EXPERIMENT 05

Aim: Exploring wireless security tools like Kismet, NetStumbler, Nmap

Theory:
Kismet, NetStumbler, and TrackerJacker are popular wireless security tools that are used to audit and secure wireless networks. In this experiment, we will explore these tools and learn how to use them to identify vulnerabilities and secure wireless networks.

1. Kismet:
Kismet is an open-source wireless network detector, sniffer, and intrusion detection system. It can detect the presence of wireless networks, identify the type of access point (AP), and display detailed information about each network.

Features:
1. Wireless Network Discovery: Kismet can scan for wireless networks within its range and display them in a list with their SSID, signal strength, encryption type, and other details.
2. Real-time Network Monitoring: Kismet continuously monitors the wireless network traffic and displays it in real-time. It can capture packets and display them in a human-readable format.
3. Protocol Support: Kismet supports a wide range of wireless protocols, including 802.11a, b, g, n, and ac. It can also capture traffic from Bluetooth devices and some proprietary protocols.

Advantages:
1. Open-source and free: Kismet is an open-source and free wireless network scanner and intrusion detection system. This makes it an affordable option for individuals and organizations with limited budgets.
2. Compatibility: Kismet supports a wide range of wireless network cards, making it compatible with many different devices. This ensures that users can use Kismet with the hardware they already have.

Disadvantages:
1. Complexity: Kismet can be quite complex to use, especially for beginners. Its interface may not be intuitive, and users may require some technical knowledge to fully utilize its features.
2. Limited functionality: While Kismet is a powerful tool, it may not have all the features that some users need. For example, it may not be as comprehensive as some commercial wireless network scanners in terms of intrusion detection capabilities.

2. NetStumbler:
NetStumbler is a popular wireless network scanner for Windows operating systems. It can detect wireless networks, identify their details, and display them in a user-friendly interface.

Features:
1. Network Discovery: NetStumbler can detect and display a list of wireless networks within range, along with their signal strength, channel, encryption type, and other details.

2. Network Analysis: Once a network is discovered, NetStumbler can provide detailed information about it, such as the network's SSID (network name), MAC address (network adapter's unique identifier), and IP address (network's internet address).
3. Network Security Analysis: NetStumbler can also detect the security measures implemented on a wireless network, such as WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), or WPA2 (Wi-Fi Protected Access II). It can also determine whether the network is using a hidden SSID or not.

Advantages:
1. Network Discovery: NetStumbler is a powerful tool for discovering wireless networks. It can detect hidden and unsecured networks, which can be useful for network administrators and security professionals.
2. Network Analysis: NetStumbler provides detailed information about wireless networks, including signal strength, channel usage, and network security settings. This information can be used to optimize network performance and security.

Disadvantages:
1. Legal Issues: In some countries, using NetStumbler to scan for wireless networks without permission is considered a violation of privacy laws. This can lead to legal issues and fines.
2. Network Disruption: NetStumbler can cause disruption to wireless networks by flooding them with traffic and consuming bandwidth. This can negatively impact network performance and cause connectivity issues for other users.

3. Nmap:
(Network Mapper) Initial release date: September 1997 Developer: Gordon Lyon License: NPSL or modified GPLv2 Nmap (Network Mapper) is a popular open-source network scanning tool used to discover hosts and services on a network. It is available for free on various operating systems, including Linux, macOS, and Windows. In this article, we will discuss the features, use cases, advantages, and disadvantages of Nmap.

Features:
1. Port Scanning: Nmap can scan a range of IP addresses and ports to identify open, closed, or filtered ports. It can also perform stealth scans to avoid detection.
2. Service Detection: Nmap can detect the services running on open ports and identify the operating system and version of the device.
3. Network Mapping: Nmap can create a visual map of the network by scanning multiple IP ranges and displaying the results in a graphical format.

Advantages:

1. Open-Source: Nmap is an open-source tool that is free to use and customize according to specific requirements.
2. Cross-Platform: Nmap is available for various operating systems, making it easy to use on different devices.

Disadvantages:

1. False Positives: Nmap may sometimes report false positives due to outdated service signatures or incorrect port identification. This can lead to unnecessary alerts and false alarms.
2. Resource Intensive: Running a large-scale scan using Nmap can be resource-intensive and may require significant processing power and bandwidth resources. This can impact network performance during scans.

Conclusion:

we explored wireless security tools like Kismet, NetStumbler, and Nmap, each offering unique features for auditing and securing wireless networks. Kismet provides real-time monitoring and protocol support, while NetStumbler offers user-friendly network discovery and analysis specifically for Windows systems. Nmap, on the other hand, is a versatile network scanning tool used for discovering hosts, services, and network mapping across various operating systems. While these tools offer valuable insights into wireless network security, users should be aware of their complexities, legal implications, and resource requirements to effectively utilize them in securing their networks.