ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

Wireless Intrusion Detection and Logging System

Suraj Kendhey[1], Nitin Khobragade[1], Sumit Raut[1], Vikrant Naik[1]

Student, Department of Computer Technology, Yeshwantrao Chavan College Of Engineering, Nagpur –441110, India[1]

ABSTRACT: Intrusion detection is the security patrol, and become the eyes and ears of the network, alerting the potential vulnerabilities and intrusion attempts. Monitoring can help to spot problems in the network, as well as identify performance problems, but watching every second of traffic that passes through the network, manually searching for attacks, would be impossible. This is why there is need of specialized network intrusion detection software. This software inspects all network traffic, looking for potential attacks and intrusions. Wireless Intrusion Detection System (WIDS) is wireless network sniffing tool. It is used for securing the WLAN. And it generates the alarms to the administrator as soon as something goes wrong in the WLAN.WIDS attempts to identify computers system, network intrusions and misuse by gathering and analyzing data.WIDS can monitor and analyze user and system activities. It generates the alerts based either on predefined signatures or on anomalies in the traffic.

Keywords: Intrusion, sniffing tool, WIDS, WLAN, security.

I. INTRODUCTION

Wireless Intrusion Detection System (WIDS) is wireless network sniffing tool. It is used for securing the WLAN. And it generates the alarms to the administrator as soon as something goes wrong in the WLAN.

WIDS attempts to identify computers system, network intrusions and misuse by gathering and analyzing data.WIDS can monitor and analyze user and system activities. It generates the alerts based either on predefined signatures or on anomalies in the traffic.

The main objectives analyzed behind developing the Support Executive System are as follows:

- Network IP range detection
- Graphical mapping of networks
- Manufacturer and model identification of access points and clients
- Detection of known default access point configurations. Using WIDS we can make an efficient system to protect the wireless network. Implement attack recognition launch response to protect system or network.

WIDS units monitor all wireless LAN traffic and identify policy violations, misconfigurations, unauthorized operations, as well as many wireless LAN discovery and intrusion techniques.

To detect:

- Rogue Access Points.
- Mac Address Spoofing
- Port Scan Detection
- Unauthorized Mac Address Detection
- War Driving

II. BACKGROUND

A.Intrusion Methods

Signals from wireless networks are usually omni-directional and emanate beyond the intended coverage area. Such properties make the physical security of the network mostly impractical. Many passive and active intrusion methods quickly arose to abuse this weakness. Passive methods use radio frequency (RF) monitoring and do not broadcast any signals. Active methods may merely broadcast signals to query the status of the network, or they may even insert malicious data into the network to cause disruptions. This is a description of the most common methods and is by no means exhaustive, especially since new exploits and tools appear every week.

The most common wireless intrusion method is “Wardriving”. This is usually done using a Windows laptop running Wardriving software, such as NetStumbler, and equipped with an IEEE 802.11b adapter and external antenna. The “Wardriver” drives around high-tech neighborhoods hoping to detect IEEE 802.11b signals that have leaked out onto the street. NetStumbler looks for beacon frames from the access Points(Aps). From these beacon frames, it is typically possible to determine the encryption strength, channel, and type of hardware used. If the network is unsecured, the Wardriver may also record other details of the network like the Service Set Identifier (SSID). In many cases, this is performed by hobbyists and no further invasive action is taken. Such hobbyists would generally combine the data with Global Positioning System (GPS) information to produce geographic maps of wireless networks in the area and their configurations. There are other less common software available for Wardriving, depending on the platform used.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

DStumbler runs on BSD systems, MiniStumbler runs on PocketPC handhelds, Kismet runs on several platforms, and Wellenreiter runs on Linux systems. Depending on the software used, Wardriving ISBN 0-7803-7809-1/03/$17.00 ⚠ 2003 IEEE 68 Proceedings of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY June 2003 may be passive or active. Active software like NetStumbler, dStumbler, and MiniStumbler actually broadcast probe request frames to elicit responses from Aps [1]. This improves their chances of detecting Aps, especially when the Wardriver is in a moving vehicle. Passive methods merely perform RF monitoring to detect chance signals from the Aps.

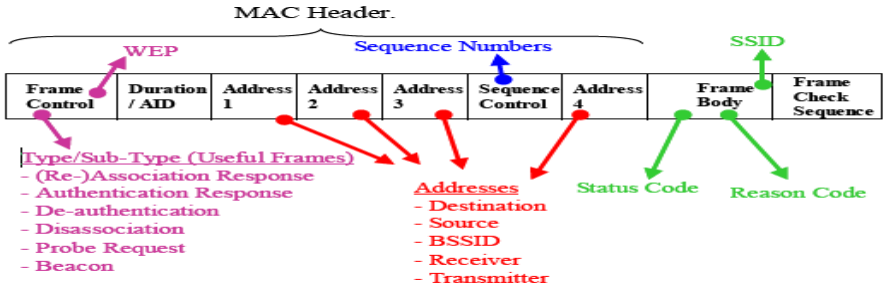
Another popular intrusion method concerns the infamous weakness in the Wired Equivalent Privacy (WEP) encryption used by IEEE 802.11b networks [2, 3]. This is usually the second stage of an intrusion following detection of a secured AP by Wardriving. The most commonly used tool for WEP key extraction is the Linux program AirSnort [4]. An intruder using AirSnort would surreptitiously collect wireless network traffic of the target network. When enough frames have been collected from the network, AirSnort can determine the WEP key of the network by examining the "weak" frames. It usually takes only a few hours to collect enough frames. Manufacturers have released updated firmware that addresses the transmission of such weak frames; however, a network remains vulnerable if a client continues to use an outdated wireless network adapter. A less common alternative to AirSnort is WEPCrack [5], but this program has less features and lower accuracy. AirSnort is a passive monitor and does not emit any signals.On many networks, intrusions are not limited to unauthorized clients but could include unauthorized Aps. Often, these "rogue" Aps might be installed by valid users attempting to increase the range of the network but doing so without proper authorization. This usually results in a security hole that may be exploited by intruders. A more relevant scenario would have an intruder planting an AP with a higher than normal broadcast power to masquerade as a legitimate AP. Unknowing clients would attempt to associate with this AP believing it is valid. The intruder could then use information collected from these association attempts to determine network security settings and other aspects of the network.

Also possible is a denial-of-service (DoS) attack on the network. This could occur in several ways, the most primitive being the use of radio equipment to broadcast noise at the 2.4 GHz operating frequency of the network. This would cause the network to drop frames, eventually to the point of total collapse. A more refined method would be to broadcast invalid frames to either clients or Aps, or even to both. The clients or Aps would respond to these invalid frames and, if present in sufficient number, these invalid frames could interrupt the flow of normal traffic.

A few other methods are proof-of-concept and have not been observed frequently in real networks. The first is the man-in-the-middle attack using Address Resolution Protocol (ARP) poisoning [6]. This uses a known vulnerability on Ethernet networks concerning unauthenticated ARP messages. Many systems have been developed for wired networks to counteract such poisoning but administrators often forget to extend this protection to wireless bridges which could also serve as entry points for such attacks.

A different method was demonstrated by 802.11ninja during DefCon in 2001 [7]. Using a program called Monkey Jack, management frames were sent to wireless clients at the convention forcing them to disconnect from valid Aps and re-associate instead with a bogus AP managed by the attackers. The attackers also offer code on their website to exploit other vulnerabilities even in wireless Virtual Private Networks (VPNs). All these rely on unauthenticated message vulnerabilities on IEEE 802.11b networks.

Figure1:



MAC Header Format

III. OUR APPROACH

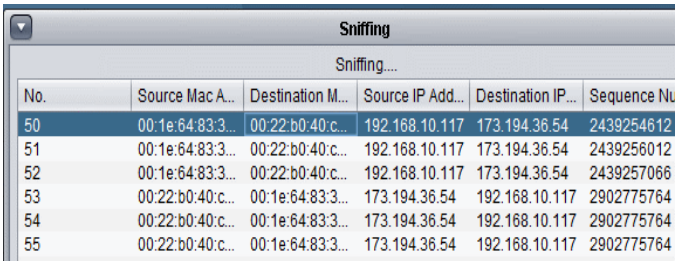
A.Track connection status of all clients.

The system shall track the status of each client (authorized or unauthorized) in real time, including, but not limited to, whether the client is offline, associated, or authentication pending. It must also detect and log illegal state transitions, such as, a client device transmitting data frames to a network device before being associated and authenticated. In order for this accumulated profiling information to be useful in determining usage patterns for each device and revealing deviations from normal patterns, the system must accumulate and analyze this profiling information over time. The system shall provide the system administrator with the ability to set this time length.

Figure 2

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013



Client Status

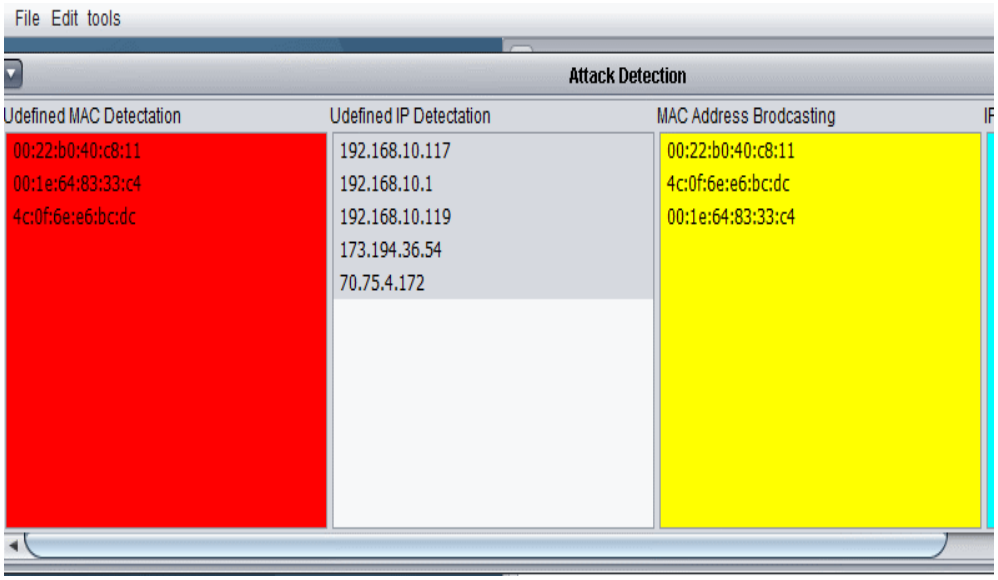
B.Detect and log unauthorized 802.11 transmiters

The system shall detect and log any unauthorized 802.11 transmitters operating in the area detectable by the sensors. Given the ubiquity of wireless equipment, it is reasonable to assume that three distinct threats to network security in the WLAN environment exist. First is the unwitting insider. It is increasingly likely that any laptop bought on the open market will have wireless capabilities. Moreover, it is quite likely the purchaser may not be aware of that fact. Such a person may accidentally activate this wireless device repeatedly over the course of an extended time period if undetected. Second is the witting insider, who may or may not have malicious intent. An example of a witting insider without malicious intent would be someone accustomed to using wireless on their home network deciding to ignore their organization's wireless policy because they enjoy the convenience of using wireless. Lastly, an example witting insider with malicious intent would be an insider with unauthorized hardware intending to use that hardware to attack or bypass the network's security measures.

C. Detect and log unauthorized clients attempting to connect to the network.

The system must detect and log any unauthorized clients attempting to connect to the wireless network. It must distinguish between the mere existence of unauthorizedhardware and an attempt by someone to use that hardware to connect to the wireless network. It is clear that the latter case presents a much greater danger to the enterprise network. There exist many documented instances of authorized personnel attaching unauthorized communications interfaces to their information appliances for the purposes of "making things easier." Logging events of both types makes the threat level more clear.

Figure 3:



Attack Detection

The system must detect and log any authorized clients associating to an unauthorized access point or communicating in ad-hoc mode with an unauthorized client.

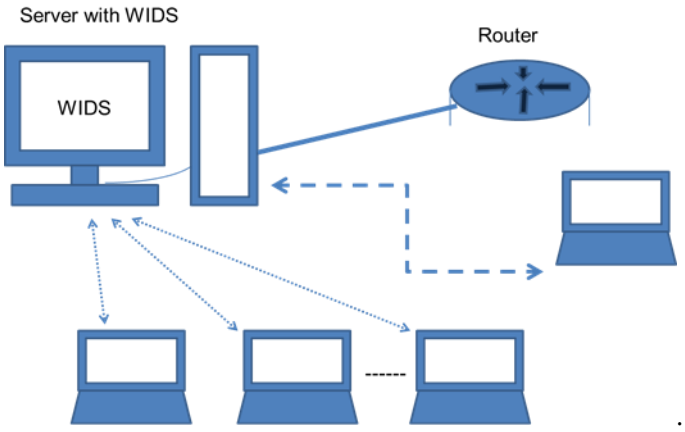
The hardware block diagram consists of a server having WIDS installed on it and a router connected to it. It also consist of client machines and the remaining machines which are not authorised.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

IV. HARDWARE DESIGN

Figure 4:



Block Diagram

V. CONCLUSION

We have argued that any secure network will have vulnerability that an adversary could exploit. This is especially true for mobile wireless networks. Intrusion detection can complement intrusion prevention techniques (such as encryption, authentication, secure MAC, secure routing, etc.) to secure the mobile computing environment. However, new techniques must be developed to make intrusion detection work better for wireless networks.

REFERENCES

[1] Yu-Xi Lim, Tim Schmoyer, John Levine, and Henry L. Owen, "Wireless intrusion Detection System And Response", IEEE Georgia Institute of Technology, 2009.
[2] Dragon pleskonjic," Wireless intrusion Detection System",2007.
[3] Haddadi F., Khanchi S., Shetabi M., Derhami V. , "Computer and Network Technology (ICCNT)", Second International Conference.,2010.
[4] Coppolino, L., D'Antonio, S., Esposito, M., Romano L., "Exploiting diversity and correlation to improve the performance of intrusion detection systems",
First International Conference on Network and Service Security, Paris, France, June 2009.
[5] SANS (Editor): "Wireless Networking Concepts - Network Security, Security Essentials ", V2.2., ISBN 0-9724273-6-8.,2009.
[6] Phifer, Lisa. "Open Source WLAN Analyzers", Jul. 20 2004.
[7]] Ristic, Ivan., "ModSecurity "website. URL: http: //www.modsecurity.org, 2006.