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.

Distributed Intrusion Detection Systems: An Introduction and Review

Intrusion Detection Systems have undergone rapid growth in power, scope and complexity in their short history. Most IDS share a similar underlying structure: agents reporting detections to a management system. Recent increases in malicious network activity worldwide have precipitated the need for IDS with global scope. These distributed Intrusion Detection Systems multiply the power of a single IDS by marrying an attack correlation engine with an database of events obtained from a large number of geographically dispers...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

Distributed Intrusion Detection Systems: An Introduction and Review

Royce Robbins
GSEC Practical Assignment, version 1.4b, Option 1.
January 2, 2002

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

Intrusion Detection Systems have undergone rapid growth in power, scope and complexity in their short history. Most IDS share a similar underlying structure: agents reporting detections to a management system. Recent increases in malicious network activity worldwide have precipitated the need for IDS with global scope. These distributed Intrusion Detection Systems multiply the power of a single IDS by marrying an attack correlation engine with an database of events obtained from a large number of geographically dispersed agents. This provides a global view of existing and emerging attacks patterns and security events, allowing rapid notification and facilitating development of countermeasures.

A number of dIDS with global scope have been active for several years, and are rapidly evolving as the nature of the threats change. Five of these are discussed and compared with each other in terms of focus, data source, notification tools, available agents, statistical reporting tools and linkage to security and vulnerability information.

Intrusion Detection Systems

IDS Defined

Intrusion detection is the process of identifying computing or network activity that is malicious or unauthorized. Most all Intrusion Detection Systems (IDS) have a similar structure and component set. This consists of a sensor (or **agent**) that monitors one or more **data sources**, applies some type of **detection algorithm**, and then initiates zero or more **responses**. Usually there is a **management system** that provides for monitoring, configuration and analysis of intrusion data[1].

Evolution of IDS

The first IDS were host-based, and looked at system operating logs performing simple pattern matches against a small set of signatures. This approach quickly expanded to systems that looked at network traffic, initially also for simple patterns. As IDS gained a level of protocol-awareness, they were able to look for certain single packet traffic types known to be malicious, examining the source and destination IP addresses, along with source and destination ports. Further sophistication brought an awareness of network sessions and the ability to examine dialogs between systems for multi-packet activity. More recent IDS can examine and respond to entire conversations between hosts, using knowledge of protocols and network sessions to analyze traffic for malicious activity based on how that traffic would appear at the destination-a task often requiring specialized network drivers to operate at full wire-speed,[1] (For a good discussion of the evolution and genealogy of IDS, see article by Inella[2].) The emerging class of IDS take this one step further by combining log analysis, along with information from other IDS and anti-virus software to correlate events in an effort to identify and respond to intrusions in real time.[3]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Relation of IDS to dIDS

From the above, it is clear that as IDS grow in function and evolve in power, they also evolve in complexity. Agents of each new generation of IDS use agents of the previous generation as data sources, applying ever more sophisticated detection algorithms to determine ever more targeted responses. Often, one or more IDS and management system(s) may be deployed by an organization within its own network, with little regard to their neighbors or the global Internet. Just as all individual networks and intranets connect to form "The Internet", so can information from stand-alone internal and perimeter host- and network-based intrusion detection systems be combined to create a distributed Intrusion Detection System (dIDS).

Motivation for dIDS

Current IDS technology is increasingly unable to protect the global information infrastructure due to several problems: 1) the existence of single intruder attacks that cannot be detected based on the observations of only a single site, 2) coordinated attacks involving multiple attackers that require global scope for assessment, 3) normal variations in system behavior and changes in attack behavior that cause false detection and identification, 4) detection of attack intention and trending is needed for prevention[4], 5) advances in automated and autonomous attacks, i.e. rapidly spreading worms, require rapid assessment and mitigation, and 6) the sheer volume of attack notifications received by ISPs and host owners can become overwhelming. If aggregated attack details are provided to the responsible party, the likelihood of a positive response increases. The 2002 InforWorld IT Security Survey indicates that "there are too many successful attacks because a large contingent of the IT community … refuses to share its hard-won security knowledge. If IT leaders banded together, they could develop a consensus on which attacks are worth preventing and which countermeasures work best."[5]

Distributed Intrusion Detection Systems

dIDS Defined

A distributed Intrusion Detection System (dIDS), therefore, is an effort to share this hard-won knowledge. A dIDS can be defined as:

> "multiple Intrusion Detection Systems (IDS) [spread] over a large network, all of which communicate with each other, or with a central server that facilitates advanced network monitoring, incident analysis, and instant attack data."[6]

The "large network" in the present discussion is presumed to be the global Internet, not merely a network or intranet of any single organization. A dIDS then, can be considered a "Meta-IDS", collecting data from widely dispersed IDS, correlating attacks and providing information for determining patterns and mitigation strategies across the Internet as a whole. As a "Meta-IDS", the components of the dIDS are familiar, although the roles expand and contract compared to a purely local IDS.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Agents

In a dIDS, the agent might be a simple personal firewall on a home user's dialup machine, a commercial IDS on a Fortune 500 company's network perimeter, or a host-based IDS on a network inside an educational institution. For most agents, participation in a global dIDS is a secondary function, and is subservient to the function as an IDS within the organization.

Data sources

Depending on where the agent resides, the IDS agent may be reporting on network traffic internal to an organization, at the perimeter, or both. For a dIDS, both locations can be useful as it is known that certain malicious software behaves differently when inside private network space (i.e. behind a NAT router) versus when in public space[7]. When the agent is located inside an organization, it can gather useful information about attacks that might have penetrated the perimeter, attacks originating inside, or hosts cooperating in outbound attacks.

Detection algorithm

In a dIDS, the detection algorithms are likewise as varied as the agents. Since the agents are generally deployed to the benefit of the organization, they will be tuned to those needs, which by definition, will vary widely. Thus, there is no single "detection algorithm" used or required by most dIDS.

Responses

In a dIDS of global scope, each agent contributes minimal data: often only the source and destination address, source and destination port, protocol, agent type, and a timestamp. The agent may even submit its data anonymously after scrubbing destination addresses. Generally, the agent provides little response to an incident beyond this simple data. Instead, it is the management system at the heart of the dIDS that provides some kind of response, usually in the form of notification to the owners of attacking sources.

Central Analysis Server

In a dIDS, the management system or Central Analysis Server (CAS) is the heart and soul of the system. "Management system" is somewhat of a misnomer as the CAS usually has little control over the autonomous and likely voluntary agents. The CAS commonly consists of a database, web server and reporting engine.[6] Its function is to collect responses from the agents, perform weighting based on agent type, location, number of monitored hosts, etc. to permit attack correlation, data aggregation, statistical analysis, visualization and reporting.

Incident analysis and attack correlation is what a dIDS is all about. By aggregating data from multiple geographically dispersed agents, an analyst using a dIDS can examine attacks across multiple network segments in many different ways. Some examples of data aggregation and uses (adapted from Einwechter[6]) are:

- Aggregation by source IP: can follow an attack across multiple networks, from start to finish, watching how an attack progresses.
- Aggregation by destination port: permits looking for new trends in attack types

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

and methods--indeed several recent worm attacks were first identified by dIDS this way[8,9,10].

- Aggregation by agent ID: can watch attacks targeted to a specific network or subnet, by industry, country or other criteria; can determine if attacks might be coordinated by several attackers, etc.
- Aggregation by date/time: can determine new attack patterns, or attacks by a particular worm or virus for example, that triggers at a certain time.
- Aggregation by protocol: allows discovery of new attacks in particular protocols or protocol use where it shouldn't be (i.e. use of ICMP for file transfer).

In addition to the results of its analyses, a dIDS may provide certain services to the contributing agents. These services are usually the reason many organizations choose to contribute information from their agents to dIDS. Common services offered include:

- Client software: This is the software that enables an IDS, firewall, router, etc. to act as an agent within the dIDS. It provides for the upload (often encrypted and secure) of data about intrusions and attacks to the CAS. Most dIDS implementations support a wide range of agents, from appliance devices to public domain IDS to personal firewalls.
- Private web site: Provided by the CAS for use by the agent owner to examine results of aggregated analysis, including most recent attacks on the agent, attacks shared by the agent with other agents, type of attack, severity and ports used. Often full details of a specific attack are available, along with information about mitigation and any response made by the dIDS.
- Incident reporting: Once a source of attacks is determined from analysis of aggregated data, the CAS may send an automated response to the owner of the affected host/domain documenting details of the attack. Details of the complaint, escalation and any response from the ISP may be available on the private web site for the agents. Rapid response to an attack can help mitigate an attack, and is especially critical in fast-spreading attacks (such as worms).
- Summary database/knowledgebase: Maintained by the owner/operator of the CAS, usually links to and information on known attacks and Computer Emergency Response Teams (CERTs), charting and visualization tools for top attacks, top ports attacked, top attacking IP addresses, ISPs, top destinations, an historical timeline by protocol, date, etc., as well as DNS, WHOIS and other tools. The capabilities vary widely among dIDS.
- Security management services: Much of the work of the CAS requires intensive human analysis. These value-added analyses may then be resold to clients of commercial security management services, or provided to the subscribers of the supporting organization, i.e. US or foreign CERTs or SANS, but may or may not be made publicly available.

Implementations of dIDS

Several examples of dIDS exist. The remainder of this paper will describe and compare several of these dIDS of global scope that use voluntary agents for acquisition

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

of attack data.

Internet Storm Center

The Internet Storm Center (http://isc.incidents.org) (ISC) is probably the best known of the global dIDS, claiming "several millions of records added to our database daily."[11] The primary focus of the ISC is to provide a global Internet security status so that individuals and security personnel can be better informed of existing and approaching security "storms". It is a free public service to the Internet community whose goal is to detect new attacks and attackers faster, and provide authoritative information on new and existing attacks around the globe. It is supported by the SANS Institute, and has relationships with US Government Internet monitoring and analysis agencies, government CERTs in the US and around the world, ISPs and other commercial organizations with managed security services, large corporations and universities, as well as other dIDS[8].

The ISC "About" page[8] offers an excellent analogy of a dIDS to a weather reporting system--where changes in local conditions contribute to global patterns of weather that are only readily apparent to a central analysis system. The "Global Analysis and Coordination Center" sits at the top of a hierarchy of "regional and industry specific Internet Storm Center Analysis and Coordination Centers" to which a large number of IDS sensors/agents report. When incidents of interest arise, a team of intrusion detection analysts is convened to determine the severity of the threat, the appropriate response, and to take action.

The ISC provides client software through DShield.org (see below) for a very wide range of agents. Individuals are not able to become agents of ISC directly, but rather can register with DShield.org, which then submits reports to the ISC. However, the ISC maintains very extensive information on their web site about the top ten attacks and trends, target port activity, historical information and trends, current viruses and worms, plus links to a huge amount of other security related material. The ISC also publishes a "block list" of the top 20 attacking networks, has excellent trend graphics, numerous customizable visualization tools, and a reporting feature that permits drilling down from network through subnet to host to obtain contact information where available. The ISC provides automatic notification to ISPs of attacking hosts (termed its "FightBack facility"), but does not provide a mechanism for users to track ISP responses or escalation.

DShield.org

DShield.org (http://www.dshield.org) is a straight forward dIDS. Started as a volunteer effort focused on providing an easy way to share information about attacks to help protect oneself and others, it now also receives support from SANS, and is one of the sources of data for the ISC. As a free service begun in November of 2000, "it has grown to be a dominating attack correlation engine with worldwide coverage"[12] with several million records added per day. DShield focuses on "users of firewalls" as dIDS agents. Client software is available on the site or via link to sources for a very extensive list of firewalls that is constantly being updated, as well as instructions for writing one's own client log parser. Users may run client software to upload reports or upload raw firewall logs manually to a web-based form. Users may register if desired, or reports

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

may be uploaded anonymously. DShield's "FightBack" program sends summary analyses of attacks to the responsible ISP. Only information from registered users will be provided to the ISP, and the submitter will receive a copy of any correspondence. Individual log entries are available to the submitter by specific request only.

DShield has far fewer reports and tools than the ISC, and several of the reports and graphics actually link back to the ISC. The main page has a graphic that provides a geographic distribution of attack sources (indeed, this is the graphic displayed on the main page of the ISC), an animation of the last five days, and a prominent display of "FightBack" responses. The few reports that are available include the top 10 offenders, the top 10 most attacked ports, and a thirty-day history report on a user-selected port. Information about a specific IP address comes from another site, while reports on a specific subnet link back to the ISC. "Block Lists" are available, along with customization scripts for a number of different router/firewalls. One unique feature is the ability to search DShield's database for records based on the source IP, date and source or destination port. DShield's "Links" page, has links to other security web sites, as well as personal firewall information and vendors. DShield also maintains several mailing lists relating to the service.

The paper by Jensen[13] is an excellent resource for configuring a small home-office gateway as a DShield.org agent. This paper provides a step-by-step guide to configuring a LinkSys SOHO router agent to automate collection and reporting of attack data using two different software clients; a freeware and a commercial solution. The author includes an evaluation of the clients, their ease of use, and discusses methods for testing the security of the installation.

MyNetWatchman

MyNetWatchman (http://www.mynetwatchman.com) (mNW) is a free service to individuals and describes itself as a:

- "Security Event Aggregator,
- Centralized, web-based firewall log analyzer,
- Fully automated abuse escalation/management system."[14]

It is a full-fledged dIDS whose primary focus is on notification of owners of attacking or compromised systems. The owner/operator Lawrence Baldwin is enthusiastically evangelical about his message, saying in the mNW vision statement: "in order to protect ourselves, we need to ensure that others are protected. When we discover that someone is obviously exposed, we should let them know and guide them to the information they need to get protected."[15] In the design of this dIDS, Mr. Baldwin followed three principles: "1) minimize effort required to report events, 2) avoid false reports, and 3) provide aggregated attack report to responsible party."[15] The result is a dIDS that is extremely useful and usable by the owners of the approximately 1400 contributing agents. Events from agents are collected and aggregated in near-real time, and identified incidents are reported immediately to the responsible ISP via e-mail. Agent-owners are able to view and track incident status as well as view correspondence from the ISP.

MyNetWatchman provides a number of clients targeted at personal firewalls and a honey-pot package, as well as a web-based interface for uploading attack data.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Registration of each agent is required. Compared to the DShield dIDS, the number of available clients is somewhat smaller, but the mNW clients are more automatic and simpler to use. In keeping with mNW's agent-centric philosophy, there are numerous reports on incident status ("hot", current, escalated, re-escalated, closed, cleaned) both for all events/incidents identified by mNW and for each agent (available on a private page). Reports are also available by top port target (daily and weekly), top port trends (daily and weekly) and incidents by source provider: all, high, medium and low volume. By drilling down on a specific target (port, top-level domain, incident), it is possible to obtain information on the owner of the attacking host, attack description, and listing of other agents similarly attacked and hence who contributed to the determination/discovery of the incident. MNW provides a customized knowledgebase that describes many common attacks and mitigation steps, as well as a number of custom analyses of specific incidents. Links to a few other security sites, DSL information and press clippings featuring mNW round out the information available. The site has several active newsgroups that discuss mNW, its administration, incidents, and general intrusion detection questions.

The paper by Zuver[16] further discusses the capabilities of myNetWatchman and compares it to the ISC and DShield.

DeScan.net

DeScan.net (http://descan.net) is a dIDS with the very limited focus of looking only for malicious TCP SYN scans. DeScan.net is a for-profit company that requires registration of its Linux resident agent to upload log data and intends to sell services to ISPs and backbone carriers to support its agent. Agents log only the source and destination address and destination port of all incoming requests, then periodically upload logs to be summarized and examined for malicious scanning patterns. When a scan is found, an e-mail alert is sent to the party responsible for the scanning address. Agent source-code has been recently posted, and support for non-Linux platforms is in the works. A very recent arrival, DeScan.net identified the MS SQLSnake worm (a.k.a. Spida virus) activity over three weeks before the media first reported the virus outbreak, while the dIDS was still in Alpha-testing[10]. DeScan.net presently has less than 300 active agents[17].

DeScan.net has minimal reporting capability and very little information available on its site. A "Weekly Internet Situation Report" lists the top five attacked ports and displays a top five port trend plot. A report of the most recent incidents provides date, time and e-mail for contact; drilling down lists the source address and the last two octets of the scanned addresses. A report of the top ten scanning IP addresses and a brief "Threat Analysis" page with links to selected CERT incident announcements are also available. A facility to search for a specific IP address or address range within the database of known scanners rounds out the information available. DeScan.net does send e-mail alerts of scanning activity to registered users at user specified frequency, but has no mechanism for tracking responses or escalations. There are no links to other security information resources, no description of the targeted ports and no details provided on site of what constitutes a "malicious scan".

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Symantec DeepSight™

Symantec DeepSight™ (http://enterprisesecurity.symantec.com) is part of Symantec's enterprise managed security services, early warning solutions. Developed by Security Focus and acquired by Symantec in August of 2002, DeepSight is a dIDS with over 16,000 "data partners" (contributing one or more agents) distributed in over 179 countries worldwide.[18] The DeepSight system focuses on providing customized threat information to its customers. Not just highly detailed current and trending attack data, statistical analyses and attacker notification, but extensive information about attacks, countermeasures, patches, workarounds and IDS signature updates. DeepSight provides "actionable security intelligence", including alerts and vulnerabilities, tailored to each customer's specific environment. To do this, the DeepSight system integrates an enhanced vulnerabilities knowledgebase (with extensive links to CERT, Bugtraq and other security information resources) with an attack correlation engine, event database, web server and reporting engine. Symantec repackages information from this dIDS and provides it to customers in three different services: DeepSight Alert Services; Analyzer; and the Threat Management System.

At the core of the DeepSight system are the registered "data partners" who contribute attack and intrusion information from their own firewalls and/or IDS using the client software agent DeepSight Extractor. This software can extract and upload logs from numerous personal firewalls, firewall appliances and most of the leading IDS packages and appliances, uploading from each device individually or from the partner's local dIDS management system. In return for uploading data, each partner receives access to the web-based DeepSight Analyzer for incident tracking, analysis and management of threats against their own network. They also receive discounted pricing on the DeepSight Threat Management System which provides early warning of attacks, customizable alerts, more detailed analysis, countermeasures and a host of other security information.

The types of reports and analyses available with the DeepSight system only begin with the basic reports available from the other dIDS discussed above. Additional reports and analyses include extremely detailed information on a specific attack, including vulnerabilities listed by OS, package and version, what specific mitigation steps to take, and even sample exploits for testing. DeepSight tracks the different types of attacks used against a partner's site, and facilitates correlation and communication with other sites receiving the same attacks. Partners can also use DeepSight to correlate information from their own internal IDS agents. Reports are available online and are fully customizable by user selectable criteria; plus alerts can be customized to be sent to the user via e-mail, SMS, pager, FAX, etc. DeepSight provides tools to assist the user in generating attacker notifications, escalation and tracking responses if desired, but this function is not automatically performed by this dIDS. Being a commercial venture, DeepSight has a large cadre of security analysts available 24/7 to partners as well as extensive online help and support which goes far beyond e-mail lists and newsgroups.

Comparison of Implementations

The following two tables compare selected characteristics of the five dIDS implementations described above. Table 1 summarizes the dIDS by primary focus or

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

design objective, sources of data used, ability to do anonymous uploads and availability of attacker notification and tracking tools. Each dIDS has strengths and weaknesses from the standpoint of the owner of a contributing agent, and these should be evaluated prior to choosing to participate. Some users may be more interested in obtaining security information and early warnings of attacks for their particular situation, while others may be more interested in simply contributing to the Greater Good of the Internet community.

Table 1
Selected Characteristics of Five dIDS

	Primary Focus	**Data Sources**	**Incident reporting tools**	**Registration required to upload**
Internet Storm Center	Provide global Internet security status, warnings and information about security "storms".	US and global CERTs, ISPs, managed security services, other dIDS, universities, corporations.	Automatic. No feedback to attacked agent.	N/A
DShield.org	Share information about attacks to better protect oneself and others.	Individual and corporate firewalls.	Automatic. Agent receives copies of correspondence, can view ISP responses.	Optional
myNetWatchman	Notify owners of attacking or compromised systems.	Individual and corporate firewalls.	Automatic. Extensive tracking of notification and escalation.	Yes
DeScan.net	Monitor Internet for malicious TCP SYN scans.	Individual and corporate Linux hosts.	Automatic. Agent receives copies of correspondence.	Yes
Symantec DeepSight™	Provide customized threat information to customers.	Individual and corporate firewalls and IDS, on internal nets and Internet.	Manual. Online tools for notification tracking and escalation.	Yes

Table 2 lists the supported agents and their client software. Client lists were obtained from the relevant page on the dIDS web site. Several log daemons listed (Kiwi

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Syslog Daemon, Link Logger, RouterLog, WallWatcher) also support additional router/firewall/gateway devices that are not specifically listed. The choice of dIDS in which to participate may also be heavily influenced by the agent owned and what client software is available for it.

Table 2
Supported Agents for Five dIDS

Internet Storm Center	None directly. Individuals participate through DShield.org. ISPs and others may participate through special arrangement.
DShield.org	Web upload. Instructions to build-your-own agent. Asante FriendlyNET, BlackIce Defender, Checkpoint Firewall-1, Cisco IOS, Cisco PIX, Compatible Systems Microrouter, D-Link, Gauntlet firewall, Gnatbox firewall, IPCop Firewall, ipfw, ipchains, iptables, Kerio (formally Tiny) Firewall Syslog, Kerio Personal Firewall, Kerio Software WinRoute Pro, Kiwi Syslog Daemon, LaBrea, Link Logger, Linksys routers, McAfee Firewall, Microsoft ISA, Norton Personal Firewall, Open BSD Packet Filter, Prestige/Netgear, Psionic Portsentry, RouterLog, SMC Barricade, Smoothwall , Snort and Snort Portscan, SonicWall, Sygate Personal Firewall, Tiny Personal Firewall 4.0, Trend Micro PC-Cillin, US Robotics 8000 router, Vicom Internet Gateway, VisNetic (formerlly Ambra) Firewall, Wallwatcher, WatchGuard , Windows XP Internet Connection Firewall (ICF), ZoneAlarm, ZyXel ZyWall
myNetWatchman	Web upload. BlackICE Defender, Cisco PIX, Cisco IOS, Dlink DI-704, ipchains, ipfw, iptables, LaBrea TarPit, Linksys Router, Kiwi Syslog Daemon, WallWatcher, Microsoft XP ICF, Netgear Cable/DSL Router, Portsentry, SMC Barricade, Snort, Sonic Wall, Zone Alarm
DeScan.net	Linux only. Code is available to build-your-own agent .
Symantec DeepSight™	Black Ice, Checkpoint Firewall-1, Cisco IOS, Cisco PIX, Cisco Secure IDS (Netranger), Enterasys Dragon, ipchains, ipfw, NetProwler, NetScreen, Real Secure, Snort & Snort Portscan, ZoneAlarm

Conclusion

Intrusion Detection Systems have grown in power and scope rapidly in their short history. The occasional odd bit of anomalous behavior on an individual network may not be meaningful, but if that same odd bit shows up on multiple networks around the globe, there may be something not so anomalous and probably not so benign at work.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Being able to correlate events from the IDS of many different networks and declare that a security incident is in progress is what distributed Intrusion Detection Systems are all about.

Several dIDS are currently available that individuals and corporations may benefit from and contribute to. Those described range from a minimalist system sending nasty-grams to TCP SYN scanners, to a full-blown, managed security system providing warnings and detailed descriptions about the latest attack *du jour* direct to your pager. As attacks become more sophisticated, more coordinated and more distributed, the strength that dIDS can bring to attack discovery, countermeasures and resolution will continue increase in the future. Using an IDS on your own net is good, participating in and contributing to a dIDS of global scope is the next logical step. Sharing that hard-won security knowledge is the best way to make the 'Net safer for everyone. It just makes your "defense in depth" that much deeper.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

[1] ISS Security Systems. "The Evolution of Intrusion Detection Technology". 29 Aug 2001. URL: http://documents.iss.net/whitepapers/TheEvolutionofIntrusionDetectionTechnology.pdf (10 Oct 2002).

[2] Inella, Paul. "The Evolution of Intrusion Detection Systems". 16 Nov 2001. URL: http://online.securityfocus.com/infocus/1514 (27 Sep 2002).

[3] Sturdevant, Cameron. "The Emerging Class of Security Tools". eWEEK. 6 Dec 2002. URL: http://www.eweek.com/print_article/0,3668,a=34499,00.asp (9 Dec 2002).

[4] "GIANT - Global Intrusion Assessment Through Distributed Decision Making". URL: http://project.anr.mcnc.org/GIANT/GIANT.html (27 Oct 2002).

[5] Yager, Tom. "Security Part I: Strategies". 16 Aug 2002. URL: http://www.infoworld.com/articles/fe/xml/02/08/19/020819feintro.xml (7 Sep 2002).

[6] Einwechter, Nathan. "An Introduction To Distributed Intrusion Detection Systems". 8 Jan 2001. URL: http://online.securityfocus.com/infocus/1532 (28 Dec 2002).

[7] Baldwin, Lawrence. "Worm immortal - Why Code Red and Nimda won't die". 31 Mar 2002. URL: http://www.mynetwatchman.com/kb/security/articles/persist.htm (29 Dec 2002).

[8] SANS Institute. "Internet Storm Center: About". URL: http://isc.incidents.org/about.html (28 Oct 2002)

[9] Ullrich, Johannes B. "[DShield] 27374/TCP Probes". 25 Jun 2001. URL: http://www1.DShield.org/pipermail/DShield/2001-June/000572.html (29 Dec 2002).

[10] Wolf, Tom. Press Release. 2 Sep 2002. URL: http://www.descan.net/spida.html (7 Sep 2002).

[11] SANS Institute. "Internet Storm Center: Trends". URL: http://isc.incidents.org/trends.html (30 Dec 2002).

[12] DShield.org. "DShield - About". 12 Dec 2001. URL: http://www.DShield.org/about.html (28 Oct 2002).

[13] Jensen, Sydney. "Doing My Part - Sending Data to the Internet Storm Center". 1 Jul 2002. URL: http://rr.sans.org/intrustion/stormcenter.php (27 Oct 2002).

[14] Baldwin, Lawrence. "myNetWatchman - FAQ". 9 May 2001. URL: http://www.mynetwatchman.com/myNetwatchman/faq.htm (28 Oct 2002).

[15] Baldwin, Lawrence, "myNetWatcman - Vision". URL: http://www.mynetwatchman.com/vision.htm (28 Oct 2002).

[16] Zuver, Robert. "A Thousand Heads Are Better Than One - The Present and Future of Distributed Intrusion Detection". 30 Apr 2002. URL: http://rr.sans.org/intrusion/thousand.php (26 Sep 2002).

[17] DeScan.net. "Descan Situation Report - Week of 16 December - 22 December, 2002". 23 Dec 2002. URL: http://descan.net/sitrep.html (31 Dec 2002).

[18] Symantec Corporation. "Symantec DeepSight™ Threat Management System". URL: "http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=158 (30 Dec 2002).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: February 14th, 2016

Upcoming SANS Training

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

SANS Northern Virginia - McLean 2016	McLean, VAUS	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS Munich Winter 2016	Munich, DE	Feb 15, 2016 - Feb 20, 2016	Live Event
ICS Security Summit & Training - Orlando	Orlando, FLUS	Feb 16, 2016 - Feb 23, 2016	Live Event
SANS Southern California - Anaheim 2016	Anaheim, CAUS	Feb 22, 2016 - Feb 27, 2016	Live Event
SANS Secure India 2016	Bangalore, IN	Feb 22, 2016 - Mar 05, 2016	Live Event
RSA Conference 2016	San Francisco, CAUS	Feb 28, 2016 - Feb 29, 2016	Live Event
SANS London Spring 2016	London, GB	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Philadelphia 2016	Philadelphia, PAUS	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Abu Dhabi 2016	Abu Dhabi, AE	Mar 05, 2016 - Mar 10, 2016	Live Event
SANS 2016	Orlando, FLUS	Mar 12, 2016 - Mar 21, 2016	Live Event
ICS410 Dubai 2016	Dubai, AE	Mar 13, 2016 - Mar 17, 2016	Live Event
SANS Secure Singapore 2016	Singapore, SG	Mar 28, 2016 - Apr 09, 2016	Live Event
SANS Secure Europe 2016	Amsterdam, NL	Apr 04, 2016 - Apr 16, 2016	Live Event
SANS Northern Virginia - Reston 2016	Reston, VAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
SANS Atlanta 2016	Atlanta, GAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
Threat Hunting and Incident Response Summit	New Orleans, LAUS	Apr 12, 2016 - Apr 19, 2016	Live Event
ICS Amsterdam 2016	Amsterdam, NL	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Secure Canberra 2016	Canberra, AU	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Pen Test Austin	Austin, TXUS	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Copenhagen 2016	Copenhagen, DK	Apr 25, 2016 - Apr 30, 2016	Live Event
SANS Security West 2016	San Diego, CAUS	Apr 29, 2016 - May 06, 2016	Live Event
SANS Baltimore Spring 2016	Baltimore, MDUS	May 09, 2016 - May 14, 2016	Live Event
SANS Houston 2016	Houston, TXUS	May 09, 2016 - May 14, 2016	Live Event
SANS Stockholm 2016	Stockholm, SE	May 09, 2016 - May 14, 2016	Live Event
SANS Prague 2016	Prague, CZ	May 09, 2016 - May 14, 2016	Live Event
SANS Secure Japan 2016	OnlineJP	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced