UNIVERSAL

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:

Introduction

Wireless networks are more convenient than wired networks and allow you to move from room to room in your home. Further, with a advance- ment in wireless hardware, higher throughput and lower latency support has become possible. But they can also be more vulnerable if not properly secured. If our wireless network is 'unsecured' or 'open' then an intruder can easily gain access to our internal network resources as well as to the Internet, all without our consent.

Once the intruder has access to our network, he/she can use it for a variety of operations, such as:

- To steal your Internet bandwidth.
- To perform disruptive or illegal acts.
- To steal your sensitive information.
- To perform Denial-of-Service (DoS) attacks to make the network unusable by sending out false requests.
- To infect the network with malicious threats

Thus, wireless networking is inherently risky because we are transmitting information via radiowaves. Data from your wireless network can be intercepted just like signals from our cellular or cordless phones. Whenever we use a wireless connection, we might want to ensure that our communications and files are private and protected. If four transmissions are not secure, it may be possible for others to intercept our e-mails, examine our files and records, and use our network and Internet connection to distribute their own messages and communications.

Hence, we need security in wireless network.

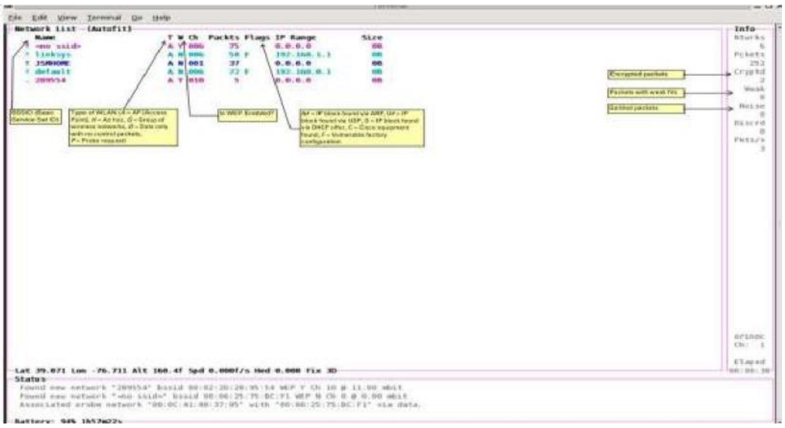
1) Kismet

Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff
802.11a, 802.11b, 802.11g, and 802.11 traffic. The program runs under Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X. The client can also run on Microsoft Windows, although, aside from external drones, there's only one supported wireless hardware available as packet source. Distributed under the GNU General Public License, Kismet is free software.

A. Working of kismet

Kismet differs from other wireless network detectors in working passively. Namely, without sending any loggable packets, it is able to detect the presence of both wireless access points and wireless clients, and to associate them with each other. It is also the most widely used and up to date open source wireless monitoring tool. Refer fig. 1 to view at explanation of the headings displayed in Kismet.

1. Kismet also includes basic wireless IDS features such as detecting active wireless sniffing programs including NetStumbler, as well as a number of wireless network attacks.
2. Kismet also features the ability to detect default or "not configured" networks, probe requests, and determine what level of wireless encryption is used on a given access point.
3. Kismet also supports logging of the geographical coordinates of the network if the input from a GPS receiver is additionally available.
4. Kismet works with a lot of wireless cards supporting "monitor" mode. This mode captures packets without being able to associate in the same time with an access point and require privileges rights.
5. Kismet detects networks by passively sniffing providing it the advantages to discover the "hidden" wireless networks and being itself undetectable.



File Edit View Terminal Go Help
SSID (Basic Service Set ID)
Type of WLAN (A = AP (Access Point), H = Ad hoc, G = Group of wireless networks, D = Data only with no control packets, P = Probe request)
Is WEP Enabled?
A4 = IP block found via ARP, U4 = IP block found via UDP, D = IP block found via DHCP offer, C = Cisco equipment found, F = Vulnerable factory configuration
Encrypted packets
Packets with weak IVs
Garbled packets

```
Network List - (Autofit)                                                Info
  Name          T W Ch  Packts Flags IP Range        Size               Ntwrks
  <no ssid>     A Y 006   75         0.0.0.0         0B                      6
  linksys       A N 006   58   F     192.168.1.1     0B                 Pckets
  JSHOME        A N 001   37         0.0.0.0         0B                    252
  default       A N 006   72   F     192.168.0.1     0B                 Cryptd
  209554        A Y 010    5         0.0.0.0         0B                      2
                                                                        Weak
                                                                             0
                                                                        Noise
                                                                             0
                                                                        Discrd
                                                                             0
                                                                        Pkts/s
                                                                             3

                                                                        orinoc
                                                                        Ch:  1
                                                                        Elapsd
Lat 39.071 Lon -76.711 Alt 160.4f Spd 0.000f/s Hed 0.000 Fix 3D         00:00:30
Status
 Found new network "209554" bssid 00:02:2D:20:95:54 WEP Y Ch 10 @ 11.00 mbit
 Found new network "<no ssid>" bssid 00:06:25:75:BC:F1 WEP N Ch 0 @ 0.00 mbit
 Associated probe network "00:0C:41:40:37:05" with "00:06:25:75:BC:F1" via data.

Battery: 94% 1h57m22s
```

Fig. 1: An explanation of the headings displayed in Kismet

B. Advantage of kismet

- It results is very good for small area.
- It has a Server – Client architecture
- Drones: distributed kismet servers running on remote devices, reporting back to central server, allow for the building of distributed reporting and intrusion detection systems.
- Kismet is powerful - especially when combined with other tools like wireshark, nmap.

C. Disadvantage of kismet

- It takes long time to search networks.
- It can only identify the wireless network (WiFi) in a small area, if the range is more it cannot work properly.

D. System requirements

(a) Kismet – packet sniffer
(b) Spectrum analyzers: airview, wispy
(c) General networking tools: wireshark, ntop, mrtg, rrdtool, nmap etc.

2) NETSTUMBLER

NetStumbler (also known as Network Stumbler) is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards. It runs on Microsoft Windows operating systems from Windows 2000 to Windows XP.
The program is commonly used for:

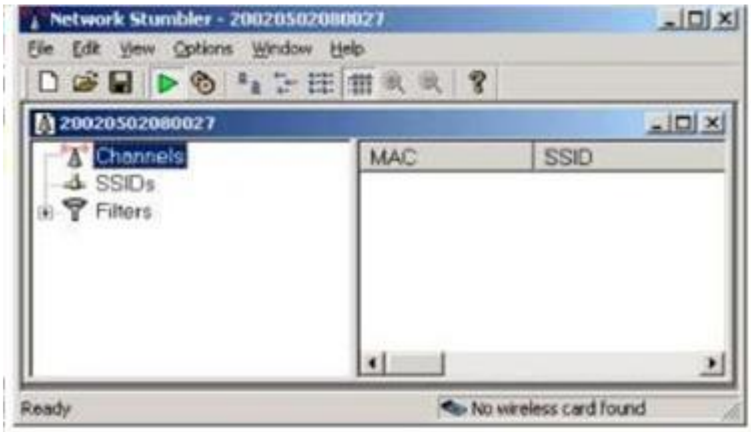
- Wardriving
- Verifying network configurations
- Finding locations with poor coverage in a WLAN
- Detecting causes of wireless interference
- Detecting unauthorized ("rogue") access points
- Aiming directional antennas for long-haul WLAN links

The NetStumbler application is a Windows-based tool generally used to discover WLAN networks running on 802.11 a/b/g standards. It helps detect other networks that may cause interference to your network, and is generally used for war driving purposes by attackers. It can also find out poor coverage areas in the WLAN network, and helps the administrator set up the network the way it is intended to be.

A. Working of NetStumbler

1. **Automatic Scanning & File Naming Convention:** When NetStumbler is launched, it begins scanning for beacons automatically. Upon startup, it generates a new file, naming it based on the current date and time in the format YYYYMMDDHHMM (year, month, day, hour, and minutes). For example, if the date is April 21, 2002, at 3:15 PM, the file will be named 200204211515. This structured naming system helps users track data files efficiently over long periods.

2. **NetStumbler Startup & Initial Screen:** As soon as NetStumbler starts, it is ready to scan for wireless networks. If a workstation does not have a wireless card installed, the interface will display an empty list. This scenario can be observed in Figure 2, which illustrates the NetStumbler screen right after launch without a wireless card.



Network Stumbler - 20020502080027

20020502080027

Ready

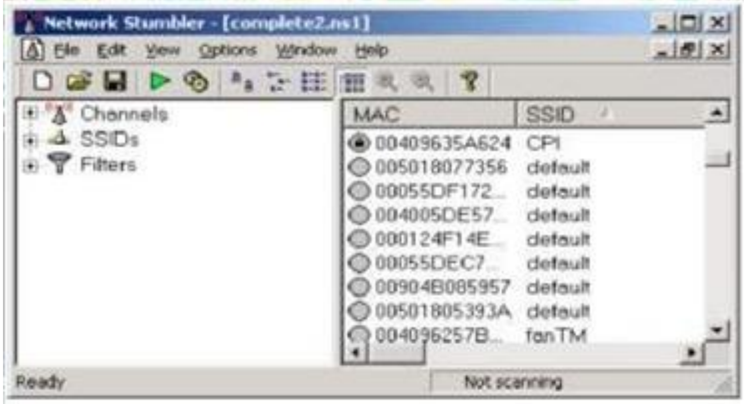
No wireless card found

Fig. 2: NetStumbler screen immediately after startup

3. Connecting a GPS Receiver: To integrate a GPS receiver with NetStumbler, users must modify the GPS settings. This can be done by navigating to Options → GPS → Port and selecting the appropriate COM port from the available options. NetStumbler supports the NMEA protocol by default, operating at 4800 bps, which is compatible with most GPS receivers. Before connecting, ensure the GPS device is configured to use the NMEA protocol. For instance, the **Garmin** GPS III integrates seamlessly after being set up correctly.

4. **Saving and Managing Sessions:** Since network detection is typically a continuous process, saving NetStumbler sessions is crucial. Users can manually save a session by selecting File → Save or enable the AutoSave option through Options → AutoSave, which automatically saves files with every scan (indicated by a checkmark next to the option). Additionally, multiple saved files can be merged into a single dataset using File → Merge**,** allowing users to combine all collected data for better analysis.

5. Working with NetStumbler Results: Once NetStumbler completes scanning, it generates a list of detected wireless access points and their locations. To map these access points, users must first export the data by selecting File → Export → Summary and saving the exported file on the system. This file needs to be converted into a format compatible with Microsoft MapPoint. To do this, users can visit the NetStumbler website and use the MapPoint Converter tool, which processes the summary file and generates structured output. Since Microsoft MapPoint does not support direct imports, the formatted output must first be copied into an Excel spreadsheet**,** saved, and then imported into MapPoint for visualization. Once imported, users can view a mapped representation of all detected wireless networks.



MAC	SSID
00409635A624	CPI
005018077356	default
00055DF172...	default
004005DE57...	default
000124F14E...	default
00055DEC7...	default
00904B085957	default
00501805393A	default
004096257B...	fanTM

Fig. 3: Some Wireless Access points found by MiniStumbler shown in NetStumbler

6. **Mapping Wireless Networks:** Once the data is imported into Microsoft MapPoint, the software generates a visual representation of detected wireless networks. Figure 4 demonstrates an example map of Indianapolis Wireless LANs created using this process.

B. Advantage of NetStumbler:

- **Passive Monitoring:** Kismet operates passively, meaning it doesn't send any packets and simply listens to the wireless traffic. This makes it less likely to be detected by other devices on the network.
- **Wide Protocol Support:** It supports a variety of wireless protocols and standards, including 802.11a, 802.11b, 802.11g, and more, making it versatile for monitoring various types of wireless networks.
- **Channel Hopping:** Kismet dynamically hops between Wi-Fi channels during operation, allowing it to capture information from all available channels. This provides a comprehensive view of the wireless spectrum.
- **Wireless Intrusion Detection System (WIDS):** Kismet can function as a Wireless Intrusion Detection System, identifying security threats and anomalies in the wireless environment, such as rogue access points or unauthorized devices.

C. Disadvantage of NetStumbler

- **Platform Compatibility:** It is available for various operating systems, including Linux, making it accessible to a broad user base.
- **Command-Line Interface (CLI):** The powerful command-line interface provides flexibility and control for users comfortable with command-line tools.

D. System requirements:

(a) Netstumbler (windows).

(b) General networking tools: wireshark, ntop,mrtg,rrdtool, nmap etc.

(c) WEP/WPA/WPA2 cracking: aircrack etc

The requirements for NetStumbler are somewhat complex and depend on hardware, firmware versions, driver versions and operating system. The best way to see if it works on your system is to try it.

The following are rules of thumb that you can follow in case you cannot reach the web site for some reason.

1) This version of NetStumbler requires Windows 2000, Windows XP, or better.
2) The Proxim models 8410-WD and 8420-WD are known to work. The 8410-WD has also been sold as the Dell TrueMobile 1150, Compaq WL110, Avaya Wireless 802.11b PC Card, and others.
3) Most cards based on the Intersil Prism/Prism2 chip set also work.

GitHub Link:

CONCLUSION: We studied the necessity of security tools for wireless networks and also gathered information about two popular security tools : Kismet and NetStumbler.