Experiment No: 10

Aim: Study of Security Tools - Kismet and NetStumbler

Introduction:

Wireless networks have become an integral part of modern communication, but they are vulnerable to various security threats. Unauthorized access, data interception, and rogue access points pose significant risks. To address these concerns, network administrators and cybersecurity professionals use security tools like Kismet and NetStumbler to analyze, secure, and troubleshoot wireless networks.

Objective:

The primary objective of this case study is to explore the functionality, features, and applications of Kismet and NetStumbler as security tools in wireless networks.

Background:

Wireless security tools play a crucial role in identifying vulnerabilities in network infrastructure. Kismet and NetStumbler are widely used for detecting wireless networks, analyzing traffic, and identifying unauthorized devices.

1. Kismet

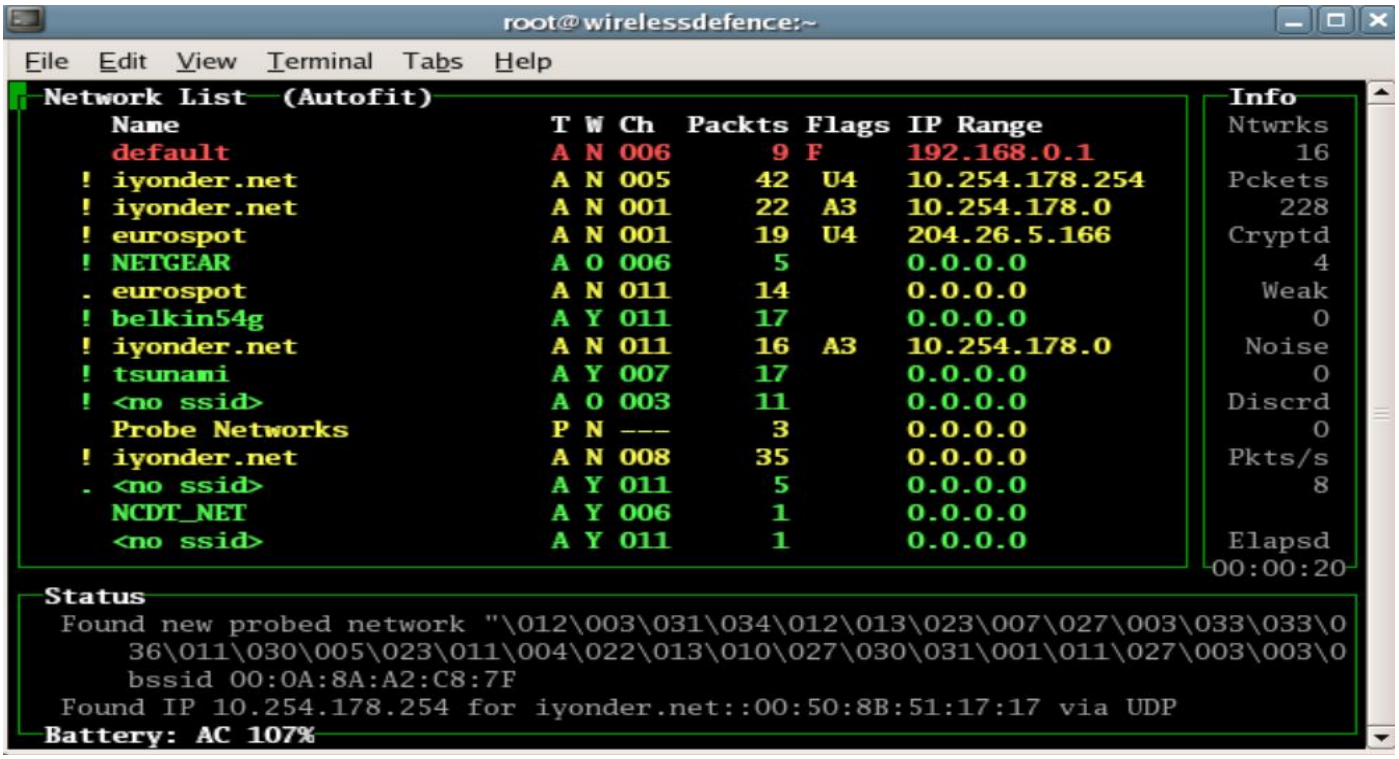
Kismet is an open-source, passive wireless network detector and intrusion detection system. It operates by capturing network packets without actively probing the network.

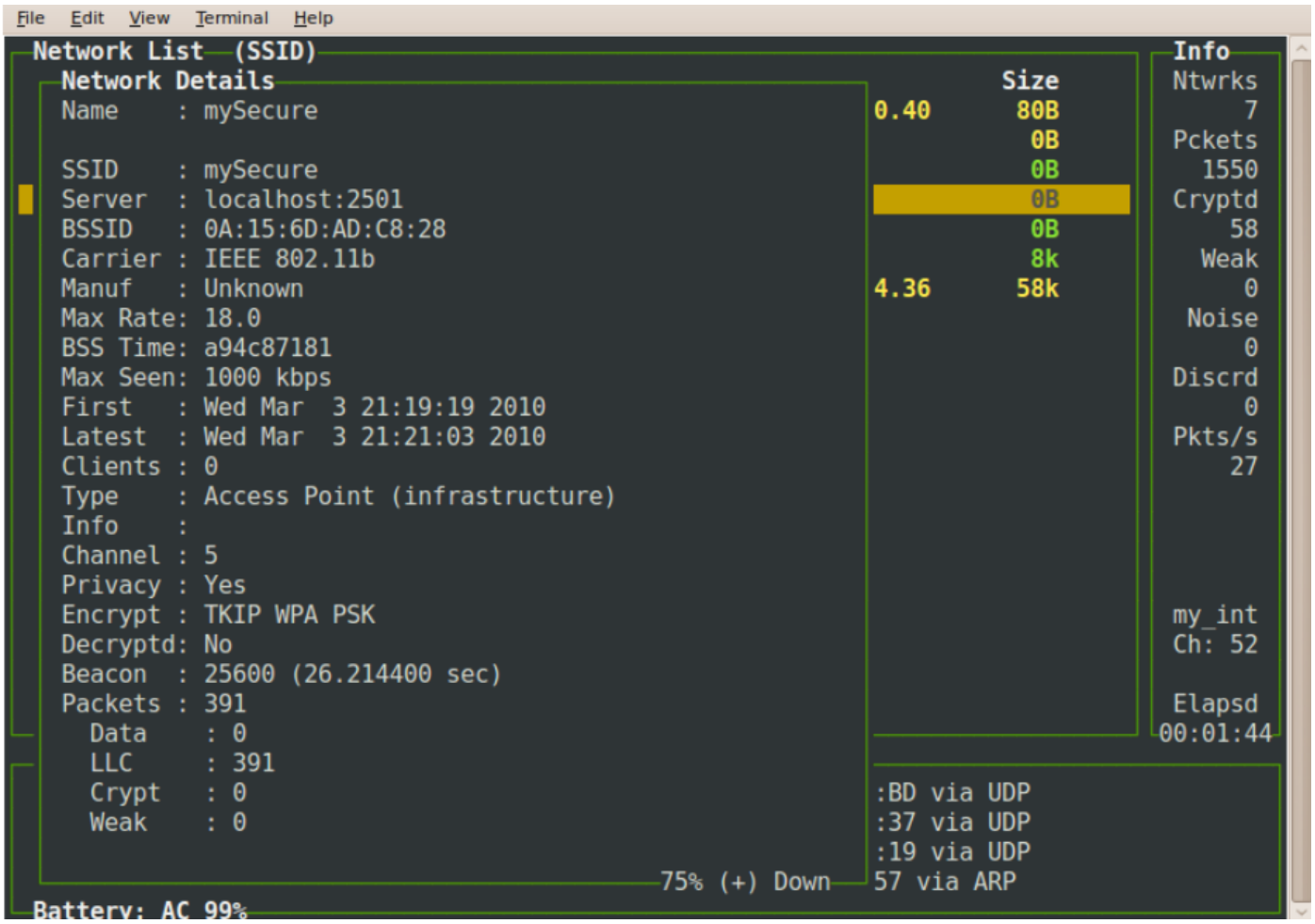
Features:

- Packet Sniffing: Captures raw data packets from wireless networks.
- Hidden SSID Detection: Identifies networks that do not broadcast their SSID.
- Intrusion Detection: Recognizes unauthorized access points and security threats.
- GPS Integration: Helps in mapping detected networks with location tracking.

Use Cases:

- Identifying rogue access points in corporate environments.
- Detecting unauthorized devices in restricted areas.
- Conducting security audits for wireless network infrastructure.


root@wirelessdefence:~
File Edit View Terminal Tabs Help
Network List (Autofit)
Name T W Ch Packts Flags IP Range
default A N 006 9 F 192.168.0.1
! iyonder.net A N 005 42 U4 10.254.178.254
! iyonder.net A N 001 22 A3 10.254.178.0
! eurospot A N 001 19 U4 204.26.5.166
! NETGEAR A O 006 5 0.0.0.0
. eurospot A N 011 14 0.0.0.0
! belkin54g A Y 011 17 0.0.0.0
! iyonder.net A N 011 16 A3 10.254.178.0
! tsunami A Y 007 17 0.0.0.0
! <no ssid> A O 003 11 0.0.0.0
Probe Networks P N --- 3 0.0.0.0
! iyonder.net A N 008 35 0.0.0.0
. <no ssid> A Y 011 5 0.0.0.0
NCDT_NET A Y 006 1 0.0.0.0
<no ssid> A Y 011 1 0.0.0.0
Info
Ntwrks 16
Pckets 228
Cryptd 4
Weak 0
Noise 0
Discrd 0
Pkts/s 8
Elapsd 00:00:20
Status
Found new probed network "\012\003\031\034\012\013\023\007\027\003\033\033\036\011\030\005\023\011\004\022\013\010\027\030\031\001\011\027\003\003\0
bssid 00:0A:8A:A2:C8:7F
Found IP 10.254.178.254 for iyonder.net::00:50:8B:51:17:17 via UDP
Battery: AC 107%


File Edit View Terminal Help
Network List (SSID)
Network Details
Name : mySecure
SSID : mySecure
Server : localhost:2501
BSSID : 0A:15:6D:AD:C8:28
Carrier : IEEE 802.11b
Manuf : Unknown
Max Rate: 18.0
BSS Time: a94c87181
Max Seen: 1000 kbps
First : Wed Mar 3 21:19:19 2010
Latest : Wed Mar 3 21:21:03 2010
Clients : 0
Type : Access Point (infrastructure)
Info :
Channel : 5
Privacy : Yes
Encrypt : TKIP WPA PSK
Decryptd: No
Beacon : 25600 (26.214400 sec)
Packets : 391
Data : 0
LLC : 391
Crypt : 0
Weak : 0
Size
0.40 80B
0B
0B
0B
8k
4.36 58k
:BD via UDP
:37 via UDP
:19 via UDP
75% (+) Down 57 via ARP
Info
Ntwrks 7
Pckets 1550
Cryptd 58
Weak 0
Noise 0
Discrd 0
Pkts/s 27
my_int
Ch: 52
Elapsd 00:01:44
Battery: AC 99%

2. NetStumbler

NetStumbler is a Windows-based wireless network discovery tool that actively scans for available networks and provides detailed information about them.

- **Features:**
  - Active Scanning: Detects nearby wireless networks.
  - Signal Strength Measurement: Helps in optimizing network placement.
  - SSID and Channel Detection: Displays detailed network information.
  - GPS Support: Assists in wardriving (mapping of wireless networks).
- **Use Cases:**
  - Network troubleshooting and performance optimization.
  - Identifying weak signal areas for better coverage planning.
  - Wardriving for mapping and securing networks against unauthorized access.

Platform Support:

- Windows

Case Scenario:

A large organization suspected unauthorized access points in its premises. The IT security team used Kismet to passively scan the environment and identified multiple rogue access points. Additionally, they employed NetStumbler to actively scan and analyze signal strength, optimizing their Wi-Fi deployment. The combined use of these tools helped secure their network against unauthorized intrusions.

GitHubLink:

https://github.com/ganeshgupta2004/Mobile-Computing-VI/tree/main/Exp-10%20MC

Conclusion:

Kismet and NetStumbler serve as effective tools in wireless network security. While Kismet is ideal for passive network monitoring and intrusion detection, NetStumbler excels in active network discovery and optimization. Understanding their functionalities helps security professionals strengthen network defenses and mitigate security risks.