Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

An Overview of the Wireless Intrusion Detection System

Wireless technology has emerged as a very popular alternative to wired technology in recent years and has become readily available in more networks everywhere, whether it is for a home, an office, or any size of business. Wireless or WiFi technology is another way of connecting a number of computers to a network without using wires. WiFi uses radio frequency to connect wirelessly, so there is greater freedom to connect computers from anywhere in a home or an office network. This technology is similar to how a cordless ...

Copyright SANS Institute
Author Retains Full Rights

AD

An Overview of the Wireless Intrusion Detection System

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b

Option 1, Research on Topics in Information Security

Submitted by Oliver Poblete
24 January 2005

© SANS Institute 2005, Author retains full rights.

I. Abstract

Wireless technology can now be seen almost everywhere. This technology has recently become very popular, and with the convenience that comes with its use, it will probably be the most commonly used technology among computer networks in the near future. Unfortunately, new technology is always under fire when it comes to security, which is a topic that has now become more imperative and indispensable when dealing with transferring and storing sensitive computer information. The realm of wireless technology is still new, and as it becomes more common among many types of computer networks, hackers or intruders will find more ways to intrude a wireless system. We will discuss why wireless networks are vulnerable to such intrusions.

While the number of vulnerabilities and risks continue to rise, security engineers have attempted to slow and hope to eventually halt the many types of wireless network intrusions. A wireless network Intrusion Detection System (IDS) is a system for detecting such intrusions. Because of the multitude of methods of intrusions, there are several reasons why IDS is essential to any network, both wired and wireless. While the wireless IDS technology is new, we need to find out its capabilities and how it can help in providing a robust level of security for wireless networks. Additionally, we need to know what types of IDS are available and the drawbacks that come with using a wireless IDS.

II. Basics of Wireless Technology

Wireless technology has emerged as a very popular alternative to wired technology in recent years and has become more readily available for computer networks anywhere, whether it is for a home, an office, or any size of business. Wireless or WiFi technology is another way of connecting a number of computers to a network without using wires. WiFi uses radio frequency to connect wirelessly, so there is greater freedom to connect computers from anywhere in a home or an office network.[1] This technology is similar to how a cordless phone would work, using radio signals to transmit data from one point to another. However, wireless technology has restrictions on accessing a network, such as the network range. Two types of wireless networks are Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Bluetooth is the industry standard wireless technology that WPAN uses. These devices operate in a range of up to 30 feet away. Compared to the WLAN, the speed and wireless operation range are both less with the Bluetooth, but this technology does save on power and makes it more ideal for a number of personal devices, such as mobile phones, PDA's, headphones, laptops, speakers, and other battery-dependent devices.

In a WLAN, a device called an Access Point (AP), or key point, connects multiple computers to the network. The access point usually has a small

[1] Internet: D-Link Systems, Inc., D-Link Wireless Solutions; Retrieved 12/2005; Address http://www.dlink.com/tutorial/wireless/basics.asp?q=1

© SANS Institute 2005 Author retains full rights.

antenna attached, which allows the device to transmit data back and forth over radio signals. These radio signals can travel up to 300 feet. With an outdoor access point with larger antennas, a signal can travel up to 30 miles to serve public places such as college and high school campuses, airports, and many other outdoor venues.

The basic configuration of a WLAN is not much different from a regular LAN, except that the network uses radio waves instead of wires and cables. By adopting the use of radio waves, the range of communication is much farther than with infrared rays with much less interference[2]. The large frequency gap that exists between mobile phones and WLAN's allows less risk of crossing transmissions with other communication devices.

Because WLAN uses radio waves, there is the potential that a third party could attempt to access or intrude into networks illegally. To prevent such intrusions, one of the tools available for use is a wireless Intrusion Detection System.

III. Wireless Network Vulnerabilities and Risks

Having a wireless network set up has made life a lot easier by getting rid of the annoying wires and cables that may lie across the room, over the ceilings, and under the floors. Today's network marketplace indicates that wireless networking has been installed in many businesses, even in preference to the wired networks that have been commonplace for many years. By just about any measure, WLAN usage is growing at a rapid pace worldwide. However, this has also created an environment where there is great chance for intrusion, such as people being able to see each other's files and personal information. Therefore, Wireless LAN's still have their share of problems, with security playing a major part.

Not all networks, and definitely not all wired networks, are secure. In the case of a wired LAN, the level of security provided by the physical construction is usually sufficient. Adding the technology of wireless transmission, however, comes with vulnerabilities with which wired networks are often not required to deal with, such as the need to authenticate every network user. The following characteristics must be provided if security is desired for a WLAN[3]:

- Confidentiality: Assurance that the message sent is readable only by the intended recipient (i.e., protection against interception, or eavesdropping)
- Authenticity: Assurance that the message originates from the claimed entity (i.e., protection against spoofing, or impersonation)
- Integrity: Assurance that the message has not changed in transmission (i.e., protection from transmission errors and/or intended modification of message)
- Availability: Assurance that the data will be available whenever and

[2] Internet: Welcome to MagicLAN, WLAN Introduction; Retrieved 12/2004; Address http://www.magiclan.com/en/about/KmlMLanIntro_03.jsp

[3] Stanley, Richard A., Internet: Wireless LAN Risks and Vulnerabilities; Retrieved 1/2005; Address http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=13592

© SANS Institute 2005 Author retains full rights.

wherever required (i.e., protection against denial of service or poor reliability)

Wired networks already have to deal with a wide array of vulnerabilities against which they need to have themselves protected. However, in addition to all the vulnerabilities that are commonly seen on wired networks, wireless LAN's introduce a new series of risks. The most critical vulnerabilities are eavesdropping, illicit entry into the network, integrity attacks, denial of service, and even social engineering attacks. Since data on wireless networks are generally exposed to remote outsiders, true network security argues for cryptographic integrity checks. The IEEE 802.11 standard is by far the most popular and most commonly found WLAN standard at this time.[4] However, almost all wireless LAN's face the same collection of risks to message confidentiality, integrity, authenticity, and denial of service as are faced by the popular standard. Only the technical details of the individual vulnerabilities and risks and dealing with each threat differ from standard to standard.

Eavesdropping is the vulnerability of compromising the level of confidentiality that a wireless system possesses, and is the most highly visible since it is nearly impossible to control the transmitted radio signals and who can receive them. A network administrator must assume that any WLAN install is subject to this vulnerability by any third party. The prevalent solution would be to have data stream encryption, which is usually less than perfect when implemented.

Encrypted data frames are susceptible to serious integrity attacks. An attacker could potentially corrupt or make arbitrary modifications to an encrypted message without fear of detection, even with only partial knowledge of the message.[5] The WLAN then becomes vulnerable to a known plaintext attack, which is not so difficult to arrange; a sent e-mail by the attacker to a client of the WLAN only needs to be opened. Additionally, the repeatable characteristic of the initialization vector of a message provides another chance for attackers to pull out details of the messages and presents another way to alter messages without being detected. Although there are encryption features like wired equivalent privacy (WEP) to provide data integrity checking for wireless packets, it does not perform adequately. Insufficiency of WEP eventually led to the development of Wi-Fi Protected Access (WPA), which is a specification of standards-based, interoperable security enhancements that strengthens the level of encryption and authentication for WLANs.

Another vulnerability of the WLAN is possible illicit entry into the network due to poor authentication exploits. This is a major security hole for WLANs. Most administrators do not bother to change the default name, IP addresses,

---

[4] Internet: Wireless Network; Retrieved 1/2005; Address http://lifesci.rutgers.edu/~helpdesk/wireless.htm

[5] Boden-Cummins, Casper and Viney, Simon; Internet: Qinetiq; IPsec Over WLAN: Residual Vulnerabilities; Retrieved 1/2005;Address http://www.qinetiq.com/home/core_skills/knowledge_information_and_systems/trusted_information_management/white_paper_index.Par.0014.File.pdf

© SANS Institute 2005 Author retains full rights.

and level of access on the network interface cards used, so when a wireless client senses the access point, an easy attempt to connect to the network will most likely occur. Many WLANs are set up so that there is maximum coverage available for its intended users. This is great from a coverage standpoint, but this is not very helpful from a security standpoint. Anyone can connect to the network undetected from outside the network perimeter of the place of business. In addition, there is software available, such as NetStumbler[6], which can turn a wireless-capable laptop into a tool that detects wireless networks, presents users with the network identification and encryption information, and allows user to log into unprotected wireless networks.

A denial-of-service (DoS) attack is an attack in which an attacker attempts to leave the target network unable to serve its intended users. On a wired network, protocol-based attacks, such as SYN flooding and Ping of Death, which overwhelms the network thereby crashing the network servers, have become the most common types of DoS attacks. These attacks are also effective against wireless networks. WLANs are also vulnerable to DoS attacks that were previously unseen in wired networks. Since the radio signals must travel through exposed public airwaves, they are susceptible to radio interference either accidentally or deliberately. Although deliberate jamming attacks are not as common yet, they are certainly straightforward and easy to perform. All that is required is a transmitter, which covers the band in which the WLAN operates, that has sufficient power to overwhelm the relatively weak LAN nodes.

Finally, the largest risks to network integrity include the following. If a WLAN user loses a wireless network card, either by loss or by theft, the entire network cryptographic system can be compromised.[7] Therefore, new keys must be provisioned immediately for all remaining legitimate WLAN users to maintain security for the network. For the most part, this activity is logistically a discouraging chore for an administrator. There is also a great chance that the lost wireless network card will not be reported in a timely manner because either its loss was not discovered quickly enough by the user, or just ignores the loss of the wireless network card.

IV. Basics of Intrusion Detection Systems

An intrusion is when anyone, usually a hacker, attempts to break into or misuse a computer system. An Intrusion Detection System is a system for detecting such intrusions. A network IDS will continually monitor packets on a network wire and attempt to discover whether a break into the system has been attempted. The IDS can also try to determine other intrusions such as an attempt to cause a 'denial of service' attack to freeze the ability of the network to handle data traffic. In some cases, an IDS may be able to respond to anomalous or malicious traffic by taking action, such as reconfiguring a remote

---

[6] Internet: Netstumbler; Address www.netstumbler.com

[7] Stanley, Richard A., Internet: Wireless LAN Risks and Vulnerabilities; Retrieved 1/2005; Address http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=13592

© SANS Institute 2005 Author retains full rights.

firewall in order to block a user IP address or port from gaining access into a network.

An IDS may run on the target machine watching its own traffic (host-based), usually integrated with the stack and services themselves. Only packets from the device are monitored and they will provide alerts when suspicious activity is detected. Alternatively, an IDS can run on an independent machine promiscuously watching all network traffic (net-based). The IDS's are placed at strategic points within the network to provide maximum monitoring of all inbound and outbound traffic. There are IDS's that detect intrusion based on specific signatures of known malicious threats - similar to how most antivirus software protect against malware. On the other hand, there are IDS that detect intrusion based on comparing traffic patterns against a baseline and looking for anomalies. The baseline will identify what may be considered "normal" for that network, and that includes protocols, services, ports and IP's used. This type of IDS will alert against traffic that are anomalous, or significantly different, from the established baseline.[8] Additionally, there are passive IDS's and reactive IDS's. A passive IDS simply detects intrusion and alerts the appropriate personnel, who will decide which actions to take next. A reactive IDS will not only detect suspicious network traffic, but will also take pre-defined proactive actions as a response to the detected intrusion. Typically, this reaction involves blocking any further network traffic from the IP address or user of the network connection.

Best practices for securing a network includes a need to implement an IDS in order to monitor inbound and outbound traffic in the network. An IDS can identify suspicious and malicious traffic which has somehow managed to bypass the firewall. In addition, an IDS will be able to detect intrusion that may originate from inside your network. When dealing with wireless networks, the source of intrusion could come from almost anywhere since no direct connection with a wire or cable is required. The need of a wireless IDS has become an integral part of creating a secure wireless computer network. A wireless IDS is not very different from wired IDS, with additional deployment requirements as well as other unique features specific to WLAN intrusion and detection of exploitation.

V. Wireless IDS

The way IDS works on a WLAN is quite different from how it operates with a traditional LAN, primarily because when on a wired network, you have full control over what kind of traffic is being transmitted on the wires in your network. In WLANs, air is used as the medium, which means that the 802.11 frequency being broadcasted can bleed over other people's environments. Therefore, there comes a need to do internal and external monitoring for WLANs. Another difference is that wireless IDS's are needed for computer networks that have

[8] Bradley, Tony, Internet: About Inc., Introduction to Intrusion Detection Systems (IDS); Retrieved 1/2005; Address http://netsecurity.about.com/cs/hackertools/a/aa030504.htm

© SANS Institute 2005 Author retains full rights.

deployed WLANs and for enterprises that have not yet deployed one. The reason for this is that, although it may not be apparent, attacks from a WLAN into a wired LAN are a very factual threat. This threat is viewed as something that only concerns those who have configured a WLAN. But the truth is that all organizations who have configured a wired LAN should also perform monitoring for WLAN traffic to ensure that the air surrounding them does not pose as a threat to the devices within the organization, or within the accepted use for that organization[9]. You should always be concerned with the internal environment and rogue access points regardless of whether you have a wired or wireless LAN. Keep in mind also that rogue access points can be devices that have been installed either with or without malevolent intent. Sometimes you cannot be sure if someone in your network has deployed a WLAN when you assume that wireless technology has not been implemented.

Wireless IDSs can be obtained from several sources online through a vendor, or they can be developed in-house. Several vendors can provide wireless IDS, which usually comes with extensive effective features. Some of the popular vendors include Airdefense RogueWatch, Airdefense Guard, and Internet Security Systems Realsecure Server sensor and wireless scanner products. On the other hand, in-house wireless IDS can be developed by using available free software, such as Snort-Wireless and WIDZ, with the use of a Linux operating system.[10].

Wireless IDS can be configured to be centralized or decentralized depending on the network administrator's preference. When centralized, a combination of individual network sensors will collect and pass all collected 802.11 frequency data to a centralized management console, where the wireless IDS data can be stored and processed for detecting intrusion. For most centralized configured IDS, a number of sensors are implemented to perform the detection for the entire coverage. Logs and alerts are then reported to a single management console for convenience, allowing for easier analysis and reporting of data. The management console can also be used to manage and update all the sensors.

On the other hand, a decentralized wireless IDS usually consists of one or more devices that will perform both activities which is done by the sensor and the console. The latter is preferable for WLANs that are smaller and contain less than three access points, and is more cost-effective. When WLANs are larger, a centralized wireless IDS is ideal for easier management and effective data processing.

Typically, WLANs can cover quite a large physical area so that it can more easily provide more accesses that are convenient to its legitimate users. For this reason, many wireless access points (WAPs) can be set up for a

---

[9] Shopis, Mia; Internet: SearchSecurity.com; Wireless IDS, a crucial part of your security strategy; Retrieved 1/2005; Address http://searchsecurity.techtarget.com/qna/0,289202,sid14_gci931628,00.htm

[10] Bradley, Tony; Internet: About, Inc; Free Wireless Security Tools; Retrieved 1/2005; Address http://netsecurity.about.com/cs/hackertools/a/aafreewifi.htm

© SANS Institute 2005 Author retains full rights.

wireless network so that adequate signal strength is available for that area. One general rule when implementing a wireless IDS solution is that sensors should be deployed wherever a WAP is configured. An advantage found by doing this is that the majority of attempted attacks and exploits can be detected when there is a comprehensive coverage of the physical infrastructure of the wireless LAN with wireless IDS sensors at each WAP location. In addition, by following this rule of thumb, an attacker can more easily be pinpointed after being detected, when it is known to the administrator which sensor is in close proximity of the attempted intrusion.

Detection of the physical location of an attack is a critical aspect of a wireless IDS. For the most common standard 802.11, attacks are often carried out from a close proximity to a WAP, and most likely are carried out in an extremely short period to further avoid detection. When applying a physical response to an attempted wireless intrusion, it is imperative that not only does the response need to be logical as is with the wired IDS, which usually is configured to block or cutoff a connection from a suspected IP address by alerting another device or firewall, but also the response needs an additional element. The physical response needs to incorporate the physical exploitation of individuals in order to identify the attacker, and it must perform this in a timely manner. When compared with wired attacks where an attacker is usually at great distances from the affected LAN, attacks on WLANs usually involve attackers who are in close proximity to the WAP, and are therefore physically located on the local areas. Having a wireless IDS can definitely aid in being able to determine the attacker's location by analyzing the captured suspected wireless data with the location of the attacked WAP, and giving a general estimate of the attacker's physical location. An enhancement for the wireless IDS that could improve performance on this effort could be the use of directional antennae, which could further minimize the identified size of the location of the source of attack. If a security team were to further investigate an attempted wireless intrusion, even more actions can be taken after the physical location of the attacker has been narrowed. Such actions could include scanning the general vicinity identified by the wireless IDS by using tools like Kismet[11], which is an 802.11 layer 2 wireless network detector, sniffer, and intrusion detection system. The Kismet products identify networks by passively collecting packets from the remote area and detecting standard named networks, detecting and given time, uncloaking hidden networks, and surmising the presence of non-beaconing networks through analyses of wireless data traffic. A security response team will be able to identify and intercept suspected attackers more effectively with the combination of a wireless IDS and scanning tools.

In addition to physical location detection of attackers, wireless IDS can also help to enforce a robust security policy on an otherwise vulnerable WLAN. As mentioned previously, there are numerous security-relevant issues that deal

[11] Internet: Kismet; Address www.kismetwireless.net

© SANS Institute 2005 Author retains full rights.

with a wireless LAN, and in fact, many of these weaknesses can be made more secure. A strong wireless policy needs to be developed and then enforced properly. As a result, WLAN's vulnerabilities can be mitigated. A wireless IDS can aid in enforcing such policies.

The following features of the wireless IDS can provide a great enhancement for the security available for wireless networks:

- Most security policies applied on WLANs suggest that all of the wireless communications in the network should be encrypted. Therefore, while monitoring wireless 802.11 traffic and data from a WAP or other 802.11 devices, a wireless IDS can alert whenever unencrypted wireless data traffic has been detected.
- Another attribute that can be implemented on the wireless IDS is to create a listing or be pre-configured with all known and authorized WAPs, so that whenever an unidentified or rogue WAP is found in the network, the wireless IDS can quickly detect and alert.
- Additionally, enhancing enforcement of policies by the wireless IDS can take full advantage of human resources available. Some of the tasks that are usually carried out by administrators such as monitoring for unauthorized WAPs can be accomplished by automating this feature on a wireless IDS.

There are many forms of intrusions attempted on a wireless LAN, and an IDS can aid in detecting most of these. In addition to the previously mentioned capabilities of the wireless IDS, it can also detect other common and uncommon wireless attacks and probes. The first step taken by most hackers in an attempt to perform intrusion on a wireless network is to find a wireless network. To find such a network, usually an attacker would use some kind of a scanner software, such as the ones mentioned previously - Netstumbler or Kismet - to find nearby wireless networks. Along with the scanner software, an attacker may use a Global Positioning System to find their geographical location for easier access. Having a wireless IDS can allow a network administrator to detect these types of attempts and other scans and become more aware of what type of threats can be encountered by his/her WLAN.

Another vulnerability described earlier is the ability of some intruders to attack a wireless LAN is such a way that it is no longer able to respond or provide service to its legitimate users. A threat called a DoS (denial of service) attack may be more significant than probe and scan detection, and it can also be detected by a wireless IDS. DoS attacks are very common with WLANs, as many of these occurrences come from loss of wireless signal due to an intended or unintended frequency conflict or just from new structures that have been created in nearby areas. However, we cannot rule out that some of these occurrences can come from intended attackers that are attempting to deny services provided by the WLAN. The wireless IDS, when configured correctly, can detect many patterns, such as flooding authentication requests, or

© SANS Institute 2005 Author retains full rights.

disassociation/deauthentication frames[12]. Moreover, a wireless IDS can react to such an intrusion by signaling a nearby device, such as a firewall, to begin denying or blocking such traffic in order to free up services on the WLAN for its users.

Other types of attacks and threats to the WLAN can also be detected by a wireless IDS. One of the more common attacks is MAC address spoofing, which can be used by a hacker to be disguised as a WAP of the network, or as one of the legitimate wireless clients. This spoofing is being used currently in several available tools including HostAP and WLAN-jack, which is a tool that performs a DoS attack against users on a target wireless network by sending spoofed deauthenticate frames to a broadcast address, purportedly from the WAPs MAC address[13]. The presence of MAC address spoofing can be detected by a wireless IDS in a number of ways, one of which is sequence number analysis[14]. The wireless IDS is generally capable of detecting and recognizing ad-hoc WLANs, a common configuration which could potentially allow attackers to exploit a wireless device. However, a great attribute of a wireless IDS is that can detect intrusions that are new, or unique and non-standard, through the deployment of custom user developed rules. This is a flexible feature, which is common with most standard IDSs, that creates a scaleable security tool that can be modified to meet new and future threats and address a multitude of individual detection requirements.

The wireless IDS contains many features that address the security threats and vulnerabilities that are surrounding the popular wireless network technology. The features mentioned above provide a firm layer of security to an otherwise weakly secured WLAN. Simply having the knowledge that a WLAN is equipped with a wireless IDS may deter attackers from attempting intrusion, which is an enhancement to the security of the network.

VI. Downsides to the Wireless IDS

Although there are countless benefits and features to the wireless IDS, and that it is based on a proven and effective wired network IDS, we must consider that it is still a rather new technology. There are some drawbacks that may be considered when using wireless IDS. As with any new technology, some caution should be considered before applying them to an existing network or WLAN. There may be bugs and loopholes in the technology, which may, at worse, potentially weaken the security level of the WLAN, or increase its vulnerabilities. This is a stipulation that may not be a restriction in the near future, since wireless IDS technology is being developed and improved at a very

---

[12] Farshchi Jamil, Internet: Security Focus; Wireless Intrusion Detection Systems; Retrieved 1/2005; Address http://www.securityfocus.com/infocus/1742

[13] Wright, Joshua; Internet: Detecting Wireless LAN MAC Address Spoofing; Retrieved 1/2005; Address http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf

[14] Zalewski, Michal; Internet: Strange Attractors and TCP/IP Sequence Number Analysis; Retrieved 1/2005; Address http://alon.wox.org/tcpseq.html

© SANS Institute 2005 Author retains full rights.

rapid pace.

One drawback that may be considered is the cost of the wireless IDS, which when obtained from various vendors, can reach to high expenses that may become unaffordable or unreasonable. This is even more significant when you have a large range for your WLAN, which would require additional sensors to manage the entire coverage of the network. However, an ambitious developer could develop a homegrown solution to provide a wireless IDS for a WLAN. This approach could also prove to be somewhat expensive because of the amount of human resources required to develop such an effective security tool. Again, the amount of human capital would also grow in conjunction with the amount of coverage provided by the WLAN being protected. A network administrator would then have to assume that generally, the larger the WLAN coverage, and the more WAP are set up, then the more expensive the implementation of the wireless IDS will become.

One important aspect of the use of the wireless IDS, is that it will be only as effective as how well a network administrator will configure them. If they are tuned correctly and are pre-configured to know exactly what should and should not be on the network, then they will function to their optimal capability. However, when not configured correctly, a wireless IDS can be quite ineffective. Several hundreds false positives or false negatives could be produced which would present more confusion for the administrator, who may eventually just ignore data and alerts being provided by the wireless IDS. In general, IDSs are great tools for proactively monitoring and protecting the network from malicious activity, but they very prone to false alarms. Therefore, with any IDS solution, tuning is continually required for effective intrusion detection.

Similarly, the wireless IDS can also only be as effective as the administrators who will analyze and respond to the wireless data gathered by the wireless IDS. Similar to wired IDSs, vast human resources may be required to analyze and, more importantly, respond to the detected intrusion or threat. A wireless IDS may even require more resources than a wired IDS because of the need to address both the alert data found by the IDS, and the responsibility to find and catch the attackers located by the wireless IDS. Despite the numbers of downsides that exist with the wireless IDS, when it is used effectively and configured properly, it can still provide as a great security solution to a WLAN.

VII. Wireless IDS Available

There are a number of wireless IDS available online that can be purchased, and there are some that are available for free use. Listed below are a few of these wireless IDS and its correlating information:

- Airdefense Guard[15] is a commercial wireless IDS created by AirDefense, Inc. The Guard is an 802.11a/b/g wireless LAN intrusion detection and security solution that identifies security risks and attacks, provides real-

[15] Internet: AirDefense; Retrieved 1/2005; Address http://www.airdefense.net/products/airdefense_ids.shtm

© SANS Institute 2005 Author retains full rights.

time network audits and monitors the health of the wireless LAN. It is capable of detecting all rogue WLANs (Full functionality of AirDefense RogueWatch) and securing a wireless LAN by recognizing and responding to intruders and attacks as they happen. It also performs real-time network audits to inventory all hardware, tracks all wireless LAN activity and enforces WLAN policies for security and management. Lastly, it monitors the health of the network to identify and respond to hardware failures, network interferences and performance degradation.

- Neutrino Wireless Sensor is equipped with its own intelligent surveillance agent, purpose-built for 802.11. It looks at packets, devices, and clients to automatically detect a multitude of conditions that can influence wireless LAN security and performance. The Neutrino Sensors are small hardware appliances and include two network adaptors, one wireless and one Ethernet. They are deployed as necessary to provide comprehensive coverage to a physical infrastructure, since security threats may appear anywhere in the enterprise.
- WIDZ[16] is a proof of concept IDS system for 802.11 wireless networks. It guards WAPs and monitors local frequencies for malicious activity. It detects scans, association floods, and bogus/Rogue AP's. It can also be integrated with SNORT or RealSecure.
- The Snort-Wireless[17] project is an attempt to make a scalable, and not to mention- free, 802.11 intrusion detection system that can easily be integrated into an IDS infrastructure. It is completely backwards compatible with Snort 2.0.x and adds several additional features. Currently it allows for 802.11 specific detection rules through the new "WiFi" rule protocol, as well as rogue AP, AdHoc network, and Netstumbler detection.

VIII. Conclusion

When it comes to the ability to provide security to wireless local area networks, wireless IDSs will become an essential tool. Even though there are some downsides to implementing a wireless IDS to a WLAN, the advantages prove to outweigh these drawbacks. With all its capabilities along with assistance with policy enforcement, the advantages of the wireless IDS can be significant. Keep in mind however that the wireless IDS is only one part of a potential greater solution to wireless security. Other security measures may be deployed to reach the level of security desired for the entire WLAN, but the wireless IDS, which can identify and report on WLAN threat information, can greatly enhance the WLAN's security.

---

[16] Internet: Freshmeat; WIDZ; Retrieved 1/2005; Address http://freshmeat.net/projects/widz/?topic_id=43,245,151,152

[17] Internet: Snort-Wireless; Retrieved 1/2005; Address http://snort-wireless.org/

© SANS Institute 2005 Author retains full rights.

VIII. References

- Internet: D-Link Systems, Inc., D-Link Wireless Solutions; Retrieved 12/2005; Address http://www.dlink.com/tutorial/wireless/basics.asp?q=1

- Internet: Welcome to MagicLAN, WLAN Introduction; Retrieved 12/2004; Address http://www.magiclan.com/en/about/KmlMLanIntro_03.jsp

- Stanley, Richard A., Internet: Wireless LAN Risks and Vulnerabilities; Retrieved 1/2005; Address http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=13592

- Internet: Wireless Network; Retrieved 1/2005; Address http://lifesci.rutgers.edu/~helpdesk/wireless.htm

- Boden-Cummins, Casper and Viney, Simon; Internet: Qinetiq; IPsec Over WLAN: Residual Vulnerabilities; Retrieved 1/2005;Address http://www.qinetiq.com/home/core_skills/knowledge_information_and_systems/trusted_information_management/white_paper_index.Par.0014.File.pdf

- Internet: Netstumbler; Address www.netstumbler.com

- Bradley, Tony, Internet: About Inc., Introduction to Intrusion Detection Systems (IDS); Retrieved 1/2005; Address http://netsecurity.about.com/cs/hackertools/a/aa030504.htm

- Bradley, Tony; Internet: About, Inc; Free Wireless Security Tools; Retrieved 1/2005; Address http://netsecurity.about.com/cs/hackertools/a/aafreewifi.htm

- Shopis, Mia; Internet: SearchSecurity.com; Wireless IDS, a crucial part of your security strategy; Retrieved 1/2005; Address http://searchsecurity.techtarget.com/qna/0,289202,sid14_gci931628,00.htm

- Internet: Kismet; Address www.kismetwireless.net

- Farshchi Jamil, Internet: Security Focus; Wireless Intrusion Detection Systems; Retrieved 1/2005; Address http://www.securityfocus.com/infocus/1742

- Wright, Joshua; Internet: Detecting Wireless LAN MAC Address

© SANS Institute 2005 Author retains full rights.

Spoofing; Retrieved 1/2005; Address http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf

- Zalewski, Michal; Internet: Strange Attractors and TCP/IP Sequence Number Analysis; Retrieved 1/2005; Address http://alon.wox.org/tcpseq.html

- Internet: AirDefense; Retrieved 1/2005; Address http://www.airdefense.net/products/airdefense_ids.shtm

- Internet: Freshmeat; WIDZ; Retrieved 1/2005; Address http://freshmeat.net/projects/widz/?topic_id=43,245,151,152

- Internet: Snort-Wireless; Retrieved 1/2005; Address http://snort-wireless.org/

© SANS Institute 2005, Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced