Don Bosco Institute of Technology, Kurla(W)
Department of Computer Engineering
CSL603 - Mobile Computing Lab 2023-24

Experiment 10

Name: Jess John Roll no.: 32 Batch: B

Aim: Study of security tools like Kismet, Netstumbler.

Theory: Kismet and NetStumbler are both widely-used security tools in the realm of network monitoring and security assessment, particularly for wireless networks.

Kismet:

Purpose: Kismet is primarily designed as a wireless network detector, sniffer, and intrusion detection system. It's used to detect hidden wireless networks, track network activity, and identify unauthorized access points.

Features:

1. Passive Scanning: Kismet passively scans for wireless networks without actively transmitting any data, making it stealthier and less likely to be detected.
2. Packet Sniffing: It captures data packets transmitted over wireless networks, allowing for analysis of network traffic and identification of potential security threats.
3. Wireless Intrusion Detection System (WIDS): Kismet can detect unauthorized access points, rogue devices, and potential attacks on wireless networks.
4. Cross-Platform Compatibility: It's available for various platforms including Linux, macOS, and Windows, making it versatile for different environments.
5. Customization: Users can customize Kismet's settings and filters to tailor it to their specific monitoring needs.

Use Cases:

- Security professionals use Kismet to identify and mitigate security vulnerabilities in wireless networks.
- It's employed by organizations to ensure compliance with security policies and regulations regarding wireless network security.
- Penetration testers utilize Kismet to assess the security posture of wireless networks during security assessments.

NetStumbler:

Purpose: NetStumbler is a wireless network scanner and detector primarily used for Windows operating systems. It's designed to detect and analyze wireless networks within range of the user's device.

Features:

1. Network Discovery: NetStumbler scans for available wireless networks and provides information such as SSID, signal strength, encryption status, and channel.
2. Signal Strength Mapping: It displays signal strength measurements, allowing users to map out the coverage area of wireless networks.

3. Wireless Network Troubleshooting: NetStumbler can assist in troubleshooting wireless network connectivity issues by identifying signal interference and overlapping channels.
4. Wardriving: While not its intended purpose, NetStumbler can be used for wardriving, which involves driving around to detect and map out wireless networks.

Use Cases:

- IT professionals use NetStumbler to survey wireless networks, identify coverage areas, and optimize network performance.
- Security analysts employ NetStumbler to detect unauthorized access points and identify potential security vulnerabilities in wireless networks.
- Enthusiasts may use NetStumbler for wardriving activities, although its usage for such purposes may be subject to legal restrictions in some jurisdictions.

Both Kismet and NetStumbler play crucial roles in assessing the security and performance of wireless networks, albeit with slightly different focuses and feature sets.