Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Intrusion Detection - Systems for Today and Tomorrow

In today's booming e-commerce economy age, virtually every business, including the 'brick and mortal', is connected to compete for market share in the cyberspace. Enterprise's networked systems are inevitably exposed to the increasing threats from external hackers as well as from internal. The consequences can be loss or modification of critical business data, disruption of services (availability), compromise of proprietary business plans or processes (confidentiality and integrity). To counter these threats, Informati...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

Intrusion Detection - Systems for today and tomorrow

Ho, Swee Yenn (George)
Version 1.2e

Introduction

In today's booming e-commerce economy age, virtually every business, including the 'brick and mortal', is connected to compete for market share in the cyberspace. Enterprise's networked systems are inevitably exposed to the increasing threats from external hackers as well as from internal. The consequences can be loss or modification of critical business data, disruption of services (**availability**), compromise of proprietary business plans or processes (**confidentiality** and **integrity**).

To counter these threats, Information Security organization today deploy many methods, tools and technology to defend the legitimacy of the systems. Methods like implementing policies and procedure, user awareness, deploying firewall and authentication systems, control systems access and forming computer incident handling teams. Theses approach aims to prevent, protect, detect, contain, eradicate, recover and serve as a lesson learnt.

This paper will examine the intrusion detection systems, one of the relative new technologies in information security. It aims to explore, in high level, the intrusion detection systems available today, as well as new developments in the technology.

Intrusion Detection Systems (IDS)

At its core, IDS for computer network systems resemble burglar alarm systems to a physical building, it is capable of detecting and alerting the systems administrator on potential intrusion, providing guidance against any potential loss of integrity and confidentiality to the enterprise's valuable intellectual assets.

Firewalls and authentication are effective in protecting and preventing unauthorized access to the systems but lacks capabilities to monitor the network traffic where majority of attacks are taking place. These attacks could be initiated by disgruntled employees and others who have legitimate network access and use that privilege to do harm.

Firewall and authentication systems are vital, but they work at the point of entry to the network, if an attack able to breached the firewall, he can roam freely through the whole network. To keep a constant eye on network traffic and to know anything out of ordinary is happening, network security should be supplemented with Intrusion Detection Systems (IDS).

There are two ways intrusion detection works. IDS is Host based, Network-based or the hybrids of the two. Each type of intrusion detection systems has its own merits and legitimate shortcoming. Regardless of the type of systems deployed, it should include the following key features:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

1. Robust
2. Flexibility and Scalability
3. Ease of use

Robust

IDS is expected to run continually in the background without human intervention, it should be fault tolerant, meaning that in the event of a crash or failure the product won't have to be rebuilt or reconfigured. It should remain impervious to attacks!

Flexibility and Scalability

IDS should be configurable and is flexible in response to changes on the network environment, it should also be able of coping with the growth of the network traffic while maintaining fairly high accuracy in performance (scalable).

Ease of use

IDS is to be managed without consuming too much of bandwidth or high overhead from the organization. However, balance should be sought between ease of use and system effectiveness. In a real situation, it requires considerable resources to manage and operate the devices.

Host based Intrusion detection systems (HIDS)

Host based IDS typically reside in the hosts they are monitored, the system agent will records important system file attributes, including hashes of the files. The agent will periodically scans log files for anomalous activity and notifies the system administrator if they have detected suspicious pattern of systems access on the hosts. Another host-based approach monitors all packets as they enter and exit the host, just like a personal firewall.

Host based IDS is popular in that it can tell you if an attack actually happened and if it is significant enough to warrant action. For example the IDS can detect changes in system files and knows if someone tries to install potentially malicious software such as back doors. Back doors are highly specialized programs that let hackers remotely control a server and either steal information from or modify it in a harmful way.

Also, the host is the best location to respond to any attacks. It can also get a fine granularity of information, such as who is accessing what files and when the users log in and out of servers. It is appropriate for protecting an individual computer systems and the information it contains. However it doesn't provide data on the network as a whole. Also the security systems take on considerable processing resource of the host (CPU, RAM and storage).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Network based Intrusion detection systems (NIDS)

As its name suggests, Network based IDS monitor and analyze network traffics on a designated segment. Network based IDS can be categorized as knowledge or behavior based.

For knowledge based NIDS, the systems searches for known 'attack signatures ' that indicates the packets represent an intrusion. Signatures could be based on actual packet contents, and are checked by comparing the bits against known patterns of attacks, for example, attempts to modify systems files. Other known network attacks are protocol based where attackers seek weaknesses of a poorly administered web, file or other servers in a network. These port attack signatures will monitor and identify attempts to connect to network ports associated with service that are often vulnerable. Another protocol signature the systems monitors is the abnormal or illogical TCP/IP packet headers, which is identified as denial-of-service pattern of attacks.

Behavior based NIDS identify attacks by monitoring systems or network traffic patterns and flagging any activity that looks suspicious. The systems capture and analyze packets to define patterns of usage on the network. Once the IDS have constructed statistics or the traffic patterns, it will audit network traffic and analyzing them for any abnormality of the traffic pattern, which is deviated from the normal statistic.

Network based IDS provides real time monitoring and thus provides faster turn around time in detecting and responding to potential attacks. Also it is a system of probes that can be deployed at different points of the network which are deemed critical and is prone for attack so that it can capture those attacks packets at early stage, for example, these monitors can be located at a gateway or firewall between a corporate intranet and the outside internet (known as router based monitoring) or inside the intranet and between the dedicated server farm segment with other sub-segments (known as network based monitoring).

Network based intrusion detection has its faults, for knowledge based network intrusion detection systems, the systems are reliable and generate few false positives, but their strength relies upon the quality, comprehensiveness, and timeliness of the attack signature housed in the IDS's search engine. Poorly defined signature can cause false positives, good packets are labeled as bad packets and transmission could be interrupted. Behavior based network intrusion detection systems often trigger false alarms – false positives.

In addition, this type of intrusion detection is unable to stop encrypted packets of system attack from 'inside' the intranet. If the attacker is logged in to the computer being attacked, no information of the attack would travel the network, and the attack would go unrecognized.

Hybrids IDS

To overcome the limitations of purely host- or network- based IDS, and to combine the strength of both systems, vendors are creating hybrid systems that allow user to mix and match Host based and network based system, as well as signature based and statistical-anomaly based strategies.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

No size fits all

The IDSes available today are far from perfect, they fall short in either of these three keys areas: Robustness, flexibility, scalability and ease of use. According to the latest survey by Information Security (August, 2001 www.Infosecuritymag.com) where more than 300 info security professionals were asked about their experience with IDS products, the response showed most users expect something more from their IDS:

Importance of IDS to the security infrastructure

> Almost two-thirds of respondents said their IDS is "very important" to their security Infrastructure, while another 35 percent said it is "somewhat important." [3]

Confident on IDS to protect the systems

> Nearly one-fifth of respondents said they were either "not at all confident" or "not very confident" that their IDS is protecting their mission-critical systems from cyber attack. [3]

Most desire improvement on the IDS

> Almost half of the respondents in the poll said they'd like to receive more intelligent attack analysis--specifically, the ability to separate serious attacks from nuisance attacks. Another 23 percent of respondents said they'd like to reduce the number of false positives without sacrificing effectiveness. [3]

New Directions

The IDS technologies are still evolving. While some IDS software vendors continue to refine their products' scanning engine beef up their signature databases and expand their data-collection and analysis capabilities. Other vendors are taking new approaches to solving oft-cited problems. [3]

There are many new developments and new directions in the intrusion detection, three of which are briefly described:

Meta-IDS

"Meta-IDS" technologies allows single security console to accept from and communicate with all deployed devices that are from different vendors. This will ease the burden of tracking, reviewing and analyzing data from handful of IDSes on a busy network. This will be possible with the effort of The intrusion Detection Exchange Format working group (IDWG) of the IETF which is currently working on standards that will unify the IDS framework of protocols and data formats so the IDSes speak to each other, as well as to security console.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

IDS appliances

While the traditional IDS are mainly software based, it lack the "scalability", especially when network architectures get more complex, as traffic speeds increase and attacks are more frequent and sophisticated, the common complaints are inefficiency and false positives to this software based IDS.

IDS appliances offers the convenience of pre configured security application in a 'black box' that are tailor made to plug 'n' play in networks of all shapes and sizes. IDS appliances also promise increased processing power (accuracy, speed) and more robust remote management capabilities that are generally lacking in the software based IDS.

IDS-In-Depth

This type of IDS appliance utilize application-layer technologies to filter potential attack traffic to downstream IDSes that it works in tandem with on dedicated network segments. It captures flows of traffic, performs preliminary attack detection and filtering, and distributes a copy of the traffic to a downstream third-party IDS, which can be fine-tuned to analyze the traffic for specific attacks. The tradeoff is that the device performs only initial attack filtering, leaving the real analysis for the downstream IDS.

As the IDS are intended to sit between the Internet and the firewall to protect the network, it also provides DOS/DDOS attack mitigation and Firewall load balancing. Besides these functionalities, the IDS are also equipped with Securewatch data collection software for intrusion analysis and attack forensics.

Conclusion

Attackers are constantly dreaming up news ways to infiltrate the enterprise's network, and although firewalls and other security systems are vital, they can't see everything. So, instead of locking the doors and hoping for the best, organization can add ever-vigilant eyes and ears to their network security with intrusion detection.

Organization cannot alone solve information security problem by adding technology and ignoring the fact that they are not monitoring for security incidents. Effective information protection is attained through a combined effort of policy, process and technology that provides protection, detection, and recovery measures.

It is important for an organization to have a clear procedures and intrusion response policies for dealing with intrusion. We want to keep intruders out, but we also want to discover and locate them when they succeed.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References:

1. Anita Karve, "Can Intrusion Detection Keep an Eye on Your Network's Security?" Network Magazine 04/01/99 (1999) URL**:** http://www.networkmagazine.com/article/NMG20000508S0022 (20 Aug, 2001)

2. Robert, Winkler. "Intrusion Detection Systems" SANS Institute, December 9, 2000 (2000) URL: http://www.sans.org/infosecFAQ/intrusion/systems.htm (10 Aug, 2001)

3. Andrew L. Briney, "New Directions In Intrusion Detection" Information Security August 2001 (2001): 48 – 60 URL: http://www.infosecuritymag.com/articles/august01/cover.shtml (20 Aug 2001)

4. Andrew L. Briney, "Zen and the Art of Intrusion Detection" ComputerWorld, Mar/12/2001 (2001) URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO58458,00.html

5. Pete Loshin, "Intrusion Detection" ComputerWorld, Apr/16/2001 (2001) URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59611,00.html

© SANS Institute 2001, Author retains full rights

Last Updated: March 11th, 2014

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Northern Virginia 2014	Reston, VAUS	Mar 17, 2014 - Mar 22, 2014	Live Event
Secure Canberra 2014	Canberra, AU	Mar 17, 2014 - Mar 22, 2014	Live Event
ICS 410@ Sydney 2014	Sydney, AU	Mar 24, 2014 - Mar 28, 2014	Live Event
SANS Munich 2014	Munich, DE	Mar 31, 2014 - Apr 05, 2014	Live Event
SANS 2014	Orlando, FLUS	Apr 05, 2014 - Apr 14, 2014	Live Event
FOR518 Mac Forensic Analysis	Vienna, VAUS	Apr 22, 2014 - Apr 27, 2014	Live Event
SANS Abu Dhabi 2014	Abu Dhabi, AE	Apr 26, 2014 - May 04, 2014	Live Event
US Cyber Crime Conference	Leesburg, VAUS	Apr 27, 2014 - Apr 28, 2014	Live Event
SANS Austin 2014	Austin, TXUS	Apr 28, 2014 - May 03, 2014	Live Event
Security Leadership Summit	Boston, MAUS	Apr 29, 2014 - May 07, 2014	Live Event
SANS Security West 2014	San Diego, CAUS	May 08, 2014 - May 17, 2014	Live Event
SANS Secure Europe 2014	Amsterdam, NL	May 10, 2014 - May 24, 2014	Live Event
SANS Melbourne 2014	Melbourne, AU	May 12, 2014 - May 17, 2014	Live Event
SANS ICS410 London 2014	London, GB	May 12, 2014 - May 16, 2014	Live Event
SANS Malaysia @MCMC 2014	Cyberjaya, MY	May 12, 2014 - May 24, 2014	Live Event
SANS Bahrain May 2014	Manama, BH	May 17, 2014 - May 22, 2014	Live Event
SANS Delhi 2014	New Delhi, IN	May 19, 2014 - May 31, 2014	Live Event
SANS Secure Thailand	Bangkok, TH	May 26, 2014 - May 31, 2014	Live Event
Digital Forensics & Incident Response Summit	Austin, TXUS	Jun 03, 2014 - Jun 10, 2014	Live Event
SANS Rocky Mountain 2014	Denver, COUS	Jun 09, 2014 - Jun 14, 2014	Live Event
9th Annual ICS Security Summit	OnlineFLUS	Mar 12, 2014 - Mar 23, 2014	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced