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 riskybecause we are transmitting information via radiowaves. Data from your wireless network can beintercepted just like signals from our cellular orcordless phones. Whenever we use a wireless con-nection, 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.

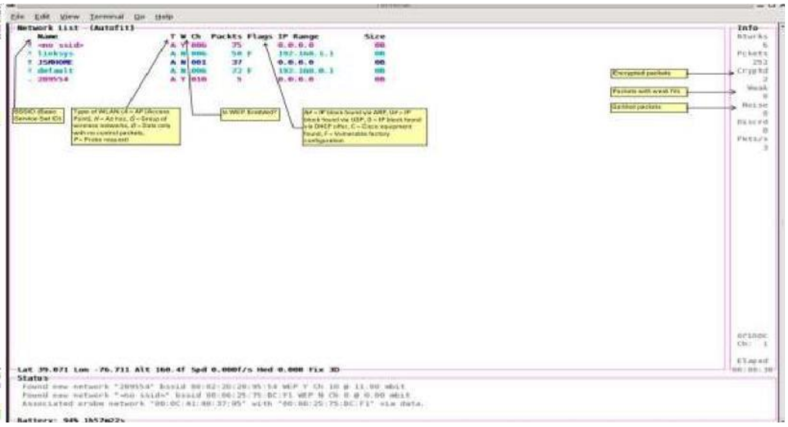
1) Kismet

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,and802.11ntraffic. 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 detec- tors 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
BSSID (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)
   Name                         T W Ch   Packts Flags IP Range          Size
 ! <no ssid>                    A Y 006     75        0.0.0.0             0B
 . linksys                      A N 006     58 F      192.168.1.1         0B
 ! JSHOME                       A N 001     37        0.0.0.0             0B
 ! default                      A N 006     72 F      192.168.0.1         0B
 . 289554                       A Y 010      5        0.0.0.0             0B

Info
Ntwrks 5
Pckets 253
Cryptd 2
Weak 0
Noise 0
Discrd 0
Pkts/s 3
orinoc
Ch: 1
Elapsd
00:00:30

Lat 39.071 Lon -76.711 Alt 160.4f Spd 0.000f/s Hed 0.000 Fix 3D
Status
 Found new network "289554" 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:41:40:37:95" 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 cannotwork properly.

D. System requirements

(a) Kismet – packet sniffer
(b) Spectrum analyzers: airview, wispy
(c) General networking tools: wireshark, ntop, mrtg, rrdtool, nmap etc.
(d) WEP/WPA/WPA2 cracking: aircrack etc
(e) It will work (at some level) on any operating system which has POSIX compatibility, however for it to do native packet capturing it needs drivers which are capable of reporting

packets in rfmon. Remote sources such WSP100 or Drones can be used on any platform we can get kismet to compile.

Kismet will work with any distribution of Linux. Currently, Linux is the recommended platform for running Kismet because it has largest selection of rfmon capable drivers.

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. By default, NetStumbler immediately starts scanning for beacons when you launch it. When NetStumbler starts, it creates a new file with the year, month, day, and 24-hour time listed serially without delimiters. For instance, if it's April 21, 2002 at 3:15 P.M., it will create a file called 200204211515. You can use this filename convention to help find data files created over the course of days or years.

2. Refer to fig. 2 that shows the NetStumbler screen immediately after startup. As you can see at thebottom of the screen, this example workstation doesn't have an installed wireless card. I've intentionally not inserted the LAN card so you can see an empty list. NetStumbler starts up ready to scan.

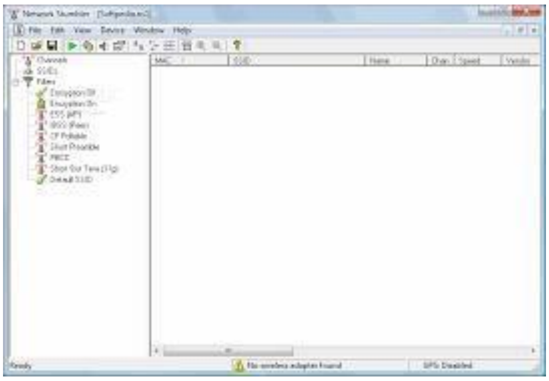


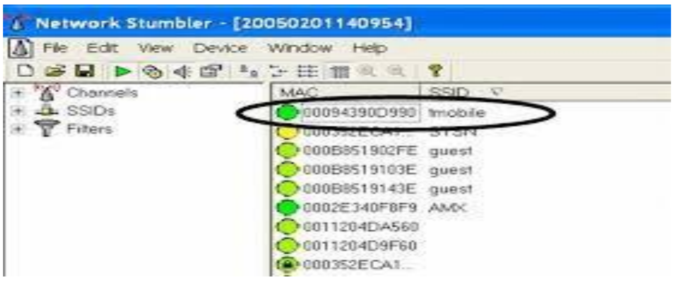
Fig. 2: NetStumbler screen immediately after startup

3. Connecting a GPS receiver If you plan to connect a GPS to NetStumbler, you'll need to change the GPS options. To do so, click Options — GPS — Port. When the Port window appears, you should select one of the available COM ports. The protocol defaults to the NMEA protocol, which most GPS receivers can output. The speed is set to the NMEA default protocol of 4800 bps. The Garmin GPS III receiver that I used connected flawlessly. Of course, I had previously set the GPS receiver to the NMEA protocol.

4. Saving sessions It's unlikely that you'll only use NetStumbler to find rogue access points in a single day. Before you shut down NetStumbler, you should save the session with the Save command on the file menu. Or, if you prefer, you can autosave the file by selecting the Options menu and then selecting AutoSave. A check mark will appear to the left of the entry when it's selected.

5. After you've saved a few files, you'll want to put them together. You can merge existing data intothe current file by selecting File and then Merge.

6. Working with the results When you run NetStumbler, all you wind up with is a list of access points and their locations. The real fun is taking those access points and mapping them. Start by making sure you've merged all of your NetStumbler files together into one large file, as described above. Refer to fig. 3 that shows a partial listing of the access points that was detected in the Indianapolis area as per survey.


Network Stumbler - [20050201140954]

MAC	SSID
00094390D990	tmobile
000352ECA...	STSN
000B851902FE	guest
000B8519103E	guest
000B8519143E	guest
0002E340F8F9	AMX
0011204DA560	
0011204D9F60	
000352ECA1...	

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

7. The next step is to convert the data in NetStumbler into a format that you can map. The conversion process takes two steps. The first is to export the data from NetStumbler by selecting
File — Export — Summary and save the export file to your system. Next, connect to the NetStumbler Web site and select the option for MapPoint Converter. This brings you to a Web page that translates the summary file into a series of rows that you can then use to create a map using Microsoft MapPoint.
Unfortunately, you can't read this file directly into MapPoint. You must first copy the results of the script into an Excel workbook. Once you've saved the Excel workbook, you can import the data into MapPoint. The results may look something like shown in fig. 4.

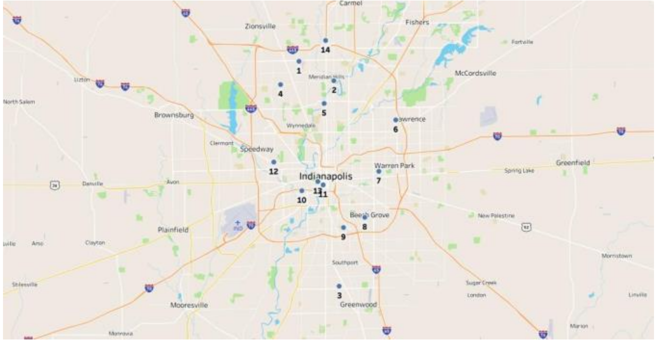


Fig. 4: Some Indianapolis Wireless LANs mapped

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.

GPS Integration: The tool supports integration with GPS devices, allowing for the geographical mapping of detected wireless networks. This feature is useful for conducting site surveys and mapping Wi-Fi coverage.

Modular Architecture: Kismet's modular architecture supports plugins, enabling users to extend its functionality and integrate it with other tools or systems

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.
4) Most 802.11b, 802.11a and 802.11g wireless LAN adapters should work on Windows XP. Some may work on Windows 2000 too. Many of them report inaccurate Signal strength, and if using the “NDIS 5.1” card access method then Noise level will not be reported. This includes cards based on Atheros, Atmel, Broadcom, Cisco and Centrino chip sets.
5) Firmware Requirements are: If you have an old WaveLAN/IEEE card then please note that the WaveLAN firmware (version 4.X and below) does not work with NetStumbler. If your

card has this version, you are advised to upgrade to the latest version available from Proxim's web site. This will also ensure compatibility with the 802.11b standard.

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.