



Experiment No: 10

Aim: Study of security tools like **Kismet** and **NetStumbler**

Theory: Wireless networks are widely used in modern communication systems, but they are also vulnerable to security threats such as unauthorized access, data interception, and rogue access points. Security tools like Kismet and NetStumbler help network administrators, cybersecurity professionals, and ethical hackers analyze, secure, and troubleshoot wireless networks.

1. Kismet

Kismet is a passive wireless network sniffer and intrusion detection system (IDS) that works by capturing network packets without actively probing the network.

```
Kismet Sort View Windows
Name      BSSID      T C  Ch Freq  Pkts  Size Bcr% Sig Clnt Manuf      Cty Seen By      DRD1812
TRENDnet  00:14:D1:5F:97:12 A 0  1 2417    1 0B --- --- 1 TrendwareI --- wlan0      Networks
linksys_SES_45997 00:16:B6:1B:E4:FF A 0  6 2447    2 0B --- --- 1 Cisco-Link --- wlan0      17
QQFP93   00:1F:90:F2:CD:C2 A W  1 2412    3 0B --- --- 1 ActiontecE US wlan0      Packets
landscapers 00:14:BF:07:2F:84 A N  6 2437    4 0B --- --- 1 Cisco-Link --- wlan0      1813
linksys   00:1A:70:D9:BC:13 A N  6 2437    5 0B --- --- 1 Cisco-Link --- wlan0
HPAA1    00:1F:90:E6:E0:84 A W  11 2462    5 0B --- --- 1 ActiontecE --- wlan0
65103    00:1F:90:FA:F4:C8 A W  --- 2412    9 0B --- --- 1 ActiontecE --- wlan0
Autogroup Probe 00:13:E8:92:3F:CB P N  --- --- 10 0B --- --- 1 IntelCorpo --- wlan0
TFS       00:09:5B:07:9D:B2 A N  11 2462   13 0B --- --- 1 Netgear --- wlan0
meskas    00:18:01:F5:65:E1 A 0  11 2462   17 0B --- --- 1 ActiontecE US wlan0
Xu Chen   00:18:01:F9:70:F0 A N  6 2442   19 0B --- --- 1 ActiontecE US wlan0
TK421     00:18:01:FE:68:77 A 0  6 2442   23 0B --- --- 1 ActiontecE --- wlan0
Elina-PC-Wireless 00:24:B2:0E:E6:E2 A 0  --- --- --- --- --- --- --- wlan0
7J4R0     00:1F:90:E6:04:F1 A W  --- --- --- --- --- --- --- wlan0
Pickles   00:1F:33:F3:C5:4A A 0  --- --- --- --- --- --- --- wlan0
38c8      00:16:CE:07:60:77 A W  --- --- --- --- --- --- --- wlan0
Danish Penguin 00:13:10:35:59 CB A W  --- --- --- --- --- --- --- wlan0
BSSID: 00:13:10:35:59 CB Crypt: WEP Manuf:

( ) Lock (*) Hop ( ) Dwell
Channels 157,3,7,11,48,64,161,4,8,36,52,149,165
Rate 3
[ Cancel ] [ Change ]

No GPS info (GPS not connected)
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
ERROR: Could not connect to the spectools server localhost:30569
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
wlan0
9
```



Features of Kismet:

- Packet Sniffing: Captures raw data packets from the air without connecting to networks.
- Hidden SSID Detection: Identifies wireless networks that do not broadcast their SSID.
- Intrusion Detection: Helps in finding unauthorized access points and security threats.
- GPS Integration: Can be used for wardriving to map wireless networks with location data.
- Multiple Wireless Card Support: Works with various Wi-Fi interfaces to capture more data.

Use Cases of Kismet:

- Penetration Testing: Identifying vulnerabilities in wireless networks.
- Network Security Auditing: Monitoring for unauthorized Wi-Fi activity.
- Forensic Investigations: Analyzing captured network packets for security incidents.

Limitations of Kismet:

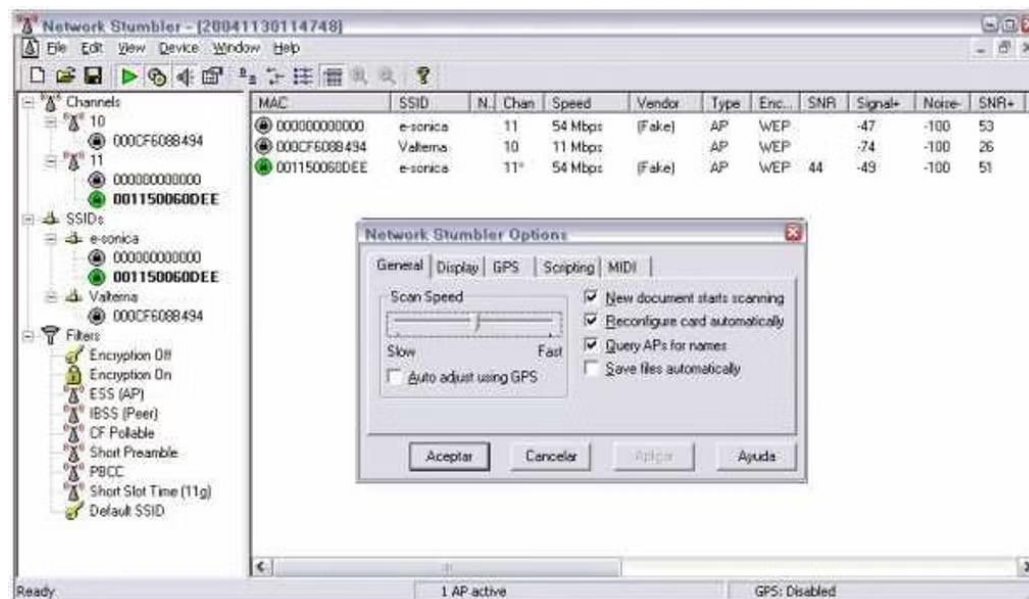
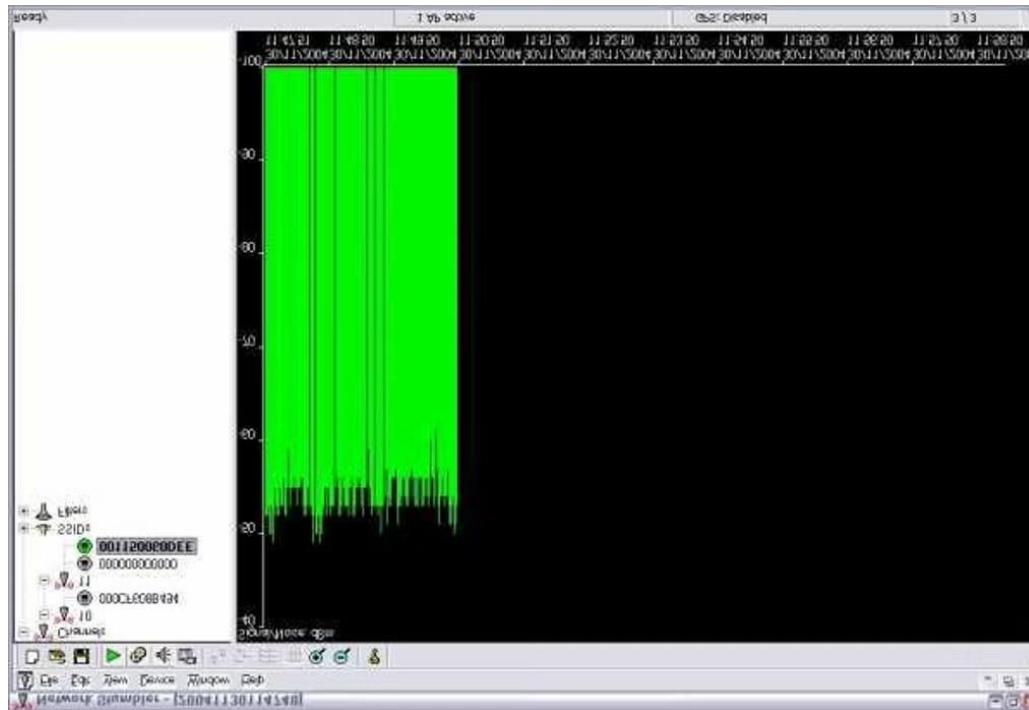
- Requires compatible wireless network cards that support monitor mode.
- Command-line interface (CLI) can be challenging for beginners.

Platform Support:

- Linux, macOS, Windows (limited support)

2. NetStumbler

NetStumbler is an active wireless network discovery tool that scans for available networks and gathers information such as signal strength, security type, and access point details.





Features of NetStumbler:

- Wi-Fi Network Discovery: Identifies all nearby wireless networks.
- Signal Strength Analysis: Helps in optimizing the placement of Wi-Fi routers.
- Rogue Access Point Detection: Detects unauthorized or misconfigured access points.
- Graphical User Interface (GUI): Easy to use for beginners.
- GPS Support: Used for wardriving to map Wi-Fi networks.

Use Cases of NetStumbler:

- Network Optimization: Finding the best placement for Wi-Fi access points.
- Troubleshooting Connectivity Issues: Identifying interference and weak signal areas.
- Wireless Security Audits: Detecting unauthorized networks in an organization.

Limitations of NetStumbler:

- Does not support hidden SSID detection.
- Not effective on modern Windows versions (last updated for Windows XP).
- Cannot capture network packets like Kismet.

Platform Support:

- Windows

GitHubLink: <https://github.com/katyayan14/Mobile-Computing-Exp/tree/main/Exp%2010%20Security%20Tools>

Conclusion: The study of security tools like Kismet and NetStumbler is essential for understanding wireless network security, network monitoring, and intrusion detection.

- Kismet is a passive tool used for packet sniffing, hidden SSID detection, and intrusion detection, making it ideal for network security auditing and penetration testing.
- NetStumbler is an active tool used for Wi-Fi network discovery, signal strength analysis, and rogue AP detection, making it useful for network optimization and troubleshooting.