Wireless Intrusion Detection Systems

Including

Incident Response & Wireless Policy

By

Jeff Dixon

Wireless Intrusion Detection Systems

Introduction

I. What is an IDS
    A. Signature Based
    B. Knowledge Based

II. Why use a WIDS
    A. What can be detected?
    B. Intrusion response

III. Incident Response
    A. The Process

IV. Choosing a WIDS
    A. Architecture
    B. Commercial
    C. Open Source

V. Wireless policy
    A. Why do you need Policies
    B. What should be included in your policy

Summary

Wireless Intrusion Detection Systems

Wireless has opened a new and exciting world for many of us. Its technology is advancing and changing every day and its popularity is increasing. The biggest concern with wireless, however, has been security. For some time wireless has had very poor, if any, security on a wide open medium. Along with improved encryption schemes, a new solution to help combat this problem is the Wireless Intrusion Detection System (WIDS). In the security and wireless world this has fast become a major part of securing a network. The next sections will cover details of what a WIDS is and can do, along with incident response, and creating a wireless policy.

What is an Intrusion Detection System?

An Intrusion Detection System (IDS) is a software or hardware tool used to detect unauthorized access of a computer system or network. (Wikipedia, 2005) A wireless IDS performs this task exclusively for the wireless network. These systems monitor traffic on your network looking for and logging threats and alerting personnel to respond. An IDS usually performs this task in one of two ways, with either signature-based or anomaly-based detection.

Almost every IDS today is at least in part signature-based. Attacks and their tools usually have a unique signature that can be detected and/or found. This means that known attacks can be detected by looking for these signatures. The downside to these is that they are easy to fool and can only detect attacks for which it has a signature. (Debar, n.d.b)

The other approach is anomaly-based systems. These are not often implemented, mostly because of the high amount of false alarms. An anomaly-based system develops a baseline of what it considers normal traffic. Any time it detects traffic which deviates from what it considers normal an alert is generated. The advantage is that it can catch many attacks that are new or unknown and that would never be seen by a signature-based IDS. The drawbacks consist mainly of large amounts of time being spent to train and retrain the IDS system, as well as the large amount of false alerts that have to be examined.(Debar, n.d.a) As a note, hybrid systems have also been evolving that use both signature-based and anomaly-based techniques.

Why Use a Wireless Intrusion Detection System?

The traditional wired IDS is a great system, but unfortunately it does little for the wireless world. The problem with wireless is that in addition to attacks that may be performed on a wired network, the medium itself has to be protected. To do this there are many measures which can be taken, however there are even more tools designed to break them. Due to the nature of wireless LANs (WLAN), it can be difficult to control the areas of access. Often the range of a wireless network reaches outside the physical boundaries of an organization. This creates limited control because it means an attacker can now sit in a car a mile away while he attempts to penetrate your network. With such a problem with wireless security, developing and implementing WIDS systems is definitely a step in the right direction. If you have wireless and are concerned about attacks and intruders, a WIDS may be a great idea.

A large number of possible attacks can be detected by a WIDS. The following will list major attacks and events that can be detected with the help of a WIDS. Rogue devices, such as an employee plugging in an unauthorized wireless router, incorrect configurations, connectivity problems, jamming, man-in-the-middle attacks, wardrivers, scanning with programs like Netstumbler or Kismet, RF interference, MAC spoofing, DoS attacks, attempts of brute force to get pass 802.1x, strong RFI, or use of traffic injection tools. (Valdimirov, Gavrilenko, & Mikhailovsky, 2004) Wired Equivalent Privacy (WEP)-related events can indicate legacy or rogue devices. This is because many organizations no longer allow WEP to be used and therefore by detecting WEP frames in use you can infer that either a legacy device is in use or someone has configured a rogue wireless device with WEP. (Valdimirov et al, 2004) Different WIDS devices and software have different capabilities in what can be detected. Make sure the WIDS you chose will fit your company's profile.

If detecting incidents is not enough, some WIDS systems now also incorporate the function of intrusion reaction. The process of intrusion reaction is simply that when an event occurs, the WIDS can automatically respond in a way that will stop the detected event from persisting. Examples of two such reactions are, weak key interference, and address rule matching. Weak key interference is designed to protect the weak keys in WEP that allow it to be easily cracked. The Idea is that encrypted frames are generated using a false key and hence prevents authentic frames from revealing the real key. Address rule matching is a way to determine if a fake MAC address is in use. If detected the address is redirected to a honeypot, quarantining the user from the production network. (Hsieh, Lo, Lee, & Huang, 2004)

Incident Response

Let's say you've got your WIDS up and running. You receive a high alert; your wireless is under attack! By most this would be considered an "Incident." An incident can be defined as an assessed event of attempted entry, unauthorized entry, or an information attack. (Incident, 2005) It is now time to go into action, or as some would say perform an incident response. But before you do, you need a plan to keep things from getting out of hand. Having a plan allows you to follow a step-by-step approach and avoid chaos and confusion in the midst of an incident.

Provided are seven steps to follow for when such an event occurs. These seven steps are preparation, identification, initial response, formulate response strategy, investigate the incident, reporting, and resolution. Preparation involves setting up systems to detect threats, creating policies, and organizing a response team that can respond when needed. Setting up your WIDS would be part of this first step. Identification of an incident (a threat which poses a risk and requires action) can also be provided in part by a WIDS that logs and alerts to potential threats. Often these alerts come from other sources as well, for example, staff members reporting unusual activity. Initial Response consist of recording what is taking place along with bringing in necessary staff or teams to start investigating and responding to the alert, as well as informing any higher authorities necessary. Formulating the response strategy is strait forward; determine the best plan of action, get approval and proceed with plan. Investigating the incident includes collecting a complete record of what happened including any data involved, what was done and by whom, along with when it happened and how to prevent it. This may include gathering

logs stored from the WIDS system, as well as determining any settings that may be modified to help prevent the threat in the future. Reporting and documenting every step and action taken, down to any command entered and by whom, is perhaps one of the most important steps involved in an incident response. A dressed up version of the report is also usually made for upper staff, while a complete record like what was created in the previous investigation phase may be kept for in-depth analysis at a later time. Finally resolution involves trying to prevent this from happening again. Tightening up your firewall and servers and adding/changing signatures and settings on your IDS/WIDS systems are all typical changes during the resolution phase. It also involves looking over what happened and how it was handled so that you can improve the process. What tools, procedures, and people, did or didn't work as planned and how or what can be done to improve the process. (Mandia, Prosise, & Pepe, 2003)

Choosing a Wireless Intrusion Detection System

Now that we have an idea of what can be detected and what to do during an incident, we need to decide which WIDS to implement and how. It is not within the depth of this paper to cover all vendors of WIDS systems; therefore, further research is suggested before choosing a WIDS. Here we'll discuss the architecture of a wireless IDS along with a general overview of Commercial WIDS systems vs. Open Source WIDS systems.

A wireless IDS can be deployed in one of two ways centralized or decentralized. In a decentralized environment each WIDS operates independently, logging, and alerting on its own. In addition this also means each WIDS has to be administered independently.

In a large network this can quickly become overwhelming and inefficient, and therefore is not recommend for networks with more than one or two access points. The idea behind a centralized WIDS is that sensors are deployed that relate information back to one central point. This one point would send alerts and log events as well as serve as a single point of administration for all sensors. Another advantage to a centralized approach is that sensors can collaborate with one another in order to detect a wider range of events with more accuracy. (Yang, Xie, & Sun, 2004) In this approach there are also three main ways in which sensors can be deployed. The first is by using existing access points (AP). Some access points on the market are able to simultaneously function as an AP and WIDS sensor. This option has the potential to be less expensive than the others however there is a downside. Using the AP for both functions will reduce the performance, potentially creating a "bottle neck" on the network. The second option is to deploy "dumb" sensors. These devices simply relay all information to the central server and rely on the server to detect all events. While inexpensive, all information is sent back to a central point causing an impact in the performance of the wired network and creating a single point of failure at the server. The third option is the use of intelligent sensors. These devices actively monitor and analyze wireless traffic, identify attack patterns and rouge devices as well as look for deviations from the norm. They then report these events back to the central server and allow an administrator to invoke countermeasures. (Madge, 2005)

Wireless IDS systems are available either as a complete hardware/software solution or as a software only solution. An example of one such commercial hardware device is AirDefense Guard (www.airdefense.net). Commercial systems are expensive

and can lack some configuration abilities, but they tend to be more of an out-of-the-box deployment, with less knowledge and work needed to get started. Commercial systems normally provide more technical support along with a more user friendly interface for configuration, monitoring, and reporting. One of the biggest disadvantages to many commercial sensors is the inability to change the antenna. Instead you typically have to buy more sensors to cover the area instead of just changing to a higher gain antenna. This can result in increased cost in equipment and time needed to setup and maintain additional devices. Examples of companies providing software solutions are: WiSentry (www.wimetrics.com), AirMagnet (www.gsec.co.uk), and WildPackets AiroPeek (www.wildpackets.com). Keep in mind also the security features or lack there of with the product itself. Does it use telnet and SNMPv1? Does it support SSH? If your WIDS is compromised it can do no good.

Open Source solutions provide many options and worlds of flexibility. These systems tend to work logically the same as the commercial solutions. They give you freedom to install on the hardware of choice. You also have more flexibility in the configuration of the software itself. Open source options are free with the exception of hardware and allow unlimited possibilities for installation, from modifying program functionality to custom hardware. However it often takes more time and effort along with a deeper knowledge to correctly install and configure open-source systems. Some examples include: wIDS which allows you to pipe the traffic into SNORT for further analysis, AirIDS, Kismet, and SNORT-Wireless. It is up to you to decide which will be the best solution for your network. There is never one solution that works for everything

so compare the capabilities of each, your budget, knowledge and needs and find one that works best for you.

Wireless Policy

By now you should have a good idea about what a WIDS is and what it can do. However before you go jumping in to set one up of your own, there is more you need to know. You need to ensure you create and have a wireless policy in place. Without one, you may violate privacy rights. You need to have a policy stating what will and will not be allowed on your wireless network. A policy establishes a set of guidelines that must be followed and often waves users rights to privacy.

Creating and enforcing a wireless policy is the most important aspect of wireless security. Without policy anything goes, within the boundaries of the law. Policies need to be read and understood by all employees and employees need to be constantly reminded of what the policy states. Either in your wireless policy or in another, an important issue that needs to be addressed is that of privacy. The Electronic Communications Privacy Act and various wiretapping statutes prohibit the interception of private communications. An exception to this is allowed by gaining consent. While the extent to which such laws apply to employees is not black and white, if you plan to conduct network monitoring of traffic and data among other things, it is best to ensure your policy be written to give consent of such actions, or face the possibility of legal actions. Your policy should be written with help from individuals of different backgrounds. This should include management, technicians, and users to represent different viewpoints and concerns. Also you will want your policy to be reviewed by a lawyer to ensure it will hold up in a court

of law. A wireless policy will not prevent threats from occurring but with a well written policy in place you can reduce the chances of such events taking place and ensure protection for when you are attacked.

Your wireless policy should include specific details concerning the following topics. Who is responsible for your wireless? Someone with knowledge of wireless and authority on your network needs to be listed in charge of wireless. Often when specifying such roles it is better to list a job title as opposed to a name. If you list specific names the policy must be changed each time that person leaves or changes roles. A risk assessment should be included that determines threats and vulnerabilities in relation to the WLAN. This may be added as a separate section to the policy as risk assessments constantly change and should be updated often. The policy should state whether the wireless is to be segmented from the remainder of the network. Depending on the needs of wireless users segmenting the WLAN can be beneficial. In the event the wireless segment was compromised, the wired LAN segment would still be protected. Your policy should include if you use authentication such as 802.1X. A big issue is confidentiality. This involves if and how communications are encrypted. The original standard for wireless encryption was Wired Equivalent Privacy (WEP). WEP has been found to have many flaws and can be easily cracked in a matter of minutes. Unless there are extenuating circumstances like the inability to update legacy equipment, WEP should never be used for encryption. If it can not be avoided it is better to use WEP over nothing as it does provide some layer of protection. When possible, WPA or WPA2 (802.11i) should be implemented with the use of TKIP or AES. Your policy should state what methods of encryption can be used, along with specifics such as encryption strength and key lengths.

Your policy should discuss logging and accounting. This includes details such as what will be logged and where the logs are stored. How long the logs will be kept and how often they are reviewed. Devices such as a RADIUS server can provide useful accounting information when used with wireless. An often overlooked issue is physical security. Your policy should address how devices will be physically secured. Most wireless devices have a reset switch and console ports. An attacker may reset a router to defaults and be able to gain instant access to your network, or if they have access to an insecure console port they can reconfigure you device to allow them access. You should address client security as part of your policy. It is highly recommended that all users be required to have an up-to-date firewall and anti-virus software installed before accessing the network. You also want to address ad-hoc connections. Many client cards automatically accept ad-hoc connections. This is a major security risk and it is recommended that this not be allowed with any nodes on the network. Your wireless technician may want to scan the area looking for rogue devices or RFI. Your policy should include what tools and frequencies may be used and by whom for this activity. A part of security that is often overlooked but never should be is education. When you educate your users, they get a better understanding of what is going on, what can happen, and what to be aware of. This makes everyone's life better. Your policy should include details about keeping users trained and aware of security issues. Your policy may also address issues such as static ARP, MAC and IP filters, SSID broadcast, and SSID naming schemes. If using a WIDS, then details of this need to be included as well. How it is to be deployed and maintained, along with details concerning storage and review of logs and alerts are all important to include. The last yet most important topic concerning policy is enforcement. For this to

work upper management must support the policy. Exceptions can not be made, the policy can not be "bent," and it must be followed by everyone. Users must read, understand, and agree to the policy and they must be reminded of the policy on a regular basis. (Farshchi, 2005) To see sample policies please visit the SANS website. (www.sans.org/resources/policies)

Summary

Wireless has and is opening many new possibilities for expanding networks. Its potential is amazing. As with most new technologies, wireless has several vulnerabilities. Luckily new developments like the Wireless IDS have come about that address many of these. Wireless IDS solutions are available from both the open-source and commercial markets and both have their advantages and disadvantages. In any network with or without wireless never forget the creation and enforcement of policy. Good luck and welcome to the world of wireless!

References

Debar, H. (n.d.). What is behavior-based intrusion detection? Retrieved November 4, 2005, from SANS Web site: <http://www.sans.org/resources/idfaq/behavior_based.php>

Debar, H. (n.d.). What is knowledge-based intrusion detection? Retrieved November 4, 2005, from SANS Web site: <http://www.sans.org/resources/idfaq/knowledge_based.php>

Farshchi, J. (2005). Wireless Policy Development (Part One)&(Part Two). Retrieved December 2, 2005, from <http://www.securityfocus.com/print/infocus/1732> <http://www.securityfocus.com/print/infocus/1735>

Hsieh, W., Lo C., Lee J., and Huang, L. (2004, Sept. 14). The implementation of a proactive wireless intrusion detection system. *Computer and Information Technology*, 2004, p. 581-586. Retrieved Apr 06, 2006, from <http://ieeexplore.ieee.org.jproxy.lib.ecu.edu/xpl/RecentCon.jsp?punumber=9381>

Incident. (n.d.). Glossary. Retrieved November 10, 2005, from US Army Web site: <https://atiam.train.army.mil/soldierPortal/atia/adlsc/view/public/6903-1/fm/3-13/glos.htm>

Madge, (2005). Wireless intrusion detection systems (ids) evolve to 3rd generation proactive protection systems. Retrieved Apr. 06, 2006, from <http://www.telecomweb.com/readingroom/Wireless_Intrusion_Detection.pdf>

Mandia, K., Prosise, C., & Pepe, M. (2003). Intro to the Incident Response Process. In INCIDENT RESPONSE & COMPUTER FORENSICS SE (pp. 12-32). Emeryville, California: Osborne.

Vladimirov, A. A., Gavrilenko, K. V., & Mikhailovsky, A. A. (2004). Counterintelligence: Wireless IDS Systems. In WI-Foo (pp. 435-456). Boston, MA: Pearson Education, Inc.

Wikipedia. (n.d.). Retrieved November 25, 2005, from Intrusion Detection System Web site: <http://en.wikipedia.org/wiki/Intrusion-detection_system>

Yang, H., Xie, L., & Sun J. (2004, June 2). Intrusion detection solution to wlans. Emerging Technologies: Frontiers of Mobile and Wireless Communication, 2004, Vol 2. p. 553-556. Retrieved Apr 06, 2006, from <http://ieeexplore.ieee.org.jproxy.lib.ecu.edu/xpl/RecentCon.jsp?punumber=9237>