Network- vs. Host-based Intrusion Detection

A Guide to Intrusion Detection Technology

6600 Peachtree-Dunwoody Road
300 Embassy Row
Atlanta, GA 30348
Tel: 678.443.6000
Toll-free: 800.776.2362
Fax: 678.443.6477
E-mail: sales@iss.net

Introduction

Most traditional intrusion detection systems (IDS) take either a network- or a host-based approach to recognizing and deflecting attacks. In either case, these products look for ***attack signatures***, specific patterns that usually indicate malicious or suspicious intent. When an IDS looks for these patterns in network traffic, it's ***network-based***. When an IDS looks for attack signatures in log files, it's ***host-based***. Each approach has its strengths and weaknesses, each is complementary to the other. A truly effective intrusion detection system will employ both technologies. This paper discusses the differences in host- and network-based intrusion detection techniques to demonstrate how the two can work together to provide additionally effective intrusion detection and protection.

Technology Overview

Network Based Intrusion Detection

Network-based intrusion detection systems use raw network packets as the data source. A network-based IDS typically utilizes a network adapter running in promiscuous mode to monitor and analyze all traffic in real-time as it travels across the network. Its attack recognition module uses four common techniques to recognize an attack signature:

- Pattern, expression or bytecode matching,
- Frequency or threshold crossing
- Correlation of lesser events
- Statistical anomaly detection

Once an attack has been detected, the IDS' response module provides a variety of options to notify, alert and take action in response to the attack. These responses vary by product, but usually involve administrator notification, connection termination and/or session recording for forensic analysis and evidence collection.

Host Based Intrusion Detection

Host-based intrusion detection started in the early 1980s before networks were as prevalent, complex and interconnected as they are today. In this simpler environment, it was common practice to review audit logs for suspicious activity. Intrusions were sufficiently rare that after-the-fact analysis proved adequate to prevent future attacks.

Today's host-based intrusion detection systems remain a powerful tool for understanding previous attacks and determining proper methods to defeat their future application. Host-based IDS still use audit logs, but they are much more automated, having evolved sophisticated and responsive detection techniques. Host based IDS typically monitor system, event, and security logs on Windows NT and syslog in Unix environments. When any of these files change, the IDS compares the new log entry with attack signatures to see if there is a match. If so, the system responds with administrator alerts and other calls to action.

Host-based IDS have grown to include other technologies. One popular method for detecting intrusions checks key system files and executables via checksums at regular intervals for unexpected changes. The timeliness of the response is in direct relation to the frequency of the polling interval. Finally, some products listen to port activity and alert administrators when specific ports are accessed. This type of detection brings an elementary level of network-based intrusion detection into the host-based environment.

Strengths of Network-Based Intrusion Detection Systems

Network-based IDS have many strengths that cannot easily be offered by host-based intrusion detection alone. Many customers, in fact, deploy network-based intrusion detection when using an IDS for the first time due to its low cost of ownership and rapid response times. Below are major reasons that make network-based intrusion detection a critical component of sound security policy implementation.

1. ***Lowers cost of ownership*** – network-based IDS allow strategic deployment at critical access points for viewing network traffic destined to multiple systems. As a result, network-based systems do not require software to be loaded and managed on a variety of hosts. Since fewer detection points are required, the cost of ownership is lower for an enterprise environment.

2. ***Detects attacks that host-based systems miss*** – network-based IDS examine all packet headers for signs of malicious and suspicious activity. Host-based IDS do not see packet headers, so they cannot detect these types of attacks. For example, many IP-based denial-of-service (DOS) and fragmented packet (TearDrop) attacks can only be identified by looking at the packet headers as they travel across a network. This type of attack can be quickly identified by a network-based system looking at the packet stream in real-time.

   Network-based IDS can investigate the content of the payload, looking for commands or syntax used in specific attacks. For example, an attacker probing for the new Back Orifice exploit on systems not yet infected with the Back Orifice software can be detected by examining the packet payload. As above, host-based systems do not see the payload, and so are not be able to recognize embedded payload attacks.

3. ***More difficult for an attacker to remove evidence –*** network-based IDS use live network traffic for real-time attack detection. Therefore, an attacker cannot remove the evidence. Captured data includes not only the method of attack, but information that may help lead to identification and prosecution. Since many hackers understand audit logs, they know how to manipulate these files to cover their tracks, frustrating host-based systems that need this information to detect an intrusion.

4. ***Real-time detection and response*** – network-based IDS detect malicious and suspicious attacks *as they occur*, and so provide faster notification and response. For example, a hacker initiating a network based denial of service (DOS) based on TCP can be stopped by having a network-based IDS send a TCP reset to terminate the attack before it crashes or damages a targeted host. Host-based systems usually do not recognize an attack or take action until after a suspicious log entry has been written. By this time, critical systems may already be compromised, or the system running the host-based IDS may have crashed. Real-time notification allows rapid reaction according to predefined parameters. These responses range from allowing the penetration in surveillance mode in order to gather information to immediate termination of the attack.

5. ***Detects unsuccessful attacks and malicious intent –*** network-based IDS add valuable data for determining malicious intent. A network-based IDS placed outside of a firewall can detect attacks intended for resources behind the firewall, even though the firewall may be rejecting these attempts. Host-based systems do not see rejected attacks that never hit a host

inside the firewall. This lost information can be critical in evaluating and refining security policies.

6. ***Operating system independence*** – network-based IDS are not dependent on host operating systems as detection sources. By way of comparison, host-based systems require specific operating systems to function properly without having been compromised to generate meaningful results.

Strengths of Host-Based Intrusion Detection Systems

While host-based intrusion detection systems are not as fast as their network counterparts, they do offer advantages that the network-based systems cannot match. These strengths include stronger forensic analysis, a close focus on host-specific event data and lower entry-level costs. Host-based intrusion detection:

1. ***Verifies success or failure of an attack*** – Since host-based IDS use logs containing events that have actually occurred, they can measure whether an attack was successful or not with greater accuracy and fewer false positives can network-based systems. In this respect, host-based IDS make an excellent complement to network-based intrusion detection, with the network component providing early warning and the host component providing verification of whether an attack was successful or not.

2. ***Monitors specific system activities*** – host-based IDS monitor user and file access activity, including file accesses, changes to file permissions, attempts to install new executables and/or attempts to access privileged services. For example, a host-based IDS can monitor all user logon and logoff activity, as well as what each user does while connected to the network. It is very difficult for a network-based system to provide this level of event detail.

   Host-based technology can also monitor activities that are normally executed only by an administrator. Operating systems log any event where user accounts are added, deleted, or modified. The host-based IDS can detect an improper change as soon as it is executed. Host-based IDS can also audit policy changes that affect what systems track in their logs.

   Finally, host-based systems can monitor changes to key system files and executables. Attempts to overwrite vital system files, or to install trojan horses or backdoors, can be detected and stopped. Network-based systems sometimes miss this kind of activity.

3. ***Detects attacks that network-based systems miss*** – Host-based systems can detect attacks that cannot be seen by network-based products. For example, attacks from the keyboard of a critical server do not cross the network, and so cannot be seen by a network-based intrusion detection system.

4. ***Well-suited for encrypted and switched environments –*** Since host-based systems reside on various hosts throughout an enterprise, they can overcome some of the deployment challenges faced by network-based intrusion detection in switched and encrypted environments.

   Switches allow large networks to be managed as many smaller network segments. As a result, it can be difficult to identify the best locations for deploying a network-based IDS to achieve sufficient network coverage. Traffic mirroring and administrative ports on switches can help, but these techniques are not always appropriate. Host-based intrusion detection provides greater visibility in a switched environment by residing on as many critical hosts as needed.

   Certain types of encryption also present challenges to network-based intrusion detection. Depending where the encryption resides within the protocol stack, it may leave a network-based system blind to certain attacks. Host-based IDS do not have this limitation. By the

time an operating system, and therefore the host-based system, sees incoming traffic, the data stream has already been de-encrypted.

5. ***Near-real-time detection and response –*** Although host-based intrusion detection does not offer true real-time response, it can come extremely close if implemented correctly. Unlike older systems, which use a process to check the status and content of log files at predefined intervals, many current host-based systems receive an interrupt from the operating system when there is a new log file entry. This new entry can be processed immediately, significantly reducing the time between attack recognition and response. There remains a delay between when the operating system records the event and the host-based system recognizes it, but in many cases an intruder can be detected and stopped before damage is done.
6. ***Requires no additional hardware*** – Host-based intrusion detection resides on existing network infrastructure, including file servers, Web servers, and other shared resources. This efficiency can make host-based systems very cost effective because they do not require another box on the network that requires addressing, maintenance, and management.
7. ***Lower cost of entry*** – While network-based intrusion detection systems can offer wide coverage for little effort, they are often expensive. Deploying a single intrusion detection system can cost more than $10,000. Host-based intrusion detection systems, on the other hand, are often priced in the hundreds of dollars for a single agent and can be deployed by a customer with limited initial capital outlay.

Network and Host-Based IDS Response Options

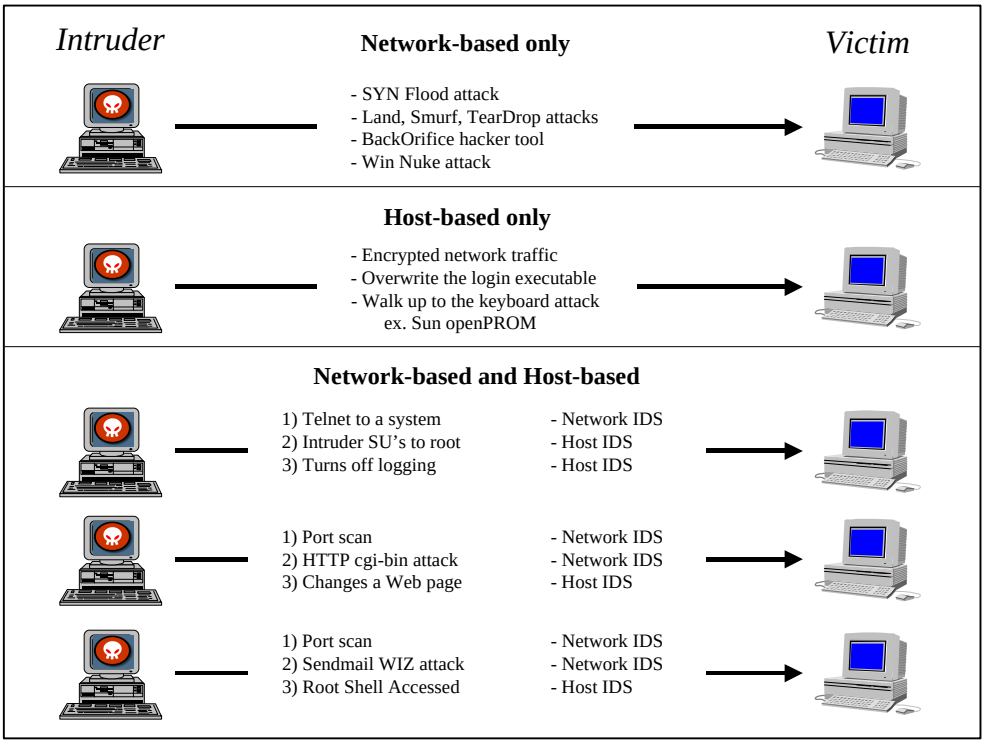
Response capabilities for threats and attacks are crucial for any intrusion detection system. Most network- and host-based IDS share common threat and attack response options. These responses fit into three categories: ***notification***, ***storage***, and ***active response***. Network- and host-based IDS also have additional capabilities representative of their host or network orientation.

	Network-Based IDS	**Host-Based IDS**
Notification	Alarm to Console	Alarm to Console
	E-Mail Notification	E-Mail Notification
	SNMP Trap	SNMP Trap
	View Active Session	
Storage	Log Summary (Reporting)	Log Summary (Reporting)
	Log Raw Network Data	
Active	Kill Connection (TCP Reset)	Terminate User Login
	Re-Configure Firewall	Disable User Account
	User Defined Action	User Defined Action

The Need for Both Network- and Host-Based Intrusion Detection

Both network- and host-based IDS solutions have unique strengths and benefits that complement each other. A next-generation IDS, therefore, must include tightly integrated host and network components. Combining these two technologies will greatly improve network resistance to attacks and misuse, enhance the enforcement of security policy and introduce greater flexibility in deployment options.

The graphic below illustrates how network- and host-based intrusion detection techniques interact to create a more powerful network defense. Some events are detectable by network means only. Others that are detectable only at the host. Several require both types of intrusion detection to function properly.



Intrusion Detection System Checklist

Features to look for in a next-generation Intrusion Detection System (IDS):

1. Network- and host-based intrusion detection integrated into a single system
2. Shared management console with a consistent interface for product configuration, policy management and single-event display for notifications from both host and network components
3. Integrated event database
4. Integrated reporting
5. Event correlation capabilities
6. Integrated on-line help for incident response
7. Unified and consistent installation procedures

Version 3.0 of RealSecure™, scheduled to ship in the fourth quarter of 1998, will meet all of these requirements.

- ***RealSecure Engine*** – detects attacks at the network level on 10/100 Ethernet, FDDI, and Token Ring networks
- ***RealSecure Agent*** – detects attacks on critical network servers and other host devices
- ***RealSecure Manager*** – management console that configures RealSecure Engines and Agenst, plus integrates real-time data and host log analysis into a seamless and comprehensive intrusion detection system

For more information on RealSecure 3.0, email Internet Security Systems at sales@iss.net, or call ISS at 678-443-6000 or 800-776-2362.