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.

Thus, wireless networking is inherently risky because we are transmitting information via radio waves. Data from your wireless network can be intercepted just like signals from our cellular cordless 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 emails, 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 networks.

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 802.11n 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 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.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

5. Kismet detects networks by passively sniffing providing it the advantages to discover the ”hidden” wireless networks and being itself undetectable.

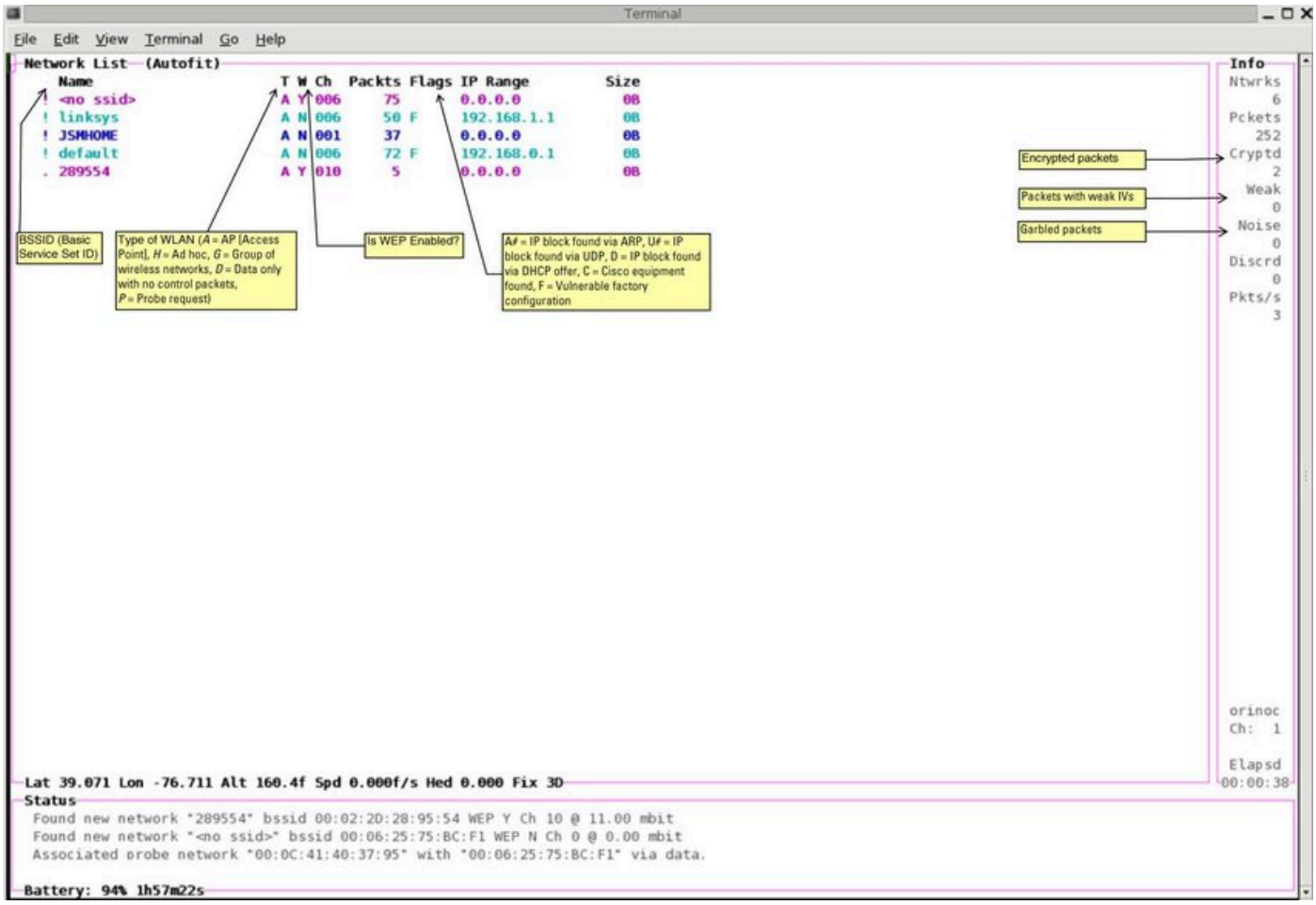

Fig. 1: An explanation of the headings displayed in Kismet

B. Advantage of kismet

• Its results are very good for small areas.
• 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 a 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.
(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.
(f) Kismet will work with any distribution of Linux. Currently, Linux is the recommended platform for running Kismet because it has the 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
• 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/a standards It helps detect other networks that mav cause interference tö your network, and is generally used for wardriving 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 the bottom 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.

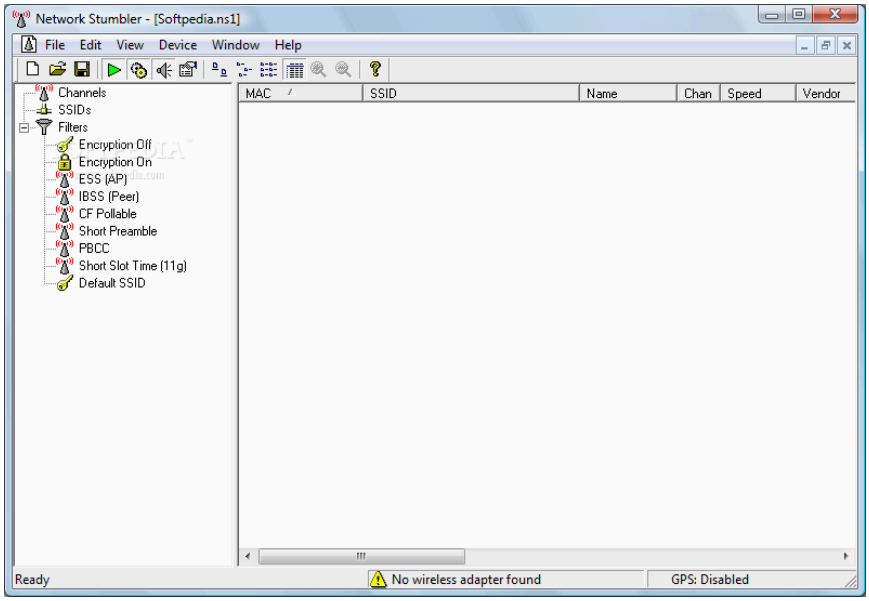

Fig. 2: NetStumbler screen immediately after startup

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.

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 NetStumbíer, you should save the session with the Save command on the file menu.

5. After you've saved a few files, you'll want to put them together. You can merge existing data into Te 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.

7. The next step is to convert the data in NetStumbler into a format that you can map.

B. Advantage of NetStumbler

• NetStumbler is a very useful tool that any wireless network administrator should be using periodically to determine not only the range of their wireless network, but also what wireless networks are available within their vicinity.
• First, determining the range of your wireless network will help you be able to provide better service. Armed with this information you can adjust antenna directions or AP placement to provide maximum coverage within your environment, and as little coverage as possible outside of the building/campus.

• NetStumbler has a tendency to be a virtual fire hose of information, overloading the casual user. If you know what you are looking for, and are familiar with NetStumbler then there is a great deal of information available to you in its screens, but this can be intimidating.
• Another thing that was true for some of the earlier versions of NetStumbler is that it depended upon the type of wireless card you have, specifically, the manufacturer of the chipset used for 802.11 modulation. As time has passed more and more cards and chipsets have been made compatible with NetStumbler.

D. System requirements

(a) Netstumbler (windows)
(b) General networking tools: wireshark, ntop
(c) WEP/WPA/WPA2 cracking: aircrack etc

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.
3) Most 802.11b, 802.11a and 802.11g wireless LAN adapters should work on Windows XP. Some may work on Windows 2000 too.
4) 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.

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