BARI ANKIT (56)

Exp 5 : Exploring wireless security tools like Kismet, NetStumbler etc.

**Exploring Wireless Security Tools: Kismet, NetStumbler, and Others**

**Wireless network security is a critical area of cybersecurity that focuses on protecting wireless communication systems, particularly Wi-Fi networks. Various tools have been developed to help analyze, monitor, and secure wireless networks. Among the most popular tools are Kismet, NetStumbler, and others like Aircrack-ng, Wireshark, and Reaver. These tools are commonly used for network reconnaissance, identifying vulnerabilities, and conducting penetration testing.**

**Below is an overview of some of the most widely-used wireless security tools, including Kismet and NetStumbler.**

---

**1. Kismet**

**Kismet is a popular wireless network detector, sniffer, and intrusion detection system. It can be used to identify hidden wireless networks, analyze the traffic, and capture data packets. It works with Wi-Fi, Bluetooth, and other wireless technologies.**

**Key Features:**

- **Wireless Network Detection: Kismet detects all wireless networks in range, including hidden networks (networks with SSIDs not broadcasted).**
- **Packet Sniffing: It captures raw network packets and analyzes traffic over wireless networks. This includes monitoring 802.11 (Wi-Fi), Bluetooth, and other radio technologies.**
- **Intrusion Detection: Kismet can be configured to detect rogue access points, misconfigured routers, and de-authentication attacks.**
- **GPS Integration: Kismet supports GPS tracking for mapping the location of wireless networks.**
- **File Logging: It allows for logging of raw packets in a format that can be analyzed later, and supports tcpdump, Wireshark, or Aircrack-ng for further analysis.**

**How to Use Kismet:**

1. **Installation: Kismet can be installed on Linux, macOS, or BSD systems. It requires the installation of dependencies such as libpcap.**
    - **On Ubuntu:**
    - **sudo apt-get install kismet**
2. **Running Kismet: Once installed, run it with superuser privileges.**
3. **sudo kismet**

4. **Detecting Networks: Kismet will automatically detect and list available wireless networks along with information such as SSID, BSSID (MAC address of AP), signal strength, encryption type, and more.**

**Usage Scenarios:**

- **Wireless Network Auditing: Detect unauthorized access points, assess signal strength, and ensure proper configuration of wireless networks.**
- **Intrusion Detection: Use Kismet for real-time monitoring of suspicious activities, such as rogue APs or man-in-the-middle (MITM) attacks.**
- **Penetration Testing: Analyze wireless network traffic to exploit vulnerabilities or crack WEP/WPA passwords (often used with tools like Aircrack-ng).**

---

**2. NetStumbler**

**NetStumbler is an older Windows-based wireless network discovery tool. It is primarily used for detecting Wi-Fi networks in the vicinity and provides useful information about their configurations. It is mainly a tool for network mapping, signal strength analysis, and detecting rogue access points.**

**Key Features:**

- **Wireless Network Discovery: NetStumbler detects and maps out nearby wireless networks, showing details like SSID, BSSID, encryption type, channel, and signal strength.**
- **Signal Strength Meter: Provides a visual representation of the signal strength of networks in the area.**
- **Geographical Mapping: It can be used with a GPS to map the locations of wireless networks and their coverage areas.**
- **Encryption Detection: It can detect networks using WEP, WPA, or WPA2 encryption, helping assess the security of wireless networks.**
- **Support for 802.11b/g networks.**

**How to Use NetStumbler:**

1. **Installation: NetStumbler is available for Windows and can be downloaded from the official website (though it is outdated).**
2. **Running NetStumbler: After installation, run the software to start scanning for nearby Wi-Fi networks.**
3. **Analysis: NetStumbler displays network information like SSID, BSSID, signal strength, and encryption type.**

**Usage Scenarios:**

- **Wi-Fi Network Mapping: Use NetStumbler for discovering nearby wireless networks, assessing signal strength, and mapping coverage.**
- **Wireless Troubleshooting: Identify weak signal areas and plan network deployment.**
- **Wireless Security: Detect insecure networks (e.g., those still using WEP encryption) and unauthorized access points.**

---

**3. Aircrack-ng**

**Aircrack-ng is a powerful and comprehensive Wi-Fi network security auditing tool suite. It is used to monitor, attack, and crack WEP, WPA, and WPA2 encrypted networks. It is one of the most popular tools for cracking Wi-Fi passwords and performing security assessments.**

**Key Features:**

- **Packet Capture: Aircrack-ng captures and analyzes packets to recover WEP/WPA keys.**
- **Cracking WEP/WPA Keys: The tool uses brute force, dictionary-based, and other attacks to crack WEP and WPA keys.**
- **Monitoring Mode: Aircrack-ng allows wireless interfaces to switch to monitor mode, where they can passively listen for all traffic on a wireless network.**
- **Injection: It allows for packet injection, which is useful for de-authentication attacks to capture handshake packets.**
- **Cracking WPA Handshakes: With the right dictionary file, Aircrack-ng can crack WPA and WPA2 handshakes.**

**How to Use Aircrack-ng:**

1. **Installation: Install it using the package manager on Linux or through the Aircrack-ng website.**
    - **On Ubuntu:**
    - **sudo apt-get install aircrack-ng**
2. **Monitoring: Start by enabling monitor mode on the wireless interface.**
3. **sudo airmon-ng start wlan0**
4. **Packet Capture: Use airodump-ng to capture packets and look for a WPA/WPA2 handshake.**
5. **sudo airodump-ng wlan0mon**
6. **Cracking: Once you have captured the handshake, use aircrack-ng to attempt to crack the password using a dictionary file.**
7. **aircrack-ng capture_file.cap -w dictionary.txt**

**Usage Scenarios:**

- **Penetration Testing: Test the strength of encryption on Wi-Fi networks.**
- **Cracking WEP/WPA: Use Aircrack-ng to recover Wi-Fi passwords from network traffic.**
- **Wi-Fi Network Auditing: Ensure that networks are securely configured and are not vulnerable to known attacks.**

---

**4. Wireshark**

**Wireshark is a powerful network protocol analyzer that captures and analyzes network traffic. It can be used to inspect the packets transmitted over wireless networks.**

**Key Features:**

- **Packet Sniffing: Wireshark captures packets from network traffic and allows users to inspect raw data.**
- **Wi-Fi Network Traffic: It supports 802.11 Wi-Fi traffic capture.**
- **Deep Protocol Analysis: Wireshark can decode hundreds of protocols and give you detailed information on each packet captured.**
- **Filters: Use advanced filtering to capture only relevant packets (e.g., only Wi-Fi traffic or packets from a specific IP).**
- **Exporting Data: It allows the export of captured data for analysis and reporting.**

**How to Use Wireshark:**

1. **Installation: Wireshark can be installed on Windows, macOS, and Linux from the official website.**
2. **Capture Packets: Select your wireless network interface and start capturing packets.**
3. **Analyze Traffic: Use filters to examine specific packets (e.g., 802.11 frames, handshakes, EAP authentication).**

**Usage Scenarios:**

- **Network Traffic Analysis: Inspect the traffic on wireless networks and identify malicious activity.**
- **Security Auditing: Use Wireshark to find sensitive data (e.g., unencrypted passwords) transmitted over Wi-Fi networks.**
- **Packet Decoding: Inspect the structure of Wi-Fi frames, including encryption and authentication methods.**

---

**5. Reaver**

**Reaver is a Wi-Fi Protected Setup (WPS) brute-forcing tool. It is used to attack WPS-enabled routers and recover their PINs, which can then be used to derive the WPA/WPA2 password.**

**Key Features:**

- **WPS PIN Brute-Forcing: Reaver exploits a vulnerability in WPS to recover the 8-digit PIN.**
- **Cracking WPA Passwords: Once the PIN is found, it can be used to recover the WPA password.**

**How to Use Reaver:**

1. **Installation: Reaver can be installed on Linux using the package manager or by cloning from the GitHub repository.**

2. **sudo apt-get install reaver**
3. **Running Reaver: Once the tool is installed, it can be used to launch a brute-force attack against the WPS PIN of a router.**
4. **sudo reaver -i wlan0mon -b [BSSID] -c [channel] -vv**

**Usage Scenarios:**

- **WPS Cracking: Recover WPA/WPA2 passwords from routers with WPS enabled using brute-force attacks.**
- **Wi-Fi Penetration Testing: Test the strength of WPS implementations in consumer routers.**