Experiment No. 5
Study wireless security tools like kismet and Netstumbler.
Date of Performance:
Date of Submission:

Experiment No. 5

Aim: Study wireless security tools like kismet and Netstumbler.

Theory:

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 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.

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.

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.

B. 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.

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.

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 into the 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.

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.

• Secondly, NetStumbler is a great tool for determining whether there are any additionalwireless networks nearby. These networks could potentially be rogue APs that have been placedbehind your firewall by uninformed users, not secured according to corporate standards, and thus a major security risk.

Disadvantage of NetStumbler

• 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.

• Also, NetStumbler on its own does nothing to tell a user whether the network is secure or not, it simply provides all of the relevant details with regard to the wireless network. Used in conjunction with other tools (WEPCrack, AirSnort, etc) NetStumbler is a useful tool for an end-to-end evaluation of wireless security, however many of the competitors to NetStumbler easily bundle these additional tools. This bundling makes the additional tools easier to use, at the sacrifice of flexibility within the tool. Some would consider this is a pro for NetStumbler, but generally it is regarded as a mixed bag.

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, WindowsXP, 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.

Conclusion:

Kismet and NetStumbler offer distinct approaches to wireless network detection and analysis. Kismet, a versatile tool with passive detection capabilities, is ideal for small-scale monitoring and intrusion detection, while NetStumbler, primarily for Windows systems, excels in identifying WLAN networks and assessing coverage and security vulnerabilities, albeit with potential information overload