Schlumberger

Technology Brief: Monitored Intrusion Detection Systems

Cyber-Crime Statistics

- 90% of large organizations detected computer security breaches in the last 12 months — even though several implemented firewall protections

  Reference: Computer Security Institute, 4/7/02

- 80% reported financial losses, with total cost in excess of $455M

  Reference: Computer Security Institute, 4/7/02

- More than 50 vulnerabilities were discovered in web-related packages in 1999 alone—no firewall could prevent these being attacked

  Reference: SecurityFocus.com

- Sites that follow a zero-tolerance monitoring and response policy report that most serious attackers are deterred—in addition, uptime is significantly increased

  Reference: all.net, counterpane.com

by Aurobindo Sundaram

Most enterprise networks are protected from the Internet by firewalls. While firewall protections are essential, they rarely identify types of attacks, or attacks on allowed services. Intrusion Detection Systems (IDS) allow administrators to detect and respond to these attacks. However, IDS are of limited use without monitoring. Monitored Intrusion Detection Systems (MIDS) offer real-time detection and response to attacks, including dynamic blocking, complaints to ISPs and report generation. MIDS are not an alternative to firewalls, they are an essential complement to them. Due to the extensive reporting built into them, they also serve as effective deterrents.

Protecting Enterprise Networks

Most enterprise networks are protected from the Internet by a firewall (or set of firewalls). These firewalls are installed at control points (usually Internet gateways) and have strict rules that ensure that only certain types of traffic can travel from the Internet to the corporate network, and vice versa.

Limitations of Firewall Protection

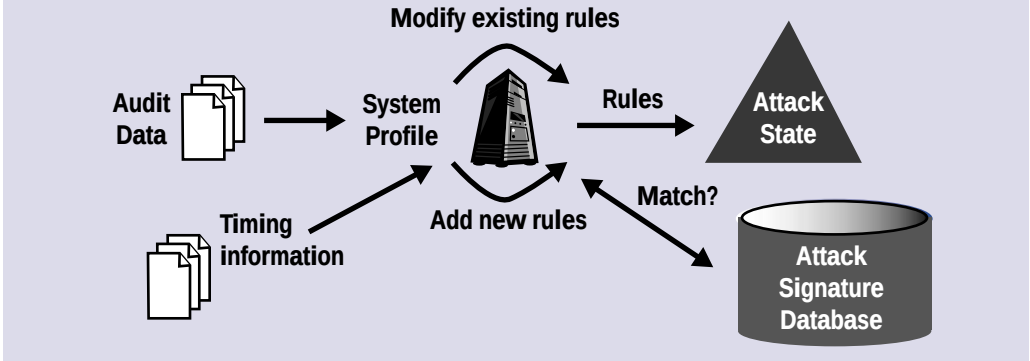
To be effective, firewalls must be installed at every single ingress point into a network. A firewall can only protect against attacks that pass through it; it cannot protect against an internal user who connects via another route such as dialing up the Internet.

While firewall protections are essential, they rarely identify types of attacks, or attacks on allowed services. Firewalls that allow web traffic cannot, in general, detect attacks on a web server. Firewalls maintain their niche in simple "allow/deny" logic at the network layer. This is not sufficient protection for the various network-based attacks seen today. As a result, many web servers have suffered from known, publicized attacks.

Finally, firewalls do not monitor the actions of authorized users. Most security incidents are caused by insiders or authorized users (due to the high level of access they have to the system). Therefore, not being able to monitor their actions is a serious deficiency.

IDS allows administrators to monitor these attacks. To use an analogy, firewalls are locks on doors, while IDS are smart alarm systems.

Figure 1: Misuse detection



DeXa
Suite of Services
Enabling the promise of the digital enterprise

Types of Intrusion Detection Systems

There are two distinct types of IDS. *Misuse detection systems* maintain a database of known attacks on systems (in the form of network packet types, suspicious URL accesses, etc.) and then match their input to this database in real-time. *Anomaly detection systems* depend on knowing what "normal" system behavior is, and then finding behavior that is markedly different from the norm.

There are also classifications of IDS based on the type of traffic they monitor, namely *host-based* and *network-based*—their functions are fairly self-explanatory.

In this Technology Brief, we will concentrate on network-based misuse detection systems. In part, this is because most commercial IDS are misuse-based, and work best when listening to network traffic.

Monitoring Intrusion Detection Systems

It should be apparent by now that simply implementing IDS does not solve all security issues. In particular, they can only detect attacks on traffic that flows through them. The logical process is to implement IDS at the Internet gateways, as well as at Intranet choke points and critical enclaves. It is important to note that IDS can be used independently of firewalls.

Monitored Intrusion Detection Systems (MIDS) are an extension of IDS—all the leading "M" means is that the results of IDS are monitored continuously, and actions performed. These actions generally include:

- Attack response (manual or automatic) in real time—using smart network re-configuration, dynamic blocking rules, etc.
- Attack monitoring in real time
- Statistics gathering and report generation
- Traffic filtering based on arbitrary rules (for example, if a new attack is occurring)

In addition, there have been situations where administrators have configured MIDS to detect and respond to virus outbreaks, such as W32/QaZ and ILOVEYOU.

It is a fundamental truth of Information Security that all the security in the world does no good, unless there is continuous monitoring and response of the security system (the feedback loop). MIDS are important deterrents of attacks for the following reasons:

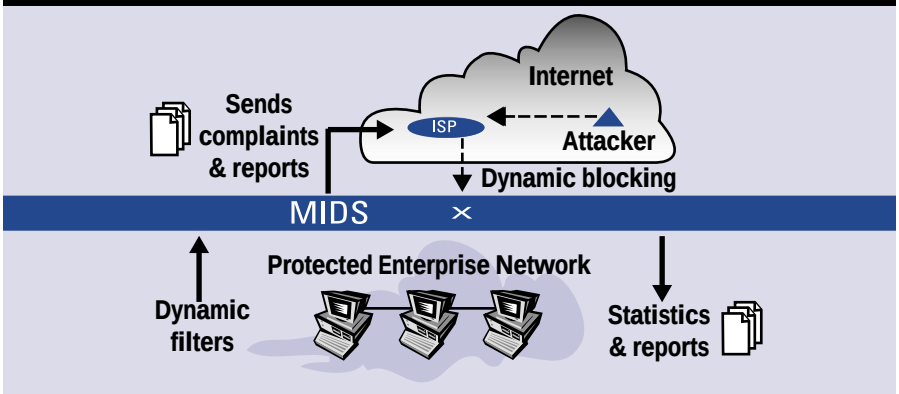
- An actively monitored system ensures that attackers know that their attempts will be detected. Such attackers typically pick a softer target.
- Law enforcement requires that adequate logs of attacks be maintained in order to press charges.
- Actively notifying the attackers' ISPs ensures that they lose their access to the system—fewer attackers on the network means fewer attacks.

Legislation and Privacy Concerns

There are several potential issues with using MIDS (or even IDS for that matter). One of them is privacy legislation. In the U.S., all traffic on an enterprise network "belongs" to the corporation, and users explicitly sign documents permitting the corporation to monitor any and all traffic across the network. This is a fairly clear-cut case, where the user has no significant privacy rights. In the European Union and some other countries, however, it is not as clear. For instance, the Data Protection Act in the United Kingdom states that a user's e-mail logs should be viewable by the user on demand. Furthermore, users should be notified that they are being monitored. This is a sensitive issue, especially when, for instance, users' web surfing habits are being monitored. In France, there is case law that prohibits the viewing of e-mail without notification. It is unclear whether the use of MIDS and other network monitoring tools is considered "user monitoring." The precedent should be established before long, and IT managers in these countries are advised to tread carefully.

Privacy issues with the use of MIDS are real, but concerns are overstated. Although MIDS were designed to allow filtering/monitoring of every network packet, their primary niche is detecting known attack patterns. They do not do very well at user monitoring, and it is doubtful that anyone wanting that sort of monitoring would select a MIDS to do it.

Figure 2: MIDS functionality



Summary

Every knowledge-based organization is at risk from increased attacks, both malicious and accidental. Most enterprises already run firewalls, yet intrusions still occur at a frightening pace. MIDS can serve as an effective deterrent against attacks—good security simply means that an attacker chooses someone else to attack, instead of you. Large enterprises that depend on networks for their business must implement a MIDS of some kind to remain operationally viable in the future.

Smaller organizations should carefully consider their options before investing in such systems. Well-run MIDS are invariably expensive because of the cost of responding to thousands of attacks each day. Instead of protecting their entire Intranet, these organizations may opt instead to simply protect their critical services (e-commerce servers, web servers, servers in the Demilitarized Zone, or DMZ) with MIDS, and protect the rest of their organization with a firewall.

For More Information

- http://www.gocsi.com/press/20020407.html
- http://online.securityfocus.com/cgi-bin/sfonline/vulns.pl

©Schlumberger

Other product and company names mentioned herein may be trademarks of their respective owners.

DeXa
Suite of Services
Enabling the promise of the digital enterprise