Network Intrusion Detection
Best of Breed Protection with Snort

by Jerry Askew, Associate Member of ILTA

Change is the only constant, and this adage is nowhere better exemplified than in the area of network security. While security exploits are increasing in number at a mind-boggling rate, their level of sophistication is increasing at an even more alarming rate. Even as the outside environment of cyberspace becomes increasingly hostile, traditional perimeter defenses are being weakened by VPNs, wireless technologies, remote access and mobile clients. Unfettered by the confluence of risks, business continues its relentless march toward increased reliance on technology — and it is your job to keep it all secure.

Why You Need an IDS

Businesses are faced with a wide variety of technological risks. Some types of risks are directly related to your technology or data assets such as unauthorized access, vandalism and resource theft. Other risks are secondary to your technology assets, such as the liability created by infringement of copyrights or the storage or transmission of offensive material. No matter the form, these all boil down to one thing — risk to your business.

Just as risks come in a variety of forms, the technology to mitigate these risks also takes various forms. An effective security configuration includes multiple technologies. No *single* tool or strategy by itself can provide effective, or even reasonable, protection against the technological risks faced by your organization. Several common risks are shown in the table below, which illustrates the effectiveness of various tools in addressing these risks.

Tools / Risks	Anti-Virus	Web Monitoring	IDS
Virus	***		
Worms	***		**
Malware	***		**
Spyware	*	*	
Browser Hijack	*	*	
Offensive Content		**	
P2P		**	**
Scripted Intrusion			***
Targeted Intrusion			***
Internal Hacking			***

Legend:
*** Provides effective protection
** Provides reasonable protection
* Provides minimal protection

While no security system can provide absolute protection, a well-designed system can prevent all but the most sophisticated attacks. Such a system will also serve to limit damage and liability in those incidents that cannot be prevented.

An IDS is an important component of your security system. Other technologies do not provide the means to detect a successful, let alone an attempted, intrusion. An intrusion that goes undetected for a period of time is certainly the most damaging security risk that a business can face, especially a business charged with a legal duty to maintain the confidentiality of client information.

IDS Backgrounder

The term "Intrusion Detection System" refers to a broad range of technologies, whose purpose is to (surprise) detect intrusions. These systems typically fall into one of the following classes.

Host-Based IDS (HIDS) – Systems that run on a target machine and monitor various types of activity on that machine. Typical HIDS include log parsing/reporting applications, file integrity checkers and protocol stack scanners.

Network IDS (NIDS) – Systems that monitor network traffic, potentially correlated from multiple sites, looking for unusual traffic patterns, signatures and behavior patterns of known exploits and other indications of an intrusion or attempted intrusion.

Network IDS Basics

Network IDSs work by scanning network traffic for suspicious activity. In order to be effective, a NIDS must be positioned strategically within your network topology. In a perfect world, a NIDS would monitor all network traffic; however this is not feasible in modern switched network environments. A reasonable and effective compromise is to monitor specific traffic concentration points, such as router interfaces and switch trunks/uplinks. In campus area and larger networks, the concentration points are likely to be geographically distributed. To accommodate this, a NIDS necessarily operates in a distributed fashion, with nodes at each physical location.

What Is Snort?

Snort is *the* leading Network IDS. Snort was named "Best Intrusion Solution" of 2005 by *Secure Computing Magazine*. Snort is open-source and runs on a multitude of platforms including Linux, Windows, *NIX, and Mac OS X. Snort is in widespread use, averaging over 70,000 downloads per month. Commercial support is available through Sourcefire (Snort's sponsor) as well as virtually any network security consultancy.

Snort's basic function is to monitor traffic on all connected network interfaces and compare that traffic against a set of attack profiles or *rules*. When a match occurs, Snort reports the alert information via any one of a number of user configurable output mechanisms. Output modules included in the distribution provide for logging to a SQL database, e-mail notifications, logging to a file and the generation of SNMP events.

Snort on the Lookout

Let's get back to our network model where Snort is the watchdog. In Snort terminology, each node is known as a sensor. A sensor may contain multiple network interfaces and can monitor a corresponding number of network segments. On small- to medium-sized networks, a single *sensor* may be all that is needed. For larger multi-location networks, multiple sensors are likely to be deployed.

A sensor may be connected to the network either by utilizing specially designed physical taps or by using the port mirroring (aka SPAN) feature of your network switch to duplicate traffic from an "interesting" port to your IDS.

On high-utilization full-duplex links, a tap is recommended since mirrored ports may be subject to saturation and packet loss. The use of hubs is discouraged because they introduce an additional point of failure and will significantly limit throughput on full-duplex links.

Management, Analysis and Reporting

A Snort-based NIDS is typically constructed from a number of independent applications. Snort itself provides monitoring, detection and alerting functions. In order to provide a complete solution, especially for large installations, it is necessary to add components that can manage all of the Snort sensors on the network. In addition, a system is needed to aggregate all of the alert data and perform analysis and reporting.

Snort is complemented by a number of applications that provide the aforementioned functions and more. A significant advantage of the open-source model, particularly with respect to Snort, is that you are free to choose from a variety of supporting applications to build a solution that uniquely addresses your particular needs. If you cannot find the perfect combination, you can modify any part of the system to make it "just right."

Management via SnortCenter

A popular application for managing Snort sensors is SnortCenter. SnortCenter is a Web-based management console that provides for centralized monitoring and configuration of an arbitrary number of Snort sensors. From the console, you can quickly see the status of all of the sensors on your network. Sensors can be stopped, started and configured via SnortCenter's straightforward interface.

Reporting via ACID

Snort generates alert data whenever suspicious traffic is detected. In a typical system, alerts occur frequently and create voluminous amounts of data. While certain events may be interesting in and of themselves, intrusion detection is more often about analyzing traffic patterns and trends. The Analysis Console for Intrusion Databases (ACID) provides a number of tools for analyzing the alert data generated across your network.

ACID can summarize the alert data from all of your sensors and provide statistics and graphs based on any number of factors including: location, source, destination, time of day, day of week, protocol, event type and more. For ease of use, ACID can be integrated within SnortCenter.

Operating Considerations

When implementing any system, it is important to consider and allocate the resources necessary for ongoing operation. This is especially true for an IDS — an IDS is not a "set and forget" type of system. An unmonitored IDS serves no purpose other than to lull you into a false sense of security. NIDSs require signature updates, similar to antivirus applications, in order to detect the latest exploits. Personnel must constantly review alert data and make adjustments to rules to compensate for changing network conditions. Recognizing these needs and planning accordingly is the single most important thing you can do to ensure an effective solution.

Conclusion

An intrusion detection system is a necessary part of your security infrastructure. Snort is recognized as the leading Network IDS and can be easily deployed. Being open-source, Snort requires little or no capital investment and can be modified to suit your exact needs. The ongoing operating costs and time requirements of Snort are comparable to those of vendor-supplied IDSs. If the security of your network is important to your business, Snort is an excellent choice for intrusion detection.

Due to space limitations, the details for implementing Snort are presented in a companion article available on ILTA's website at www.iltanet.org from the Communications tab on the navigation bar.

About our author . . .

Jerry Askew is an Associate Member of ILTA. He was formerly the Chief Information Officer for Loeb & Loeb LLP. Jerry is an active member of ILTA's Open Source Software Peer Group. He can be reached at jerry@askew.net.

This article was first published in ILTA's May, 2005 issue of Peer to Peer *and is reprinted here with permission. For more information about ILTA, visit their website at www.iltanet.org.*

Snort is the *leading Network IDS. Snort was named "Best Intrusion Solution" of 2005 by* Secure Computing Magazine.

ILTA's Values:

- Maximize the value of technology in support of the legal profession
- Provide quality, independent, unbiased and accurate information to our members about technology and the practice of law
- Maintain vendor independence
- Provide quality educational opportunities for our members and ongoing learning for navigating through change
- Foster, rely on and celebrate volunteers for their real world experience and their value as a resource for colleagues
- Recruit and retain the highest caliber of professional staff
- Act as a vehicle for meaningful peer networking
- Respect our colleagues
- Commit to the highest standard of professionalism
- Maintain a financially sound organization that provides full value for the members' investments