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 - Kismet and NetStumbler

Introduction:

Wireless networks are a fundamental part of modern communication, but they are prone to various security risks, including unauthorized access, data breaches, and rogue access points. To mitigate these threats, cybersecurity professionals and network administrators rely on specialized security tools like Kismet and NetStumbler. These tools help in monitoring, securing, and troubleshooting wireless networks effectively.

Objective:

The main goal of this case study is to understand how Kismet and NetStumbler function, their key features, and their role in enhancing wireless network security.

Background:

Security tools for wireless networks are essential in identifying potential vulnerabilities in network infrastructure. Kismet and NetStumbler are commonly used for detecting wireless networks, analyzing network traffic, and pinpointing unauthorized or suspicious devices.

1. Kismet

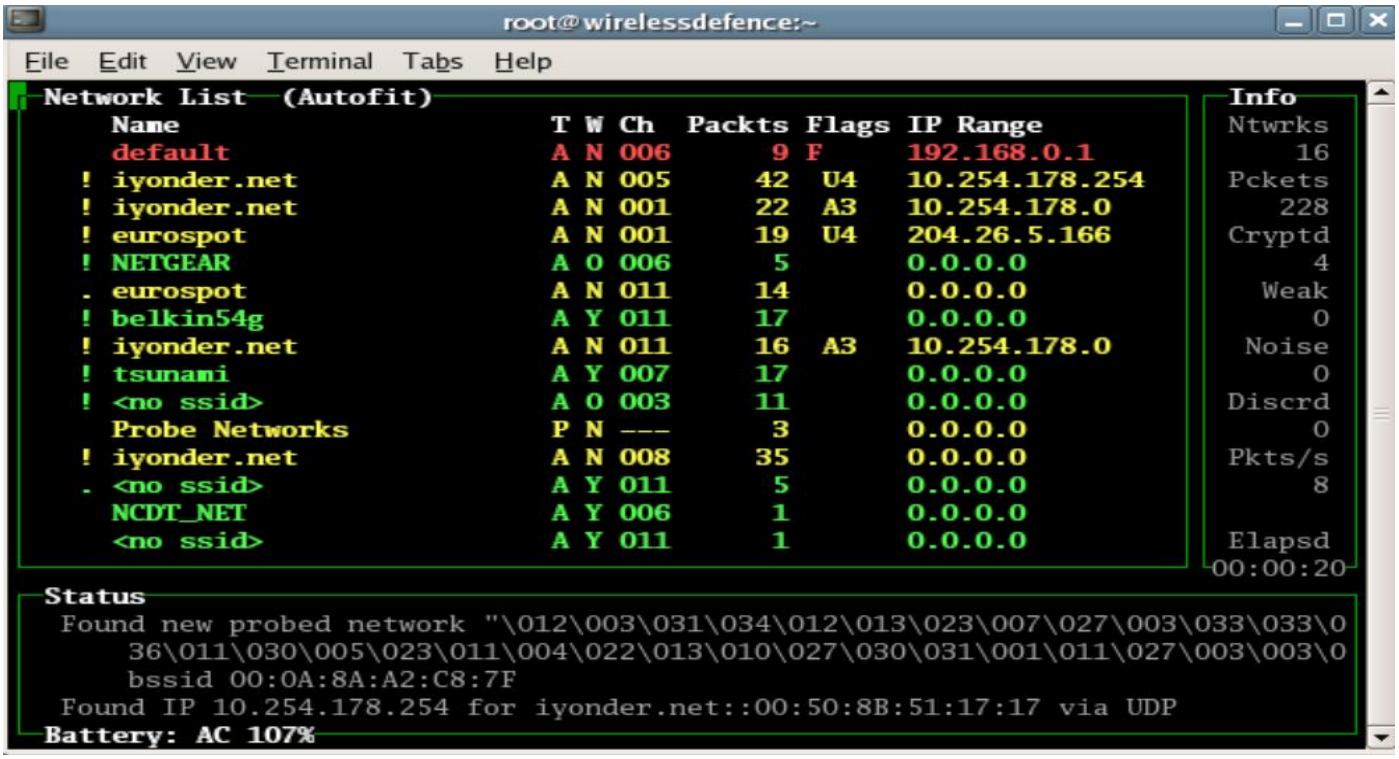
Kismet is a freely available, open-source tool used for wireless network detection and intrusion detection. Unlike active scanning tools, it works passively by capturing network packets without directly interacting with the network..

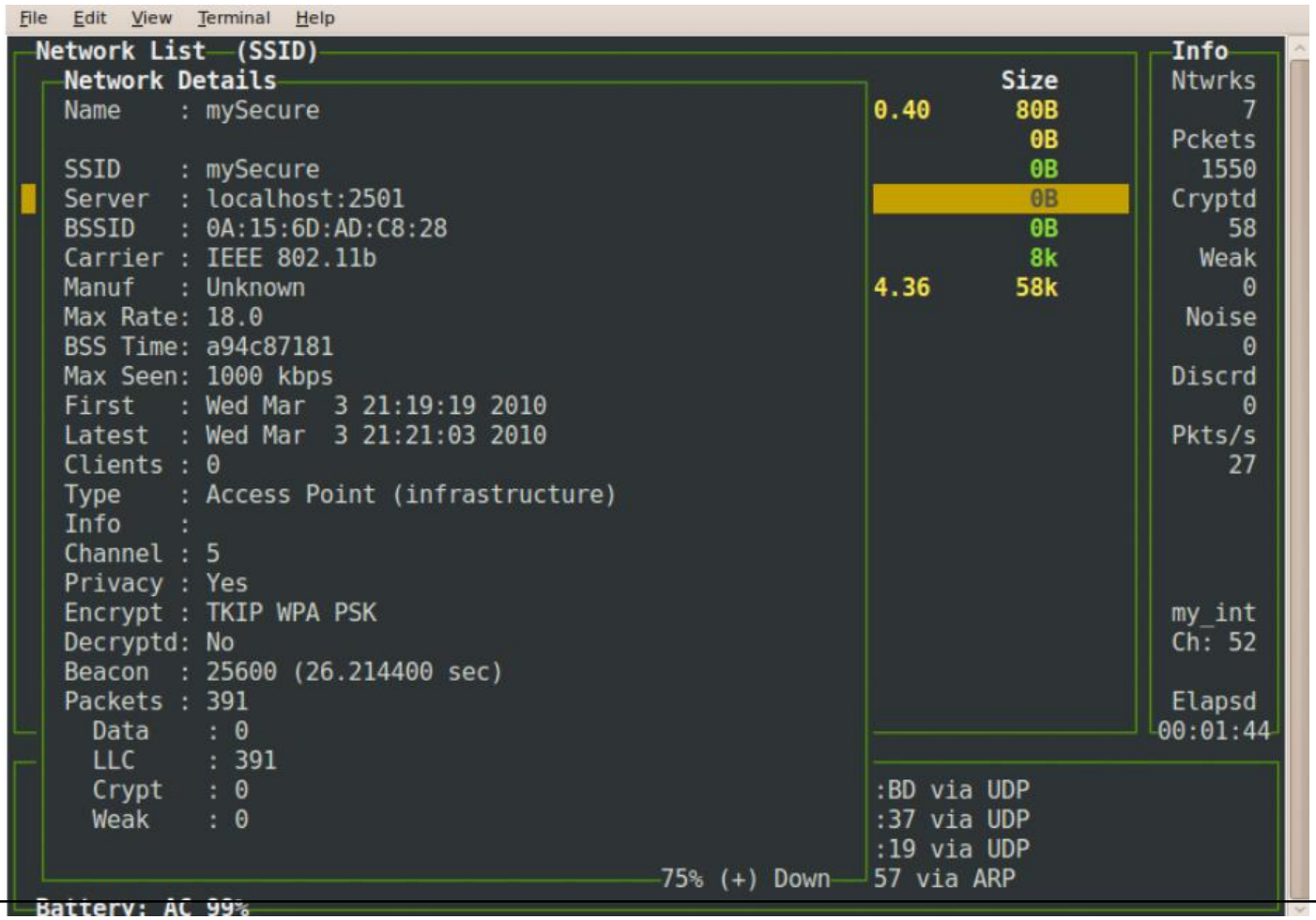
Features:

- **Packet Sniffing:** Captures raw data packets from wireless networks for analysis.
- **Hidden SSID Detection:** Detects networks that are not openly broadcasting their SSID.
- **Intrusion Detection:** Identifies unauthorized access points and potential security threats.
- **GPS Integration:** Allows mapping of detected networks using 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
0B
8k
4.36 58k
:BD via UDP
:37 via UDP
:19 via UDP
57 via ARP
75% (+) Down
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 tool designed for wireless network discovery. Unlike passive tools like Kismet, NetStumbler actively scans for available networks and provides detailed insights about them.

- **Features:**
  - **Active Scanning:** Actively detects and lists nearby wireless networks.
  - **Signal Strength Measurement:** Helps in analyzing and optimizing network coverage.
  - **SSID and Channel Detection:** Displays essential details such as network name (SSID) and channel usage.
  - **GPS Support:** Assists in wardriving by mapping wireless networks based on location.
- **Use Cases:**
  - Troubleshooting network issues and improving performance.
  - Identifying areas with weak signals to optimize coverage.
  - Mapping wireless networks to enhance security and prevent 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/ManavWaghela/mobile-computing/tree/main/Experiment%2010

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.