Vidya Vikas Education Trust's
Universal College of Engineering, Kaman Road, Vasai – 401208
Accredited A Grade by NAAC

Experiment No :10

Aim: Study of security tools (like Kismet,Netstumbler).

Theory:

With the rise of mobile computing, wireless communication technologies such as Wi-Fi, Bluetooth, and cellular networks have become essential. While these technologies provide flexibility and convenience, they also introduce various security risks. The most prevalent threats include unauthorized access, eavesdropping, and network intrusions.

To mitigate these risks, specialized security tools like Kismet and NetStumbler are used. These tools help in detecting unauthorized access points, assessing network vulnerabilities, and ensuring security compliance. They play a crucial role in protecting wireless networks from potential breaches and attacks.

1. Kismet:

Kismet is an open-source tool designed for wireless network detection, packet sniffing, and intrusion detection. It works by passively monitoring network traffic, identifying active wireless networks, and capturing data packets without sending any signals that might alert intruders.

Features of Kismet:

- Identifies hidden and rogue access points.
- Supports multiple wireless adapters for extensive scanning.
- Captures and analyzes network traffic for security monitoring.
- Provides detailed information such as SSID, encryption type, and signal strength.

How Kismet Works:

Kismet operates in a non-intrusive manner, meaning it does not interact with networks directly. Instead, it passively collects data by listening to wireless signals, allowing it to detect network vulnerabilities and unauthorized devices without being easily detected.

2. NetStumbler:

NetStumbler is a widely used tool for detecting wireless networks, primarily on Windows platforms. While newer tools have emerged, it remains a useful option for network security assessments, especially in mapping available networks and assessing their security configurations.

Features of NetStumbler:

- Detects available wireless networks and measures signal strength.
- Verifies security settings, including WEP, WPA, and WPA2 encryption.
- Integrates with GPS to map the physical locations of networks.

- Identifies unsecured or weakly protected networks.

How NetStumbler Works:

NetStumbler actively scans for wireless networks and provides a comprehensive view of available access points. It is often used for wardriving, where users search for wireless networks while moving around. It helps in analyzing security configurations and identifying potential vulnerabilities.

Methodology:

To evaluate the effectiveness of Kismet and NetStumbler in securing mobile computing environments, the following steps will be carried out in a controlled setup:

1. Configure multiple wireless access points (APs) with varying security settings, such as WEP, WPA, and WPA2.
2. Utilize Kismet and NetStumbler to scan the environment and detect available networks.
3. Analyze the efficiency of these tools in identifying security vulnerabilities and network configurations.
4. Assess their usability for both experienced professionals and beginners.
5. Compare their detection capabilities in identifying hidden and unsecured networks.

Conclusion:

By studying Kismet and NetStumbler, valuable insights can be gained into improving wireless network security in mobile computing. These tools aid network administrators and users in detecting potential threats, securing their networks, and preventing unauthorized access, ultimately strengthening overall network security.