless network security and intrusion detection.

Kismet can capture packets from various wireless protocols, Bluetooth, Zigbee, and more. It can also decode and display various types of data, such as GPS coordinates, web pages, images, and voice.

Kismet has a web-based user interface that allows users to view and interact with the captured data in real time.Kismet has been used for various purposes, such as wardriving, wireless network mapping, wireless network auditing, wireless network troubleshooting, and wireless network forensics.

Features of Kismet:

Passive Scanning:Kismet excels in passive scanning, allowing it to detect and analyze wireless networks without actively participating in the network traffic. This makes it less intrusive and stealthy in monitoring.

Packet Capture and Logging: It can capture and log packets from wireless networks, enabling detailed analysis of the wireless communication within the coverage area.

Channel Hopping: Kismet can hop between different channels, providing comprehensive coverage across various frequencies and ensuring that it can detect wireless networks operating on different channels. Device Identification: The tool is capable of identifying and categorizing different types of wireless devices, aiding in understanding the composition of the wireless environment.

Modular Architecture: Kismet's modular architecture allows users to extend its functionality through plugins, making it adaptable to different use cases and environments.

Advantages:
It can run on various operating systems and hardware, such as Linux, macOS, Windows, and Raspberry Pi.
It also has a REST-like API that enables users to control Kismet remotely and integrate it with other tools.

Disadvantages:
It takes a long time to search for networks, especially if there are many channels and devices in the area.
It can only identify the wireless networks in a small area, depending on the range and power of the wireless card and antenna.

Netstumbler

Introduction:

Netstumbler is a Windows-based tool that can discover and monitor wireless networks using the 802.11 a/b/g standards.

Netstumbler's ability to detect wireless interference, rogue access points, and spoofed MAC addresses makes it a useful tool for wireless network security and intrusion detection.

Netstumbler can be used for various purposes, such as wardriving, wireless network auditing, and wireless network troubleshooting.

Netstumbler can also display the network name, signal strength, encryption type, and channel of each network it finds.

Netstumbler has a simple and intuitive user interface that allows users to view and save the captured data. It also has a plug-in system that enables users to extend its functionality with other tools.

Features:

Network Discovery: NetStumbler scans for nearby wireless networks and provides information such as network name (SSID), signal strength, channel, and encryption status.

Signal Strength Monitoring: Users can assess the strength of Wi-Fi signals, helping them optimize the placement of access points and improve overall network performance.

Channel Information: NetStumbler provides details about the channels used by nearby Wi-Fi networks. This information can be crucial for avoiding interference and optimizing channel selection.

GPS Support: NetStumbler can integrate with a GPS device to log the geographical coordinates of discovered networks, enabling users to create maps of wireless networks.

Advantages:

It is easy to use and install, as it does not require any special drivers or hardware.

It can help users find the best location and orientation for their wireless devices, as well as avoid sources of interference and noise.

Disadvantages:

It can only run on Windows operating systems, and not on Linux, macOS, or mobile devices.

It may not be able to detect hidden networks, unless the user knows the network name or has the key or password.

Wifi Analyser

Introduction:

A WiFi analyzer mobile app is a tool designed to help users analyze and optimize their wireless network connections. It provides detailed information about the available WiFi networks in the vicinity, their signal strength, channel utilization, and other relevant data. This app assists users in identifying potential issues and optimizing their WiFi settings for better performance.

Features:

Network Scan: Conducts a comprehensive scan of available WiFi networks, displaying information such as signal strength, channel, and security status.

Signal Strength Meter: Measures the strength of the WiFi signal, helping users identify dead zones and areas with poor connectivity.

Channel Analysis: Analyzes the channels used by nearby WiFi networks, enabling users to choose the least congested channel for improved performance.

Network Security Information: Provides information about the security protocols used by WiFi networks, helping users ensure their own network is secure.

Speed Test: Allows users to perform speed tests to assess the actual data transfer speeds of their WiFi connection.

Signal Graphs: Displays signal strength and channel utilization over time, helping users identify patterns and potential interference.

Device List: Lists the devices connected to the network, allowing users to identify unauthorized or unwanted connections.

WiFi Troubleshooting Tips: Offers suggestions and tips for resolving common WiFi issues, such as interference, low signal strength, or network congestion.

Advantages:

Optimized Performance: Users can optimize their WiFi settings based on the information provided by the app, leading to improved network performance.

Troubleshooting: The app helps users identify and address issues such as interference, weak signals, or security vulnerabilities.
Network Security: By providing information about security protocols, the app assists users in ensuring the safety of their WiFi networks.
User-Friendly: Most WiFi analyzer apps have an intuitive interface, making them accessible even for users with limited technical knowledge.
Cost-Effective: Users can optimize their WiFi networks without the need for additional hardware, making it a cost-effective solution for improving connectivity.

Disadvantages:
Device Compatibility: Some features may be limited by the capabilities of the user's mobile device, and not all devices may support advanced analysis features.
Limited Network Control: While the app provides information and recommendations, users may have limited control over certain settings, especially on mobile devices.
Interference Variability: The app may not always accurately identify sources of interference, as environmental factors can impact signal strength and quality.
Data Privacy Concerns: Users should be cautious about the data collected by the app and ensure that their privacy is protected, especially if the app requires extensive permissions.
Network Changes: Making adjustments based on the app's recommendations may require a good understanding of network settings, and improper changes could potentially disrupt connectivity.