GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Intrusion Prevention as Logical Evolution from Intrusion Detection

GSEC Assignment Version 1.2f
Jeff Schultise
December 11, 2001

Introduction:

Protection of information systems has been elevated to a record high priority in most organizations. The reasons for this vary, depending on the business in which the organization is engaged. Many businesses have implemented E-Commerce capabilities, which, by their very nature, increase exposure to outside threats. New Federal regulations have been issued targeting industries such as Health Care (HIPAA) and Finance (Gramm-Leach-Bliley Act) in an attempt to assure safeguarding of customer information. Additionally, the terrorist events of September 11 and beyond have further increased security awareness.

The firewall has been the focal point for securing communications networks and information systems from external threats. The problems with using a firewall as the sole defense mechanism are that the firewall is only as secure as the rules that have been implemented, and generally firewalls are deployed at the network perimeter. This means there is no protection from internally launched attacks. A solution to these potential shortcomings of firewalls is the addition of Intrusion Detection Systems (IDS). This paper describes the capabilities of IDS systems and the limitations inherent to many current IDS products. Finally, the next step in this technology, Intrusion Prevention, is discussed.

Business problem:

The need exists for tools designed to identify potentially malicious activity within computer networks and systems. The deployment of firewalls as defense mechanisms at the network perimeter is a necessary step in overall security architecture, but other safeguards must also be deployed to provide a ”Defense in Depth” posture. While firewalls do a good job of blocking certain traffic from entering a network, malicious traffic may enter due to oversights in creation of rule sets and policies within the firewall device or by masquerading as legitimate traffic. Intrusion Detection Systems are a valuable enhancement to the overall security strategy of an organization. Using IDS in addition to the firewall allows a mechanism for verification of the effectiveness of the firewall. IDS agents (sensors) are generally available in two varieties: host-based and network-based. While there are some similarities in the functions of both, they each provide certain distinct and complimentary benefits.
Deployment of only one of the available types of sensors would provide less than the best protection available.

© SANS Institute 2000 - 2005 Author retains full rights.

Network-Based IDS Sensors:

Network IDS sensors are designed to monitor traffic as it traverses network segments on which the sensors are deployed. The network sensors are able to detect activities such as SYN floods, port scans, password cracking and other known system assaults. They cause no impact on network performance as they passively monitor traffic traversing the network segment, utilizing a function available on some network adapters known as "Promiscuous Mode." Promiscuous Mode allows a system to receive all network traffic as opposed to only traffic containing its destination address. This is the method used by protocol analyzers in data collection. Network sensors can provide an early warning of attacks, but they cannot determine if the attacks are successful. Network sensors may miss traffic on busy network segments due to the intensive processing required to thoroughly analyze all network frames. Also, in switched networks, where network conversations are generally isolated to the pair of hosts actually communicating, all network traffic may not be visible to the sensor (some vendors, most notably Cisco Systems, are incorporating the IDS function into the switch, which will alleviate this issue over time). Finally, network sensors can be very expensive to deploy if required on a large number of network segments. The reason for high cost is due to high software license costs and the software requiring a high performance, dedicated computer to operate.

Host-Based IDS Sensors:

Host-based IDS sensors are installed on computer systems within the enterprise and are designed to monitor activity occurring on the host machine itself. Host sensors are able to detect activity such as login attempts (successful or failed) via the local console or from the network. They also can detect changes in user privilege levels, changes to or deletion of critical files, unauthorized access to applications or files, and are valuable in enforcement of corporate host security policies. Most Host IDS sensors use operating system log files as the basis for analysis. While this is a valuable function, it is inherently late in detection as the log file entries are written ***after*** events occur. Several current Host IDS products have some ability to block activity before the system is affected.

Both network and host IDS commonly use a database of known "attack signatures" to compare against observed traffic patterns. The database is periodically updated and made available by the IDS vendor, similar to updates provided by anti-virus tools. However, this approach presents a potential problem: the signatures may be out of date with regard to the most recently introduced threats. It is generally the responsibility of the IDS user to make sure the latest updates are applied to the sensors, and, in many cases, the sensors must be taken out of service when performing a signature update. This requirement can create periods of increased vulnerability. In using signature pattern analysis and comparison, a common problem is generation of false positives, or "noise." This can cause generation of a

© SANS Institute 2000 - 2005 Author retains full rights.

high level of invalid alerts and usually requires much "tuning" of the sensors to minimize the false alerts. As with the "Boy Who Cried Wolf", if the level of false positives is high, people will generally begin to pay less attention when alerts are generated.

Future Directions:

With sophistication of intruders increasing and the availability of automated hacking tools, it is becoming necessary for security systems to possess the intelligence and capability to block attacks as they are initiated. After the fact, the alerting of an observed attack cannot provide an adequate defense; after all, intruders can cause significant damage or compromise sensitive data in just a few seconds. In his book "Time Based Security" [1], Winn Schwartau discusses the following formula: Prevention > Detection + Reaction. This implies that the preventive/protective mechanism must be able to protect assets longer than the sum of time required to detect the activity and the time required to react to the attempt. Clearly, this is a difficult goal if automated response capability is not present. If the system cannot stop these attacks before they are successful, the alerting and reporting functions will provide limited benefit. When configuring sensors for automated action, a great deal of care must be used to minimize the risk of a self-imposed Denial-of-Service due to the sensor blocking legitimate activity or being manipulated by a knowledgeable intruder.

Recent developments in sensors from various vendors are offering advanced reactive/preventive capabilities. Examples of some automated responses are:

1. Sensor issues TCP reset to system being attacked, using the attacker's address. This effectively cancels the session.

2. Sensors may interact with firewalls to build dynamic rules or filters to block attacks.

3. Host sensors have some ability to intercept packets before they reach the operating system kernel and discard them if viewed as suspicious. The sensor has the ability to interact with the operating system to prevent certain activities that should never be permitted (even by legitimate users).

4. Sensors may use Heuristics to identify and track activity that is outside of normal or expected behavior.

Ultimately, the functions of Intrusion Detection sensors, firewalls and anti-virus scanners should be incorporated to provide a total solution. Still, some challenges exist in detecting malicious activity. One problem is data encryption (packet data cannot be analyzed before reaching final destination, and even after reaching destination, encryption is present until data reaches higher layers of the protocol stack in destination host). The solution to the encryption problem is only possible on host-based sensors. Insertion of the monitoring process must be at a sufficient level

© SANS Institute 2000 - 2005 Author retains full rights.

in the network stack to access the data in its unencrypted form, but low enough to allow blocking of unwanted traffic before damage may be done. Fragmentation of IP packets into multiple Ethernet or Token Ring frames is also a potential problem, since the whole IP packet must be reassembled in order for proper analysis to be performed. With the availability and rapid deployment of high-speed LAN technologies such as Gigabit Ethernet, another challenge for network-based IDS is providing sufficient processing power in the sensor to inspect and analyze all of the network activity. Adding specialized logic to the sensor to quickly filter obvious violations before reaching more CPU intensive analysis, such as signature comparison, is a method for assisting with the data rate issues.

Sample of Vendors Providing Some Preventive Capability:

Armored Networks Corporation

ArmoredServer – Provides multilevel protection: At network layer it blocks selected traffic like a firewall, at the operating system level it hardens the kernel to minimize vulnerabilities, at the application layer it uses "context adaptive code" to block known application exploits such as buffer overflow attacks, at configuration layer it can find and fix insecure system settings.

Cisco Systems

Cisco IDS Network Sensor - works with Cisco PIX Firewall and Cisco routers to dynamically create firewall rules or access lists to prevent observed attacks.

Cisco IDS Host Sensor (Formerly Entercept) – Can block software calls to operating system kernel by comparing to a continually updated database of known attack behaviors.

Harris Corp. STAT Division

Stat Neutralizer – employs standard and user defined policies to block certain activities at the operating system level – before operating system can be compromised.

Internet Security Systems

RealSecure Server Sensor – May be configured to block certain activities based on port number, IP address, etc. (similar to personal firewall).

Black Ice Sentry – Network based sensor can detect attacks, based on signature recognition and send notification to Black Ice agent to block attack.

© SANS Institute 2000 - 2005 Author retains full rights.

Black Ice Agent – Host based sensor can detect and block attacks, based on signature recognition.

Network-1 Security Solutions

CyberwallPLUS – Based on detailed knowledge of operating system weaknesses, in conjunction with protocol analysis and signature recognition, unauthorized or suspicious activity is blocked before damage can be done.

Symantec Corporation

NetProwler – Network Intrusion Detection sensor – works with Symantec Enterprise Firewall (Formerly Axent Raptor) and Checkpoint Firewall-1 to dynamically create firewall rules to prevent observed attacks.

Conclusion:

The tools available for securing information systems provide significant capabilities for detecting and blocking many types of attacks. Improvements to the existing tools will be a continuous process as new threats are introduced and as the processing power available for analysis of malicious activity continues to increase and become more affordable.

It is clear that active, automated intrusion prevention is a necessary capability for truly defending information systems from malicious entities. As Network Intrusion Prevention technology becomes more robust and mature, the real-time alerting functions will be less critical and necessary for only a small number of unusual attack types. In the majority of instances, historical reporting of attacks with details of attack type, intruder address, action taken, etc., will be adequate for use in the further hardening of routers and firewalls to minimize the processing load on Intrusion/Prevention sensors. The historical data will also be useful for forensic analysis leading to possible prosecution of attackers.

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

References:

[1] Schwartau, Winn. "Time Based Security," Interact Press/MEMCO, Seminole, FL (1999)

Clarkin, Michael. "Comparison of CyberwallPLUS Intrusion Prevention and Current IDS Technology." Network-1 Security Solutions, Waltham, MA (2001).
URL: http://www.network-1.com/products/intrusion_prevention.pdf

Armored Networks Corporation White Paper "Intrusion Prevention Evolution"
URL: http://www.armoredserver.com/intrusionprevention.htm (2001).

Harris, "Security Threat Avoidance Technology (STAT) Scanner."
URL: http://www.statonline.com/products/neutralizer/neutralizer.pdf (2001).

Andress, Mandy, "Intrusion Prevention: The Ultimate Security?"
URL: http://tisc.corecom/newsletters/31.html (2001).

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: July 22nd, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor