Wireless Local Area Networks: Threats and Their Discovery Using WLANs Scanning Tools

Ms. Rakhi Budhrani
Bhavnagar, Gujarat, India.
Dr. R. Sridaran,
Dean, Faculty of Computer Applications,
Marwadi Education Foundation's Group of Institutions,
Rajkot, Gujarat, India.

----------ABSTRACT----------

Wireless Local Area Networks frequently referred to as WLANs or Wi-Fi networks are all the passion in recent times. Wireless networks offer handiness, mobility, and can even be less expensive to put into practice than wired networks in many cases. But how far this technology is going provide a protected environment in terms of privacy is again an anonymous issue. Realizing the miscellaneous threats and vulnerabilities associated with 802.11-based wireless networks and ethically hacking them to make them more secure is what this paper is all about. On this segment, we'll seize a look at common threats, vulnerabilities related with wireless networks. This paper presents an overview some of the WLANs Scanning, Sniffing and Auditing tools available on the internet. This paper Reviews these tools along with their merits, demerits and how they can be used for hacking, exploiting security holes and their usage characterization in WLANs.

Keywords - **Current threats in WLANs, Exploiting Security, WLANs Scanning, WLANs Sniffing, Multifunctional, WLANs auditing tools**

I. INTRODUCTION

The Institute of Electrical and Electronics Engineers (IEEE) provides 802.11 set of standards for WLANs. The wing ".11" refers to a subset of the 802 group which is the wireless LAN working group [1, 20]. Many industry groups are involved in work with wireless systems, however the IEEE 802.11 working group and the Wi-Fi Alliance [21] came out as key troupes. At present, Wi-Fi schemes shaped a demand in the market and they are in reality everywhere. Wireless networking presents many advantages Productivity improves because of increased accessibility to information resources. Network Configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also coupled with new security threats and alters the organization's overall information security risk profile.] According to S Vinjosh Reddy, KRijutha, K SaiRamani, Sk Mohammad Ali, CR. Pradeep Reddy [6] the expediency, cost reserves, and efficiency gains of wireless networks raise security risks. The regular security issues, like weak passwords, spyware, and missing patches are not the things that are going to matter.

Networking with no wires brings in an intact new set of vulnerabilities [2, 3] from an entirely different point of view. Wireless networks are susceptible and exposed to attack because of its borderless nature. It is easy to penetrate any wired network via wireless network as Access Point (AP) is bridging between wireless and wired network. Wireless Networks present a host of issues for network managers. Unauthorized access points, broadcasted SSIDs, unknown stations, MITM attacks such as session hijacking and spoofed MAC addresses are just a few of the problems addressed in WLAN troubleshooting. [7]

Moreover, According to Mardiana Mohamad Noor and Wan Haslina Hassan [3] hacking tools are largely available in the market and online. These tool which are usually meant to be used by penetration testers and for educational purposes are being misused and abused by underground or even novice hackers. On the other hand, the flexibility and ubiquity of mobile devices such as smartphones, tablets, phablets and laptops are the main reason of the popularity of hotspots which are exposed of the rogue access points [6].

Here comes the concept of ethical hacking. Ethical hacking [15][16], occasionally called as white-hat hacking is the use of hacking to check and advance the defenses against unethical hackers. It may be compared to access testing and susceptibility testing, but it goes even deeper. Ethical hacking entails the usage of same tools and practices the bad guys make use of, however it also involves wide range forefront planning, a set of precise tools, multifaceted testing methodologies [16], and adequate report to fix any problems before the bad guys exploit our privacy.

This paper, presents an output of detailed review of various threats to WLANS, overview of the available WLANs Monitoring Tools. These tools have been analyzed through a comprehensive study of the WLAN as Scanning, Sniffing and Auditing tools. Out of these tools the scanning tools have been explored in details in this paper

The paper is organized as follows. Secion 2 contains an overview of common threats to WLANS. Section 3 contains an overview of various Network Monitoring tools. Section 4 contains an overview of Scanning Techniques. Section 5 contains a detailed survey of Active WLANs scanning tools. Section 6 contains a detailed survey of Active WLANs scanning tools.

II. RELATED WORK IN WLANS MONITORING

As per the studies conducted WLANs Monitoring, This section briefly presents several infamous attacks to wireless network including 802.11 Specific Vulnerabilities, MAC Sniffing and AP Spoofing, Defeating MAC Address, Filtering in Windows, WEP Flaws, WEP Authentication Phase Flaws, WPA Vulnerabilities, Evil-Twin Attack, LEAP Attack Tool: ASLEAP, Man-In-The-Middle Attack (MITM), Denial-Of-Service Attacks, Hijacking and Modifying a Wireless Network, Cracking WEP with Pad Collection Attacks, wireless phishing and Rogue Access Points [1][3][15][20][21][22] as an output of the same.

As per [1] and [3] Two common vulnerabilities to the 802.11 standard are default SSIDs and beacon broadcast. Many people fail to change the SSIDs on their networks as set by the manufacturers. Attackers will see this and assume the target has not spent much time securing the network. Also, base stations regularly broadcast their existence for end users to listen and negotiate a session. These signals can be captured by anyone, who can then discover the SSID.

According to [1] and [2] Most access points have MAC address filtering capabilities, which means a network administrator can create a list of approved MAC addresses that are allowed to connect to the network. This feature has two options: open or closed. In a closed MAC filter, only listed addresses are allowed to access the network. In an open MAC filter, the addresses listed in the filter are prevented from accessing the network. The MAC address does not offer a good security mechanism because it is both easily observable and reproducible.

Even if WEP is enabled, an attacker can easily sniff MAC addresses because they appear in clear text. Moreover, it is possible to change the MAC address on a wireless card through software. Each network card has a unique MAC address. But the attacker can easily change the MAC address by using the ifconfig command. All the attacker needs to know is a trusted MAC address. When the attacker tries to login with the spoofed MAC address, the legitimate user with that MAC address is disconnected from the wireless network.

As per [6] and [4] Most commercial-grade and consumer-grade wireless networking equipment sends the MAC address in Clear text even if WEP is enabled. Passively sniffing the traffic on a wireless network using a tool such as Ethereal allows an attacker to determine one or more MAC addresses that are allowed to connect to the network. If MAC address filtering is the only security measure in place, attackers need only to change their MAC addresses to those that are allowed access.

Wired Equivalent Privacy (WEP) is a security protocol designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to that which is usually expected of a wired LAN. As observed in [1] [5] [6] [8] some basic flaws undermine WEP's ability to protect against a serious attack, including the following:

- No defined method for encryption key distribution. Pre-shared keys are set once at installation and are rarely (if ever) changed. It is easy to determine the number of plaintext messages encrypted with the same key. Use of RC4, which was designed to be a one-time cipher and not intended for multiple message use. An attacker monitors the traffic and determines the different ways to decipher the plaintext message. With knowledge of the ciphertext and the plaintext, an attacker can compute the key.
- Attackers can analyze the traffic from passive data captures and crack the WEP keys with the help of tools such as AirSnort, WEPCrack, and dweputils.
- Key generators that are used by different vendors are vulnerable.
- Key scheduling algorithms are also vulnerable to attack.
- CRC32 is not sufficient to ensure complete cryptographic integrity of a packet. By capturing two packets, an attacker can reliably flip a bit in the encrypted stream and modify the checksum so that the packet is accepted.
- WEP is based on a password. WEP is vulnerable to dictionary attacks. The small space of the initialization vector allows the attacker to create a decryption table, which is a dictionary attack.
- WEP can be vulnerable to denial-of-service attacks.
- Associate and disassociate messages are not authenticated. Eventually, an attacker can construct a decryption table of reconstructed keystreams. With about 24 GB of space, an attacker can use this table to decrypt WEP packets in real time.

- A lack of centralized key management makes it difficult to change WEP keys with any regularity.
- IV is a value that is used to randomize the keystream value, and each packet has an IV value. The standard allows only 24 bits, so the range of values can be used up within a matter of hours at a busy AP. IV values will be reused. The standard does not dictate that each packet must have a unique IV, so vendors use only a small part of the available 24-bit possibilities.There are known plaintext attacks. When there is an IV collision, it becomes possible to reconstruct the RC4 keystream based on the IV and the decrypted payload of the packet. A mechanism that depends on randomness is not random at all, allowing attackers to easily figure out the keystream and decrypt other messages.

In open system authentication (OSA) all the transactions are clear, enabling an intruder to sniff the traffic and walk through the same steps to be authenticated and associated to an AP. Shared key authentication (SKA) encrypts most, but not all, encryption components for the authentication process and data transfers. It uses WEP encryption, which can be easily defeated. The access criteria may include specific MAC addresses of stations, but intruders can easily change their MAC addresses to those that completed the authentication phase. [6] [8]

According to [8] and [1] WEP can be cracked using either passive attacks or active attacks. Passive attacks compromise the confidentiality of the network. The semi passive approach makes this more practical, but it needs some time and space to implement. The presence of the attacker does not change traffic until WEP has been cracked.
Active attacks compromise the integrity and availability of the network. They need less time and space compared to passive attacks. Active attacks increase the risk of being detected, but are more effective. If an active attack is reasonable, and the risk of detection is disregarded, the goal is to stimulate traffic to collect more pads (some attacks require only one pad) and use weak IVs.

According to EC council [1] Pads are the numbers used in the WEP encryption sequence. A pad collection attack is a semi-passive attack. It collects a set of pads and then decrypts any packet for which a pad is present. It works with 64-bit or 128-bit encryption. It requires traffic flowing across the network. It can spread the attack over time in order to slow down possible detection. There should be a separate pad for each encrypted packet that is transferred between the access point and a station. It is possible to make a table and skip the RC4 step by mapping pads to IVs.

According to [1] [8] [5] and [9] WPA (Wi-Fi Protected Access) is compatible with the 802.11i security standard. It is a software upgrade, but may also require a hardware upgrade. Nearly every Wi-Fi company has decided to employ this standard for increased security called Wi-Fi Protected Access.
WPA is vulnerable to denial-of-service attacks if an attacker injects or corrupts packets. The only way around this attack is to switch completely to WEP until it subsides. In addition, WPA is vulnerable to dictionary attacks if the preshared 14-character key is a real word.
WPA utilizes a 256-bit pre shared key or a passphrase that can vary in length from 8 to 63 bytes. Short passphrase-based keys (less than 20 bytes) are vulnerable to an offline dictionary attack. The pre shared key that is used to set up the WPA encryption can be captured during the initial communication between the access point and the client. Once the pre shared key is captured, it can be used to guess the WPA key using a standard dictionary attack. In theory, this type of dictionary attack takes less time and effort than attacking WEP.

As per [1], [4] and [17] An evil-twin is a homemade wireless access point that masquerades as a legitimate access point to gather private information without the end user's knowledge. The attacker positions the evil-twin in the vicinity of a legitimate access point and discovers what name and radio frequency that point uses. Fraudulent APs can easily advertise the same network name (SSID) as a legitimate hotspot or business WLAN, causing nearby Wi-Fi clients to connect to them. Tools like metasploit can now listen to nearby clients, discover SSIDs they're willing to connect to, and automatically start advertising those SSIDs. Once clients connect, DHCP and DNS are used to route client traffic through the Evil Twin, where local (phony) Web, mail, and file servers execute man-in-the-middle attacks. The only effective defense against Evil Twins is server authentication, from 802.1X server validation to application server certificate verification.

As mentioned in [1], The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary, closed solution that offers username/ password-based authentication between a wireless client and a RADIUS server. LEAP conducts mutual authentication. It is used with the IEEE 802.1x standard for LAN port access control.
ASLEAP, a tool for attacking LEAP networks, features the following:

- Scans the 802.11 packets by putting the wireless interface in RFMON mode
- Hops channels to look for targets (WLAN networks that use LEAP)
- Deauthenticates the users on LEAP networks, forcing them to reauthenticate by providing their usernames and passwords
- Records the LEAP exchange information to a libcap file

- Analyzes the information captured offline and compares it with values in the dictionary to guess the password

There are two types of man-in-the-middle attacks according to : eavesdropping and manipulation [1] [2] [4] and [17].
Eavesdropping is easy in a wireless network because there is no physical medium used to communicate. An attacker who is in an area near the wireless network can receive radio waves on the wireless network without much effort. The entire data frame sent across the network can be examined in real time or stored for later assessment. If a security mechanism such as IPSec, SSH, or SSL is not used for transmission, the transmitted data is available to anyone. WEP can be cracked with tools freely available on the Internet. Accessing e-mail using POP or IMAP protocols is risky because these protocols can send e-mail over a wireless network without any form of extra encryption. A determined whacker can potentially log gigabytes of WEP-protected traffic in an effort to post process the data and break the protection.
Manipulation is a higher level of attack than eavesdropping. Manipulation occurs on a wireless link when an attacker is able to receive the victim's encrypted data, manipulate it, and retransmit the changed data to the victim. In addition, an attacker can intercept packets with encrypted data and change the destination address in order to forward these packets across the Internet.

In addition to the above man-in-the-middle application attacks, hackers continue to develop new methods to phish Wi-Fi users [17]. For example, it's possible to poison Wi-Fi client Web browser caches, so long as the attacker can get into the middle of a past Web session – such as by using an Evil Twin at an open hotspot. Once poisoned, clients can be redirected to phishing sites long after leaving the hotspot, even when connected to a wired enterprise network. One technique for mitigating this threat is to clear your browser's cache upon exit. Another possibility is to route all hotspot traffic (even public) through a trusted (authenticated) VPN gateway.

As mentioned in [1],[2],[10] Denial-of-service (DoS) attacks at the application and transport layers are primarily the same. The possibility of DoS attacks on wireless networks is greater due to the relationship of the physical, data link, and network layers.
Wireless DoS attacks are divided into three types: physical, data link, and network
To conduct a physical DoS attack on a wired network, close proximity to the victim's network is required. However, this is not the case with a wireless network, since attackers can launch attacks from great distances. It is easy and inexpensive to construct a device that produces a lot of noise at 2.4 GHz. In fact, there are several commercial devices available today that can bring down a wireless network with ease. If there is interference in a particular band due to the crowding of signals, there is a good chance that a wireless network is down somewhere. If the attacker is able to produce sufficient RF noise to reduce the signal-to-noise ratio to a level where it becomes unusable, devices within range of the noise will go offline. An attacker attempting a physical DoS attack can also use large-scale Bluetooth deployments.

Since the data-link layer is so accessible, DoS attacks can be carried out easily. The attacker who is preparing for a DoS attack at this layer can ignore WEP being turned on, as it will not prevent the attack.
In addition, with WEP turned off, the attacker has total access to manipulate associations among stations and access points to terminate access to the network. If the victim's network is not using WEP authentication, it is vulnerable to spoofed APs. By spoofing the AP, the attacker can block traffic from the victim's network. If an AP is improperly using antenna diversity, an attacker can deny access to clients associated with the AP. Antenna diversity is a method in which a single radio utilizes multiple antennas to reduce multipath fade. If these antennas do not cover the same region, an attacker can deny service to associated stations by taking advantage of the improper setup.

The 802.11 network is a shared medium, allowing an attacker to reject the affected access point that users access by flooding network traffic. If the network allows any unauthorized user on the network, it is more vulnerable to a network-layer DoS attack. For instance, an attacker can generate a ping (ICMP) to flood the base station (BS). Because the speed on 802.11 networks is relatively slow, a network DoS malfunction may accidentally occur due to the transfer of large files or the running of applications that require more than the allotted bandwidth.

Numerous techniques are available for an attacker to hijack a wireless network or session [1] [4] [6]. Unlike some attacks, network and security administrators may be unable to distinguish between the hijacker and a legitimate user. Many tools are available to network hijackers. These tools are based on basic implementation issues within almost every network device available today.
As TCP/IP packets go through switches, routers, and APs, each device looks at the destination IP address and compares it with the IP addresses it knows to be local. If the address is not in the table, the device hands the packet off to its default gateway. This table is used to coordinate the IP address with the MAC addresses that are known to be local to the device. In many situations this list is a dynamic one, built up from traffic passing through the device and through Address Resolution

Protocol (ARP) notifications from new devices joining the network. There is no authentication or verification that the request the device received is valid. Thus, a malicious user is able to send messages to routing devices and APs stating that his or her MAC address is associated with a known IP address. From then on, all traffic that goes through that router destined for the hijacked IP address will be handed off to the hacker's machine. If the attacker spoofs as the default gateway or a specific host on the network, all machines trying to get to the network or the spoofed machine will connect to the attacker's machine instead of their intended target. The attacker can use this information only to identify passwords and other necessary information and then route the rest of the traffic to the intended recipients. The end users will have no idea that this man in the middle has intercepted their communications, compromising their passwords and information.

An access point should be considered a rogue if it looks suspicious. Unauthorized access points can allow anyone with an 802.11-equipped device onto the network. Sometimes a rogue access point may be an active access point that is not connected to the network, but these access points are not security issues. When an access point is found that interfaces with the network, it must be shut off immediately [1] [11].
It can possibly be located by using a simple technique that involves walking with a wireless-access-point-sniffing device in the direction the signal strength of the access point's beacon increases.[3]
According to EC Council [20], there are at least four available APs nowadays, which are:

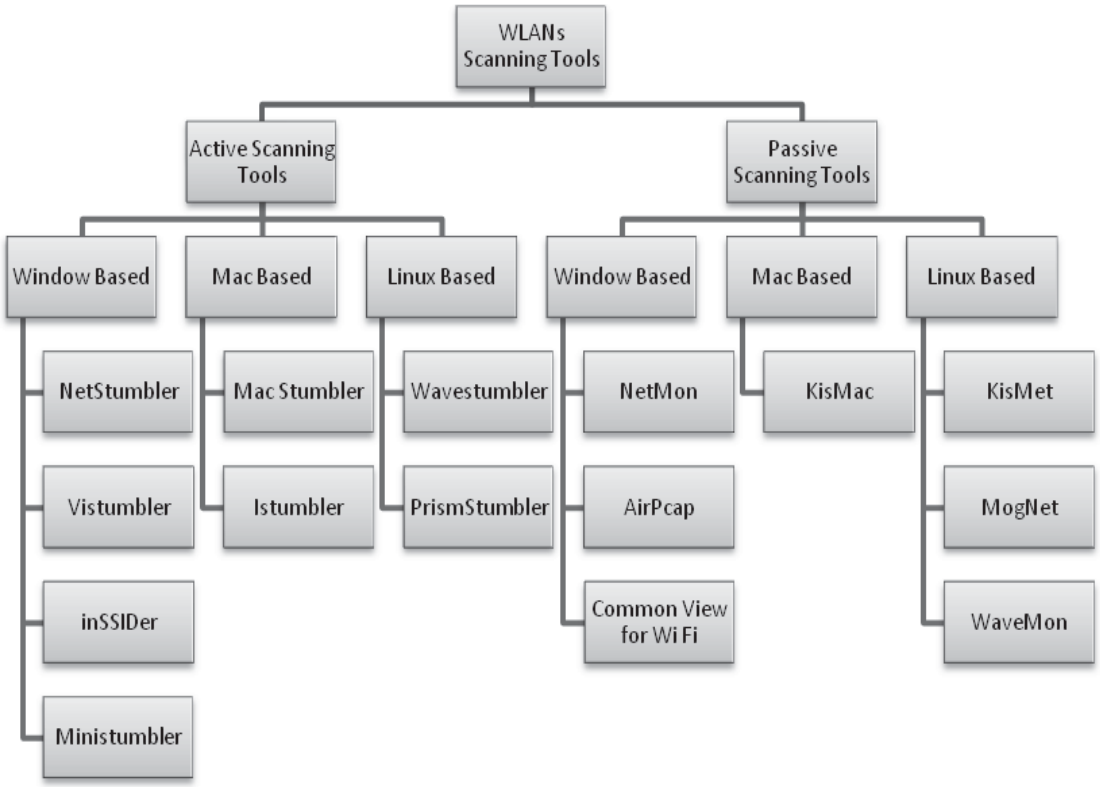
1. Compact and pocket sized RAP device plugged into an Ethernet port of corporate network
2. Software-based RAP running on a corporate Windows machines
3. RAPs connected to corporate network over a WiFi link
4. USB-based RAP access point device plugged into a corporate machine

RAPs are usually placed behind a firewall to avoid network scanner. Counter measures to RAP is an active area of research which concentrate at two end points which are client side and administrator side solutions.

III. WLANS SCANNING TOOLS

According to Mardiana Mohamad Noor and Wan Haslina Hassan [3] everybody is exposed to threats in wireless network as no network is fully guaranteed as secured. Hence, network administrators and users must be more serious in curbing security issues in wireless networks and apply countermeasures to lessen the risks of security issues. Networking with no wires brings in an intact new set of vulnerabilities [4][12] from an entirely different point of view. Here comes the concept of ethical hacking. Ethical hacking [21][22], occasionally called as white-hat hacking is the use of hacking to check and advance the defenses against unethical hackers. It may be compared to access testing and susceptibility testing, but it goes even deeper. Ethical hacking entails the usage of same tools and practices the bad guys make use of, however it also involves wide range forefront planning, a set of precise tools, multifaceted testing methodologies [22], and adequate report to fix any problems before the bad guys exploit our privacy. There are four tools for effective network monitoring; they are scanning tools, sniffing tools, multifunctional tools and Auditing tools. This paper presents an overview of several popular Scanning tools that are available in the Internet with their functionality.

According to EC Council [1] [20] Scanning is a process of discovering the wireless networks and the vulnerabilities & threats associated with them. All the scanning tools fall into one of two major categories: Active or Passive. Active tools are more rudimentary and send out probe request packets hoping to get a response. These packets are used by clients whenever they are looking for a network. Passive tools are designed to monitor the airwaves for any packets on a given channel. Moreover various attack techniques rely upon the capabilities of the underlying hardware [23]. This hardware depends on device drivers to communicate with the operating system, and device drivers are tied to a specific operating system. In addition, different wireless Scanning Tools only run on certain platforms. In the following section Active and passive scanning tools are bifurcated according to three operating systems i.e Windows, MAC and Linux .
The terminology related to wireless tools can be a bit overwhelming. Generally speaking, most tools that implement active scanning are called stumblers, whereas tools that implement passive scanning (more on this shortly) are called scanners. However, a stumbler is generally considered to be a "scanning tool" (even if not technically a scanner)[23].


WLANs Scanning Tools
Active Scanning Tools
Passive Scanning Tools
Window Based
Mac Based
Linux Based
Window Based
Mac Based
Linux Based
NetStumbler
Vistumbler
inSSIDer
Ministumbler
Mac Stumbler
Istumbler
Wavestumbler
PrismStumbler
NetMon
AirPcap
Common View for Wi Fi
KisMac
KisMet
MogNet
WaveMon

3.1 Active Scanning Tools

In Active Scanning Clients may send out targeted probe requests or they may send out broadcast probe. Clients can also use beacons to find a network. Access points send out beacon packets every tenth of a second. Each packet contains the same set of information that would be in a probe response, including name, address, supported rates, and so on [23].

3.1.1 Window Based Active Scanning Tools

3.1.1.1 NetStumbler

According to Nwabude Arinze Sunday, Network Stumbler [15] is a free Windows-based software utility for locating and interrogating Wireless LANS using 802.11b, 802.11a and 802.11g. Network Stumbler provides an easy method for enumerating wireless networks. It transmits connection requests to all the listening access points with an SSID. The APs respond by sending their own SSID. Note that NetStumbler is not a passive sniffer; this means that the traffic handled by it is visible on the victim's network. When Network Stumbler is launched, it starts a capture file and starts searching for access points. It displays MAC Address, SSID, Access Point, name, Channel, Vendor, WEP on or off, Signal Strength, GPS coordinates (if GPS device is attached)[6] [18][20][16]

It has many uses: [1][15][16]

- Verify that your network is set up the way you intended.
- Find locations with poor coverage in your WLAN.
- Detect other networks that may be causing interference on your network.
- Detect unauthorized "rogue" access points in your workplace.
- Help aim directional antennas for long-haul WLAN links.
- Use it recreationally for WarDriving.

NetStumbler is an active scanner that was popular on Windows XP. While it still works on Windows XP, it hasn't seen any maintenance since 2005. NetStumbler works with many NDIS 5 drivers, which means drivers that were written pre-Vista. People who utilized NetStumbler on older versions of Windows are encouraged to try out Vistumbler. Vistumbler is an open source active scanner for Windows Vista and 7, which is similar in function to NetStumbler [25].

Similar to Vistumbler, inSSIDer is also an active scanner that runs on Windows. InSSIDer was created by MetaGeek (purveyors of the WiSpy spectrum analyzer). One nice thing inSSIDer does that Vistumbler lacks is real-time graphing of signal strength. The graphs shown in inSSIDer can be useful when tracking down sources of signal strength indoors[23].

1.1.1.1 MiniStumbler

MiniStumbler is mini version of NetStumbler. MiniStumbler is for handheld device running on Windows CE. There is a trimmed version called which is available for handheld devices running on Windows CE. [25] MiniStumbler, is a Windows Mobile application that listens for broadcasts and captures network information [6] [18]. It provides important information, including whether or not the network is encrypted, the MAC address of the AP or wireless device, the SSID, the AP name, the channel used, the vendor, whether it is an AP or a peer device, and signal strength. MiniStumbler not only detects the different WLAN networks, but also their longitude and latitude if a GPS device is attached.

3.1.2 MAC Based Active Scanning Tools

Two active scanners are available for MAC interface. They are MACStumbler and IStumbler [23]. These tools will both find all available networks quickly, and will keep historical logs if you need to monitor wireless networks over time. MacStumbler and iStumbler work by actively sending out probe requests to all available access points. The access points respond to the probes (as they would for any legitimate wireless client), and this information is then collected, sorted, and displayed by the scanners. Unfortunately, neither of these tools will find "closed" networks, since they don't respond to probe requests. This is an unfortunate side effect for people who choose to hide their networks. Since it isn't easy to tell what channel they are using, it is very likely that someone nearby will choose to use the same (or an adjacent) channel for their own network. This causes undesirable interference for everybody. To detect "closed" networks, you need a passive scanner, such as KisMAC

3.1.2.1 MACStumbler

MacStumbler, is the Mac OS equivalent of Network Stumbler. It requires an Apple Airport Card and Mac OS 10.1 or greater; it does not currently support any kind of PCMCIA or USB wireless device. For wardriving, MacStumbler requires a NMEA (National Marine Electronics Association)-compatible GPS device, which means that the GPS must have a serial connection or a USB port. NMEA is the standard protocol used by GPS receivers to transmit data. MacStumbler has a text-to-speech option, so the ESSIDs (extended service set identifiers) of networks are read out as they appear. [1][24][26]

3.1.2.2 iStumbler

iStumbler is a utility for finding wireless networks and devices with AirPort- or Bluetooth-enabled Macintosh computers. iStumbler was originally based on MacStumbler source code. Its early development focused

on detection of open wireless (802.11) networks, but more recent versions support the detection of Bluetooth wireless devices and Bonjour network services. This tool is even simpler than MacStumbler, in that there is really nothing to configure. Just fire it up and it will find all available networks for you, complete with a real-time signal and noise meter [24][16][1].

3.1.3 Linux Based Active Scanning Tools

3.1.3.1 WaveStumbler

WaveStumbler is console based 802.11 network mapper for Linux. It reports the basic AP stuff like channel, WEP, ESSID, MAC etc. It has support for Hermes based cards (Compaq, Lucent/Agere). It still in development but tends to be stable. It consist of a patch against the kernel driver, which makes it possible to send the scan command to the driver viathe /proc/hermes/ethX/cmds file. The answer is then sent back via a netlink socket. WaveStumbler listens to this socket and displays the output data on the console. [27][23][20]

3.1.3.2 Prismstumbler

Prismstumbler, is a wireless LAN (WLAN) tool that scans for beacon frames from access points. It operates by switching channels frequently and monitoring frames received on the selected channel. The auto-homing mode of a Lucent/Orinco card can be used for this application. For doing security assessments in WLANs, the AirSnort package is required, which in turn requires a Prism2-based card. Prismstumbler was created to simplify the process of having to swap PC Cards. Prismstumbler also finds private networks. Since the method used is “receive only,” additional networks with weaker signals can also be found by Prismstumbler. It comes with a GTK2 user interface and uses an embedded SQL database to store network information. It is able to create networks lists in GPSdrive format and store captured packages to pcap dump files.[1] [28]

3.2 Passive Scanning Tools

Passive Scanning Tools analyze the packets to determine which clients are talking to which access points. The scanner sits in a loop, reading packets from the card, analyzing them, and updating the user interface as it determines new information. In order to do this, however, the wireless card needs to support what is known as monitor mode. Passive scanning tools don’t transmit packets themselves; instead, they listen to all the packets on a given channel and then analyze those packets to see what’s going on[23].

3.2.1 Window Based Passive Scanning Tools

3.2.1.1 NetMon

Wireless drivers targeted for Windows Vista or later are written to be NDIS 6.0-compliant. NDIS, the Network Driver Interface Specification, added a standard way for drivers to implement monitor mode. recent versions Microsoft Network Monitor (NetMon) can be used to place the card into monitor mode and capture packets.[23][24]

Microsoft Network Monitor is a packet analyzer. It enables capturing, viewing, and analyzing network data and deciphering network protocols. It can be used to troubleshoot network problems and applications on the network. Microsoft Network Monitor 1.0 (codenamed Bloodhound) was originally designed and developed by Raymond Patch, a transport protocol and network adapter device driver engineer on the Microsoft LAN Manager development team.[29]

Some key features of Network Monitor include the following: [30][31]

- Process tracking
- Grouping by network conversation
- Support for over 300 public and Microsoft proprietary protocols
- Simultaneous capture sessions
- Wireless Monitor Mode with supported wireless NICs
- Real-time capture and display of frames
- Reassembly of fragmented data
- Sniffing of promiscuous mode traffic
- Can read libpcap capture files
- API to access capture and parsing engine

3.2.1.2 AirPCap

AirPcap enables troubleshooting tools like Wireshark (formerly Ethereal) and WinDump to provide information about wireless protocols and radio signals. AirPcap comes as a USB 2.0 adapter and has been fully integrated with WinPcap and Wireshark. It captures and analyzes 802.11b/g wireless traffic including control frames, management frames, and power information [32][23]. AirPcap products come in a variety of configurations, most of which include support for packet injection.

All of the AirPcap adapters can operate in a completely passive mode. In this mode, the AirPcap adapter will capture all of the frames that are transferred on a channel, not just frames that are addressed to it. This includes data frames, control frames and management frames. When more than one BSS shares the same channel, the AirPcap adapter will capture the data, control, and management frames from all of the BSSs that are sharing the channel and that are within range of the AirPcap adapter.

The AirPcap adapter captures the traffic on a single channel at a time. The channel setting for the AirPcap adapter can be changed using the AirPcap Control Panel, or from the "Advanced Wireless Settings" dialog in Wireshark. Depending on the capabilities of your AirPcap adapter, it can be set to any valid 802.11 channel for packet capture.

The AirPcap software can optionally be configured to decrypt WEP-encrypted frames. An arbitrary number of keys can be configured in the driver at the same time, so that the driver can decrypt the traffic of more than one access point at the same time. WPA and WPA2 support is handled by Wireshark.[33]

3.2.1.3 Common View for WiFi

CommView for WiFi is a powerful wireless network monitor and analyzer for 802.11 a/b/g/n/ac networks. CommView for WiFi captures every packet on the air to display important information such as the list of access points and stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, protocol distribution charts, etc [23]. By providing this information, CommView for WiFi can help you view and examine packets, pinpoint network problems, and troubleshoot software and hardware. CommView for WiFi includes a VoIP module for in-depth analysis, recording, and playback of SIP and H.323 voice communications.

Packets can be decrypted utilizing user-defined WEP or WPA-PSK keys and are decoded down to the lowest layer. With over 100 supported protocols, this network analyzer allows you to see every detail of a captured packet using a convenient tree-like structure to display protocol layers and packet headers. Additionally, the product provides an open interface for plugging in custom decoding modules.

This application runs on Windows XP / Vista/ 7 / 8 or Windows Server 2003 / 2008 / 2012 (both 32- and 64-bit versions) and requires a compatible wireless network adapter [34].

Captured packets can be saved to log files for future analysis. A flexible system of filters makes it possible to drop unnecessary packets or capture the essential packets. Configurable alarms can notify the user about important events such as suspicious packets, high bandwidth utilization, or unknown addresses. Packet Generator utility is available for editing and sending packets via your wireless network adapter [35].

3.2.2 MAC Based Passive Scanning Tools

3.2.2.1 KisMAC

The passive scanner for Macs is named KisMAC. Rather than send out active probe requests, it instructs the wireless card to tune to a channel, listen for a short time, then tune to the next channel, listen for a while, and so on. In this way, it is possible to not only detect networks without announcing your presence, but also find networks that don't respond to probe requests namely, "closed" networks (APs that have beaconing disabled). But that's not all. Passive monitors have access to every frame that the radio can hear while tuned to a particular channel. This means that you can not only detect access points, but also the wireless clients of those APs[23][1] .

The standard AirPort driver doesn't provide the facility for passive monitoring, so KisMAC uses the open source Viha AirPort driver [36]. It swaps the Viha driver for your existing AirPort driver when the program starts, and automatically reinstalls the standard driver on exit. To accomplish this driver switcheroo, you have to provide your administrative password when you start KisMAC. Note that while KisMAC is running, your regular wireless connection is unavailable. KisMAC also supplies drivers for Orinoco/Avaya/Proxim cards, as well as Prism II-based wireless cards. KisMAC's main screen provides much of the same information as MacStumbler or iStumbler.

Features of KisMac [24][37]

- Reveals hidden / cloaked / closed SSIDs
- Shows logged in clients (with MAC Addresses, IP addresses and signal strengths)
- Mapping and GPS support
- Can draw area maps of network coverage
- PCAP import and export
- Support for 802.11b/g

3.2.3 Linux Based

3.2.3.1 KisMet

According to Jonny Milliken and Alan Marshall [13] Kismet is a wireless network detector, sniffer, scanner and intrusion detection system. It works with any wireless card that supports raw monitoring (RFMON) mode, and can scan 802.11b, 802.11a, 802.11n, and 802.11g traffic.

Studies of Syahrul Fahmy, Akhyari Nasir and Nooraida Shamsuddin [2] revel that Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting and decloaking hidden networks, and inferring the presence of non beaconing networks via data traffic.

Kismet’s features include the following [1] [19] [14]:

- Ethereal/Tcpdump-compatible data logging
- AirSnort-compatible weak-IV packet logging
- Network IP range detection
- Built-in channel hopping and multicard split-channel hopping
- Hidden network SSID decloaking
- Graphical mapping of networks
- Client/server architecture allows multiple clients to view a single Kismet server simultaneously
- Manufacturer and model identification of access points and clients
- Detection of known default access point configurations
- Runtime decoding of WEP packets for known networks

- Named pipe output for integration with other tools, such as an IDS like Snort
- Multiplexing of multiple simultaneous capture sources on a single Kismet instance
- Distributed remote drone sniffing

1.1.1.2 Mognet

Mognet is an 802.11b protocol analyzer/sniffer written in Java. It is available free under the GNU General PublicLicense. It is a simple, lightweight program [1],

Its features include the following:

- Real-time capture output
- Support for all 802.11 generic and frame-specific headers
- Raw/hex/ASCII views for any frame
- Text-mode capture for GUI-less devices
- Loading/saving capture sessions in Ethereal/libpcap/Tcpdump format

3.2.3.2 WaveMon

Wavemon is a monitor for wireless devices. It monitors the signal and noise levels, packet statistics, device configuration, and network parameters of wireless network hardware. This tool is not designed to assess performance over time. It gives a rolling report on how the wireless connection is functioning.

Wavemon [38] is a terrific little tool that does precisely this. It polls /proc/net/wireless many times each second to give you a rolling report of how your wireless connection is performing. Its simple curses interface keeps the code quite small, and is ideal for including in embedded to get real-time link data from remote access points. The main interface provides a nice graphical representation of the current link state. All of the statistics are updated in real time, making it ideal for monitoring point-to-point links and fine-tuning antennas on long distance shots. When you need a high performance signal and noise meter for Linux, Wavemon is hard to beat[24].

Its features include the following [39]:

- Overview screen, displaying all important information, such as device configuration, encryption, power management parameters, and network information, at once.
- Adaptive-level bar graphs for link quality, signal/noise strength, and signal-to-noise ratio
- Customizable “level alarm” feature that notifies the user of changes in signal-level strength audibly and/ or visually
- Full-screen level histogram displaying signal/noise levels and signal-to-noise ratio

IV. DISCUSSIONS AND SUMMARY

Overall there are two scanning Methodologies, Active and Passive. Wi-Fi Stumblers – which are free, easy to use for simple tasks, and available for most Operating Systems – is one of the tools that can be used for this purpose. One limitation of Stumblers is that they can find APs, but not Stations or non-802.11 interference sources. For complete vulnerability assessment, a portable WLAN Analyzer that can scan all RF channels, export details about all wireless devices, accurately plot results on floor plans, and make it easy to find newly-discovered devices is ideal.

Tools that implement passive scanning generate considerably better results than tools that use active scanning(stumblers) . The downside of passive scanning is that in order to gather any information, a client already connected to that specific network needs to be generating and therefore providing network traffic to be analyzed. While in RFMON mode, wireless clients are unable to transmit any frames; their cards are only able to receive, and therefore capture traffic. This limits the client to reporting only current or recorded network traffic .In APPENDIX-A we discuss the pros and cons of each of them. In APPENDIX-B, we discuss the various tools, categorize them according to Active/Passive and the suitable platform upon which they can work.

V. CONCLUSION

The study shows that wireless LANs are being the most spread technology over the world prone to many different kinds of attacks and are highly vulnerable to the threats of Hacking. The main outcome of this paper is the analysis of security holes and protecting the network from the hackers in order to prevent exploitation of confidential data. The first step in any vulnerability assessment is identification of all wireless devices near the site(s) under test.

Various Active and passive scanning tools such as stumblers, Kismet, KisMaC have been discussed that can etc to survey the Wireless locality. The tools that have been stated will give us the ability to break our own WEP/WPA security and this may be the time to go to the next rank of security.

REFERENCES

[1] Secure Network Infrastructures, Chapter no-1, page 1-26 EC-Council | Press Volume-5, Library of Congress Control Number: 2009933546, ISBN-13: 978-1-4354-8365-1, ISBN-10: 1-4354-8365-0

[2] Syahrul Fahmy, Akhyari Nasir and Nooraida Shamsuddin, “Wireless Network Attack: Raising the Awareness of Kampung WiFi Residents”, International Conference on Computer & Information Science (ICCIS), 2012, 978-1-4673-1938-6112, ©2012 IEEE, page 736-240]

[3] Mardiana Mohamad Noor and Wan Haslina Hassan, Wireless Networks: Developments, Threats and Countermeasures, International Journal of Digital Information and Wireless Communications (IJDIWC) 3(1): 119-134 The Society of Digital

Information and Wireless Communications, 2013 (ISSN: 2225-658X)
[4] M. Junaid , Dr Muid Mufti, M.Umar Ilyas, "Vulnerabilities of IEEE 802.11i Wireless LAN," Transactions On Engineering, Computing And Technology Vll February 2006 Issn 1305-5313.
[5] Martin Beck, Erik Tews, "Practical attacks against WEP and WPA," November S, 2005
[6] S Vinjosh Reddy*, KRijutha, K SaiRamani, Sk Mohammad Ali, CR. Pradeep Reddy, "Wireless Hacking - A WiFi Hack By Cracking WEP", 2nd International Conference on Education Technology and Computer (ICETC)-2012, 978-1-4244-6370-11 © 2010 IEEE
[7] Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, "Wireless Network Security: Vulnerabilities, Threats and Countermeasures", International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No. 3, July, 2008
[8] ARASH HABIBI LASHKARI, FARNAZ TOWHIDI, "Wired Equivalent Privacy (WEP)" International Conference on Future Computer and Communication-2009, IEEE Computer Society, 978-0-7695-3591-3/09 © 2009 IEEE, DOI 10.1109/ICFCC.2009.32
[9] Beck, M., Tews, E.: Practical Attacks Against WEP and WPA. In: Proc. 2009 Second ACM Conference on Wireless network Security (Wisec) 2009.
[10] Jelena Mirkovic, Sven Dietrich, Peter Reiher. Internet Denial Of Service: Attack and Defense Mechanisms. Prentice Hall Professional Technical Reference. 2005.
[11] Sriram, V.S.S, Sahoo, G., Agawal, K.K.: Detecting and Eliminating Rouge Access Points in IEEE-802.11 WLAN – A Multi-Agent Sourcing Agent Methodology. Birla Institute of Technology, India (2010).
[12] Jinyang Li, Charles Blake, Douglas S. J. De Couto, Hu Imm Lee, Robert Morris, "Capacity of Ad Hoc Wireless Networks," In Proc. Of Mobicom (mobicomOl) conference, 200l.
[13] Jonny Milliken and Alan Marshall, "THE THREAT-VICTIM TABLE A Security Prioritisation Framework For Diverse WLAN Network Topographies"
[14] Nguyen The Anh, Rajeev Shorey, "Network Sniffing Tools for WLANs: Merits and Limitations", 0-7803-896J-8/05/IEEE, ICPWC 2005
[15] Nwabude Arinze Sunday, "Wireless Local Area Network (WLAN): Security Risk Assessment and Countermeasures", thesis is presented as part of Degree of Master of Science in Electrical Engineering, Blekinge Institute of Technology, August 2008
[16] http://www.NetStumbler.com
[17] http://www.esecurityplanet.com/views/article.php/3869221/Top-Ten-WiFi-Security-Threats.htm dt:-27-9-14
[18] Cain & Abel, http://gexos.github.io/Hacking-Tools-Repository/#Scanning last accessed oct-2014
[19] Kershaw, M., 2010. Kismet [online]. Available at: http://www.kismetwireless.net/
[20] EC Council (2012). Certified Ethical Hacker: Hacking Wireless Networks, Module 15. pg 91-93.
[21] Regina D Hartley, "Ethical Hacking: Teaching Students To Hack"
[22] Wiley Publications, "Introduction To Ethical Hacking," available at www.media.wiley.com
[23] JOHNNY CACHE, JOSHUA WRIGHT, VINCENT LIU, "HACKING EXPOSED WIRELESS: WIRELESS SECURITY SECRETS & SOLUTIONS, Copyright © 2010 by The McGraw-Hill, ISBN: 978-0-07-166662-6, MHID: 0-07-166662-1
[24] Rob Flickenger, " Wireless Hacks" Copyright © 2003 by : O'Reilly, ISBN : 0-596-00559-8
[25] http://thebestwirelessinternet.com/netstumbler.html
[26] http://www.macupdate.com/app/mac/8035/macstumbler
[27] http://www.cqure.net/wp/tools/other/wavestumbler/
[28] http://manpages.ubuntu.com/manpages/karmic/man1/prismstumbler.1.html
[29] http://support.microsoft.com/kb/294818
[30] http://en.wikipedia.org/wiki/Microsoft_Network_Monitor
[31] http://blogs.technet.com/b/netmon/p/learn.aspx
[32] http://www.riverbed.com/products/performance-management-control/network-performance-management/wireless-packet-capture.html
[33] http://www.airpcap.nl/airpcap.htm
[34] http://www.tamos.com/products/commwifi/
[35] http://www.techspot.com/downloads/2641-commview-for-wifi.html
[36] http://www.dopesquad.net/security
[37] http://trac.kismac-ng.org/
[38] http://www.wavemage.com/projects.html
[39] http://www.blackarch.org/tools.html
[40] http://incident-management.blogspot.in/2011/11/passive-network-analysis-advantages-and.html

AUTHORS PROFILE

Ms. Rakhi Budhrani, MCA, M.Tech(IT), is presently a Research Scholar at Dept. of Computer Science, M.K.Bhavnagar University, Bhavnagar, Gujarat. She has done MCA from Indira Gandhi National Open University (IGNOU). She has also completed her M.Tech (IT) with specialization in Computer Networks. She has published and Presented 2 papers in the International Journal and 2 papers in National Journal. She has attended many workshops and three national and one International

conference. Her areas of interest are Computer Networks and Java technologies. She may be reached at rakhicnm@gmail.com

Dr. R. Sridaran has done his post graduation in Computer Applications and Management. He has been awarded the Ph.D in Computer Applications in 2010. Having started his career as an Entrepreneur, he has offered his consultancy services to various service sectors. He has also designed and delivered various training programs in the areas of IT & Management. He has published 14 research papers in leading Journals and Conferences and presently guiding four research scholars. He has got 17 years of academic experience and served in leading educational institutions at different capacities. He is currently the Dean, Faculty of Computer Applications, Marwadi Education Foundation's Group of Institutions, Rajkot, Gujarat. He may be reached at sridaran.rajagopal@gmail.com

APPENDIX-A

TABLE-1 NETWORK SCANNING TECHINQUES WITH THEIR PROS AND CONS

Scanning Methods	Advantages	Disadvantages
Active	• Highly scalable because scanning takes place from a central location or distributed locations of the security architect's choice and does not require software installation on the targets. • The technology can provide a hacker's view of the network and targets, so the vulnerability manager can have a realistic view of their risks in the production environment. • Potential to support any networked device, that is, not limited to a compatible platform for an agent. • Can provide incremental information regardless of platform support (e.g., open ports, identified protocols/applications, banners) even when the VM system has not previously seen the device.	• If the target is not connected to the network, it will not be scanned. Agents can detect vulnerability when it occurs and report the results the next time the host is connected to the network. • A potential exists for impact on the network infrastructure since all scanning is so performed. However, some basic planning will prevent such adverse effects. • Scanning is slower over slow network connections. This is typical in small offices with weak links.
Passive	• The analyzer does not interact with the network to discover hosts and their related vulnerabilities. Only the interface through which the user accesses the software to get reports is active. • Little to no testing is required to be certain there is no negative impact on the network or hosts. Since the technology is completely passive, little verification is required. Even if the device physically fails, it is not placed inline where it would have to handle the bits on the wire. • Sometimes, the device can be installed in tandem with existing IDS. This greatly simplifies implementation without any changes to the network switch. • The discovery process takes place continuously. New hosts are revealed as soon as they are connected to the network and begin communicating. In contrast to the active scanning and agents, vulnerabilities may not be known until the next scan cycle. • Hidden hosts can be discovered that do not listen for active probing traffic on the network. Instead, these hosts only communicate by initiating conversation on the network, and can therefore only be detected passively. • Since routing protocols and other network information are also visible to the traffic analyzer, it may also be able to map the topology of the network and use this information to create a picture of the attack surface of a more complex network. This type of information can also be obtained by authenticated active scans and by providing configuration data to specialized tools.	• The device typically must be installed on the switch that carries the traffic to be monitored. Remote monitoring of a network is often not practical over a busy WAN connection. This will limit the number of locations that can be scanned. If your organization requires monitoring on a broad geographic scale, this may not be the right technology. • The mechanism that copies switch traffic to the physical device can cause additional CPU load on the switch. That additional load can lower the performance of routing, access control, or other CPU-intensive operations. • There is limited visibility into vulnerabilities. Many of the vulnerabilities that can be detected with a host agent or active, authenticated network scan cannot be detected by analyzing network traffic. • Overall, passive analysis may not see as many vulnerabilities on systems but they function 24 hours a day and provide network topology information that would otherwise be unavailable. Changes to the environment on the network and hosts would be detected first using the passive analysis method if those vulnerabilities have a network footprint.

APPENDIX-B

TABLE-2 SUMMARY OF NETWORK SCANNING TOOLS WITH SUPPORTED PLATFORM

Scanner Type	Platform Type	Tool Name	Features
Active	Windows	NetStumbler Vistumbler	NetStumbler delivers a tool that helps you detect 802.11 a/b/g WLAN standards. While wardriving is its main use, the application also facilitates the verifying of network configurations. Vistumbler is a wireless network scanner written in AutoIT for Vista, Windows 7, and Windows 8. WiFiDB is a database written in php to store Vistumbler VS1 files. Keeps track of total access points w/gps, maps to kml, signal graphs, statistics, and more.
		inSSIDer	Gathers information from wireless card and software Helps choose the best wireless channel available Wi-Fi network information such as SSID, MAC, vendor, data rate, signal strength, and security Graphs signal strength over time Shows which Wi-Fi network channels overlap
		Ministumbler	A trimmed-down version called **MiniStumbler** is available for the handheld Windows CE operating system.
	Mac	MAC Stumbler	MacStumbler is mainly designed to be a tool to help find access points while traveling, or to diagnose wireless network problems. Additionally, MacStumbler can be used for "wardriving", which involves co-ordinating with a GPS unit while traveling around to help produce a map of all access points in a given area.
		iStumbler	wireless discovery tool, provides plugins for finding AirPort networks, Bluetooth devices, Bonjour services and Location information with your Mac.
	Linux	Wavestumbler	WaveStumbler is console based 802.11 network mapper for Linux. It reports the basic AP stuff like channel, WEP, ESSID, MAC etc.
		PrismStumbler	Prismstumbler is a wireless LAN (WLAN) discovery tool which scans for beaconframes from accesspoints. Prismstumbler operates by constantly switching channels and monitors any frames recived on the currently selected channel.
Passive	Windows	NetMon	Network Monitor is a utility that comes with Microsoft Systems Management Server and Microsoft Windows 2000 Server. You can use Network Monitor (also known as NetMon) to capture and observe network traffic patterns and problems.
		AirPcap	AirPcap is an adapter that captures all or a filtered set of WLAN frames and delivers the data to the Wireshark platform. Once AirPcap is installed, Wireshark displays a special toolbar that provides direct control of the AirPcap adapter during wireless data capture.
		Common View for WiFi	CommView for WiFi is a special edition of CommView designed for capturing and analyzing network packets on wireless 802.11a/b/g networks. CommView for WiFi gathers information from the wireless adapter and decodes the analyzed data.
	Mac	KisMac	KisMAC is an open-source and free sniffer/scanner application for Mac OS X. It has an advantage over MacStumbler / iStumbler / NetStumbler in that it uses monitor mode and passive scanning.
	Linux	KisMet	Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic.
		MogNet	Mognet is a simple, lightweight 802.11b sniffer written in Java and available under the GPL. It features realtime capture output, support for all 802.11b generic and frame-specific headers, easy display of frame contents in hex or ascii, text mode capture for GUI-less devices, and loading/saving capture sessions in libpcap format.
		WaveMon	wavemon is a ncurses-based monitor for wireless devices. It allows you to watch the signal and noise levels, packet statistics, device configuration, and network parameters of your wireless network hardware.