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.

Network IDS: To Tailor, or Not to Tailor

Intrusion Detection Systems (IDS) identify attacks on a company's resources. As security requirements grow more demanding, and resources more scarce, IDS vendors have attempted several approaches for increasing the amount of throughput an IDS can handle. One of those solutions is trimming the amount of resources utilized through decreasing the amount of rule sets or patterns searched for. This trimming of patterns, known as tailoring, is the greatest question mark on Network Signature-Based Intrusion Detection Systems....

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.
watchfire

GIAC Security Essentials
v1.3

Intrusion Detection Systems

Network IDS: To Tailor, or Not to Tailor

Jon-Michael C. Brook
March 6, 2002

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Table Of Contents

Network IDS:

To Tailor or Not to Tailor

Pros and Cons of IDS Tailoring 1

Introduction to Intrusion Detection 2

- IDS Definition 2
- Types of Resources 2
- Network 2
- CPU 3
- Storage 3
- Scalability 3
- Analyst 4

Tailoring 5

- Advantages 5
- Limiting resource consumption 5
- Review of the Signatures 6
- Disadvantages 6
- Delayed Release 6
- Smaller Peer Group for Review 6
- Misconfiguration 7
- Reconnaissance 7
- Analyst Mistakes 8

Tailoring in "Off-The-Shelf" IDS Products 9

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Navy's Shadow 9

Symantec's NetProwler 10

SecureNet 10

Real Secure 10

Cisco's Secure Intrusion Detection System 11

Overall 11

Conclusions 12

Internet References 13

Additional Sources 14

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Abstract

Network IDS:

To Tailor or Not to Tailor

Pros and Cons of IDS Tailoring

Intrusion Detection Systems (IDS) identify attacks on a company's resources. These IDS devices watch points in the company's network infrastructure (network intrusion detection), or operate on a specific company asset (host based intrusion detection). These products detect attacks by comparing incoming activity to rule sets and patterns in search of hostile activity (signature based) or by comparing incoming activity against a known baseline in search of out-of-the-ordinary usage (anomaly based). Both signature and anomaly based intrusion detection are resource intensive. IDS resources include CPU, Network interface card (NIC), Memory (RAM), Storage (Hard Drive, SANS, etc), and, an overlooked end analyst. This user is often the most under-appreciated component of the IDS design as well as the most important. The analyst must find details and make correlations between multiple information sources.

As security requirements grow more demanding, and resources more scarce, IDS vendors have attempted several approaches for increasing the amount of throughput an IDS can handle. One of those solutions is trimming the amount of resources utilized through decreasing the amount of rule sets or patterns searched for. In doing so, IDS vendors can increase the total network throughput their IDS systems handle. This trimming of patterns, known as tailoring, is the greatest question mark on Network Signature-Based Intrusion Detection Systems. Products such as ISS's Real Secure, Intrusion.com's Secure Net, Cisco's Secure IDS (formerly Net Ranger), Symantec's NetProwler, the Navy's Shadow project, and the open source community's Snort can all limit system resource utilization through rule-based tailoring. The following discussion centers on the benefits and detractors of rule-based Intrusion Detection Tailoring, and how, overall, it is best to leave tailoring for Network IDS systems to the product vendors. If tailoring is required due to legacy product selection or unexpected network growth, be forewarned of the consequences. When this tailoring occurs, make sure a process is set in place to review as completely as possible any changes that need to be made.

JON-MICHAEL C. BROOK 2/6/2003

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Chapter 1

Network IDS:

To Tailor or Not to Tailor

Introduction to Intrusion Detection

IDS Definition

Intrusion Detection Systems (IDS) identify attacks on a company's resources. Network IDSes watch points within the company's network infrastructure, whereas host based IDSes operate on a specific company asset such as servers and workstations. These products detect attacks by comparing incoming activity to rule sets and patterns in search of hostile activity (signature-based) or by comparing incoming activity against a known baseline in search of out-of-the-ordinary usage (anomaly-based). Both signature and anomaly based IDSes are resource intensive. A process called tailoring is often incorporated into IDSes to limit the total resources used.

Types of Resources

IDS resources include Network interface card (NIC), processor time (CPU), Storage (Hard Drive, SANS, etc), and Memory (RAM). The product vendor chosen for an IDS package determines which resources are most important to its operation. Some products load all signatures into memory; others store all packets on the local hard drive. The product vendor's implementation of the IDS places more emphasis on specific resources. The following paragraphs discuss some of these issues.

Network

All IDSes have high network interface requirements. Since most IDSes' promiscuous mode NICs are expected to keep wire speed, the network interface is vital to the success of an IDS. Lee Sutterfield, a cofounder and Executive Vice President for the WheelGroup Corporation, when asked about problems with IDS in the Computer Security Institute's Roundtable stated, "The other issue is performance. Most IDS products can't even keep up with 10Mbps Ethernet speeds. The networked environment is rapidly moving way beyond that speed." While the statement was made in early 2001, the problem still holds true; network speeds are increasing far faster than IDS technology.

Another example of problems with network interface requirements comes courtesy of Recourse Technologies, the producer of the ManHunt IDS product. They experienced performance much less than gigabit speeds (approx 700Mb/s) with Sun's x86 Solaris' stock Intel G1000 NIC drivers. After troubleshooting the problem, Recourse rewrote Sun's Intel fiber NIC driver for their 1.2 release to increase their overall IDS performance. Through current tests by Miercom labs and from first-hand experience, Recourse's v1.2 NIC drivers operate at 900+Mb/s.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

CPU

CPU utilization is important when designing an IDS. "Doing intrusion detection in real-time, especially at higher network speeds, requires significant amounts of dedicated processing resources," states David Curry, a Senior Internet Security Analyst for IBM's Emergency Response Service. A certain number of available processor cycles are required for each packet in the product. Whether it is to check the state of the connection and deny unsolicited syn-acks, examine and compare packet payloads to signatures of known attacks, or track-back a rule offender through an open connection, CPU clock cycles are necessary. The longer these actions take, the less network bandwidth the IDS is capable of watching.

The alternative to slower network connections is fewer features. One approach in limiting the up front CPU utilization is demonstrated in the Navy's Shadow project. Shadow performs all CPU intensive comparisons and sorting off-line. When asked about off-line analysis, Sutterfield responded, "Off-line analysis of traffic for the purposes of generating alarms is nearly useless. The DoD pioneered corporate-wide intrusion detection with this approach, and it was useful in that it proved the concept of corporate-wide intrusion detection." He later refined his comments in stating, "Off-line analysis of alarm data looking for trends is, of course, very valuable." This long-term analysis, however, is even more CPU intensive than the typical real-time IDSes. Dependent upon the length of time for the analysis, the potential of dealing with terabytes of information is very real. Also, long-term analysis can check for more types of abuses.

Storage

The single most important aspect of forensic analysis is storage. Packets on a network attracting no attention disappear once received. Without logging these packets, a forensic analyst cannot hope to prove anything if a network intrusion occurs. IDSes log these packets that would otherwise disappear. They are the eyes and ears for the network's security. However, as Marcus Ranum from Network Flight Recorder points out in the CSI Roundtable discussion, "If you record everything on a network, a busy network can throw data faster than an inexpensive hard disk can store it. So, the trick is to know what to record and what not to record." Ranum's trick suggests tailoring, in an attempt to better utilize the precious forensic resource of storage. This tailoring may conserve resources by shrinking the attack signature set. This obviously creates a situation in which fewer attacks are detected.

Scalability

One other network concern is scalability. If an IDS does not scale well, the network resources utilized on an enterprise level may easily overwhelm the existing architecture. Sutterfield continued in the CSI Roundtable, "Local management of an IDS technology-just as with other locally managed security technologies-brings significant hidden costs that haunt the user later. Scalability is vital for effective deployment of IDS in the vast majority of corporate networks." Placing more emphasis on the sensors and cutting down traffic sent between the sensors and end analysts can limit network resources being utilized and promote scalability.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Analyst

An additional resource often overlooked is the end IDS analyst. This person is regularly the most under-appreciated component of any IDS design. In the CSI Roundtable, Ranum points out:

> Burglar alarms [Signature-based IDSes] are much easier to implement and are fairly reliable. They don't generate lots of false-positives and require fairly little tuning. They're also brute force and "dumb"-burglar alarms look for attack patterns that match some kind of a dictionary of well-known attacks. When they see the pattern, they generate an alarm. False-positives are much more rare but can happen-for example, a person FTPing down powerpoint viewgraphs with examples of attack scripts might accidentally trigger an alarm as if they were downloading "rootkit".

Users don't have to be well trained to use signature based Intrusion Detection Systems. Their ease of use and low rate of false-positives makes them ideal for less trained analysts. But, in the same CSI discussion, Gene Spafford, Director of Purdue's COAST Labs, later responds, "Any existing system, or any system available in the near future, will require monitoring and maintenance by a knowledgeable and capable technical person-either as part of a remote monitoring service, as part of a local security staff, or both."

These knowledgeable and capable technical staff will appreciate the ease of use associated with most Commercial Off-The-Shelf (COTS) Graphical User Interface (GUI) IDSes available today. As Raghudharan points out, "skilled staff plays a crucial role for the success of any IDS. A properly trained Intrusion Detection analyst should be able to identify 'faked' traffic or at least he or she should liaise with the ISP to determine the source of the problem."

Unfortunately, even the most skilled staff may become overwhelmed. Just as the much-publicized Denial of Service (DoS) attacks occurred on Yahoo in early 2000, IDS analysts can just as easily be DoS'd with products such as Stick and Snot. Christopher Klauss, Founder, and Chief Technology Officer of Internet Security Systems, in the CSI Roundtable states, "Data overload is one of the major problems with intrusion detection systems. There are two fundamental ways to deal with it-control what the product reports and ensure that the product has robust data management facilities." Controlling what the product reports implies tailoring, or throwing facilities with more resources at it.

Most IDS Vendor's approach the problem through automation, the trimming of information down to the minimum amount of data necessary to alert the analyst. These correlation tools that perform automation are still in the development stages. When asked at the CSI Roundtable about the issues with real-time alarming, David Curry explains, "You need a reporting system that lets you collect the information from the sensors in a central location. You need a system to store that information for later analysis, along with tools to perform the analysis. You need a way to monitor all these sensors around the clock, and take instant action when an alarm comes in. An attack can be over in minutes, or even seconds." The problem of overload is so severe, that Raghudharan writes, "If the staff currently doesn't have the time to check the firewall and router logs, IDS alerts are unlikely to be acted upon in a timely manner." This overload is a serious problem as the minutes and seconds during an attack are the difference between a root compromise with evidence erasure and a successful detection and avoidance.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Chapter 2

Network IDS:

To Tailor or Not to Tailor

Tailoring

Advantages

Limiting resource consumption

Storage Area Networks (SANs), Voice over IP (VoIP), Multimedia teleconferencing, more demanding Operating System components such as Microsoft's Active Directory, and other weekly advances in technology coupled with increasingly cheaper bandwidth are prompting increased network rollouts at higher speeds. Router and switch vendors already have proprietary methods of combining multiple 1Gb fiber connections to provide aggregate 10Gb connections between products. RFC's (802.3ae) for 10Gb Ethernet are nearing ratification in the first quarter of 2002.

Unfortunately, few IDS vendors are currently operating effectively at less than 0.5 percent of that bandwidth. As all resources become scarcer, and security requirements grow more demanding, IDS vendors have attempted several approaches for increasing the amount of throughput an IDS can handle. The product-limiting resources are IDS implementation dependent. Typically, either memory or CPU is the deciding factor, and the total resources used are dependent upon the number or size of the IDS rule set and the features applied. One of the vendor-attempted solutions is trimming the amount of resources utilized by decreasing the size of rule sets or amounts of patterns through which the IDS searches. This process is referred to as tailoring. Tailoring may be manual, automatic, or performed by an outsourced service.

Christopher Klaus, from ISS, discusses the details of tailoring in the CSI Roundtable,

> Tailoring "…is making sure your IDS is appropriate to your network… Network appropriateness means fine-tuning an IDS so that it looks for attacks and prioritizes events in a manner that is consistent with your current network infrastructure. Have no old SunOS systems? Well then, you don't need to worry as much about UDP Bomb attacks because you're not vulnerable to them. This fine-tuning substantially reduces false-positives. This fine-tuning requires knowledge about the specific network's topology and inventory."

Klauss' comments take note of saving IDS Analyst resources through tailoring's reduction of false-positives. Less alerts display, as there are fewer signatures to match against. Without intimate knowledge of the network topology, Klauss' "fine-tuning" IDS signatures will allow risks to go unmitigated through IDS detection. The specific knowledge of the network topology must be accurate to the second. Working off day-old network diagrams may constitute history lessons. Also, some of this tuning may be performed using IP

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

addresses as the control factor. Care must be taken to avoid tailoring with DHCP assigned IP Addresses typically used in enterprise environments.

The problems with resource consumption also extend to the storage of IDS data. Tailoring the signature set collects less information. The problems are best summarized by Network Flight Recorder's President and CEO, Marcus Ranum, during the CSI Roundtable, "Tailoring of data management is going to be a huge problem for IDS-how much to record, how long to keep it, and how to present it to the end user." These tailoring problems are especially huge in forensic investigations and analysis. Policies regarding data management must be in written and enforced, follow industry best practices and be well drafted. Also, these policies must be regularly reviewed to minimize culpability.

Ranum, continues in detailing NFR's approach to IDSes in the CSI Roundtable, and explains how tailoring affects all of their deployments, "We call our product a general purpose traffic analysis engine. It's internally programmable, so you can pretty much tell it what to look for. If you want to look for, let's say, SYN floods, you can program it to count SYN packets and alert someone if there is a statistical anomaly…" NFR *recommends* tailoring threshold values to operate at a site's risk acceptability level.

Review of the Signatures

One common practice in IDS Signature writing is to have multiple signatures with varying degrees of granularity. One signature may refer to IP packet overlap, another may refer to a teardrop attack, and a third may list nmap or Nessus scans. Each of these signatures could be applicable to the same packet. In many IDSes, the thought is that all signatures will match, and correlations drawn between the multiple alerts. In reviewing and tailoring IDS signature sets, removal of the more specific duplicate signatures leaves the broadest signature, preserving precious resources. When the alert occurs, less information exists to draw a conclusion from.

Disadvantages

Delayed Release

New signatures must be tailored in the same methods as old signatures to maintain the tailoring resource saving benefits. Each time a new intrusion method is discovered, new vendor IDS signatures are defined to detect the intrusion. The Australian Communications Electronic Security Instruction, ACSI33, states, "Like virus checking software, an intrusion detection device should be updated regularly to ensure that the latest vulnerabilities and signatures are recognised by the detection software." Tailoring requires an additional lag time before the signatures are field ready, slowing the above recommended regularity.

Smaller Peer Group for Review

Prior to release, rule sets typically go through very stringent processes and Quality Assurance (QA) tests before release by an IDS vendor. The rule sets are regression tested to insure that other signatures are not impacted by new sets. Even open source code such as Snort rule sets are viewed and tested by the Open Source community prior to suggested usage, but provided with a use at your own risk. Tailoring is often someone's opinion if the signature applies.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Locally tailored rule sets typically do not have the same resources to validate tailored signatures, or place the same emphasis on regression testing to verify interoperability. The impact can be the same. As Lee Sutterfield, from Wheelgroup states,

> "Current technology places a lot of smarts into the sensor itself which selects only the packets that could have possible security implications…. The point is that the sensor has to be smart and select only information of value. The rest is ignored. This is the only way to do large-scale real-time ID with any efficiency."

On an enterprise scale, a small rule set change can effectively nullify the above-mentioned smarts in the sensor. The packets missed or worse, intentionally ignored due to tailoring, can easily be the initial reconnaissance, or the intrusion itself.

Misconfiguration

The likelihood of Intrusion Detection System misconfiguration is greater when tailoring is performed. The ACSI33, states, "Inappropriate initial configuration can lead to a flood of irrelevant information that requires follow-up action by administrative staff, or alternatively, may result in a poorly focused system that does not report on organisational security objectives." This poorly focused system or flood of inappropriate data wastes resources, performing the opposite objective of tailoring.

Reconnaissance

Reconnaissance allows an intruder to determine what machines are included on a network, what Operating Systems are installed on those machines, and what services are offered by those machines. Reconnaissance allows an intruder to determine vulnerabilities within a network. These determinations are made through sending packets that elicit known responses. IDS signatures tailored to a local set of machines with the expectation that the trimmed rules "should never be seen" may miss recon attempts from likely intruders.

After reconnaissance, actual intrusions require further work actually exploiting the vulnerabilities found. Gene Spafford, in the CSI Roundtable, notes, "Network-based monitors that look for known attack patterns are fine in environments where your biggest worry is outsiders coming into a corporate network using well-known "toolkits" to probe established vulnerabilities." Signature based IDSes are well designed for detecting well-known reconnaissance and intrusions. Unfortunately, some of these alerts may easily be tailored out of the IDS architecture.

Spafford in the CSI Roundtable, notes how quickly a network design can change:

> Firewalls and filtering are intended to keep the "bad things" out of the network. However, sometimes those mechanisms fail because of bugs, hardware failures, user mistakes, or simple ignorance. For instance, someone may not understand about the needs of network security and thus set up a modem on his desk for weekend and evening access. Firewalls and proxies don't help in this, and may not even be able to detect it happening. An IDS should detect if problems occur because of the connection. Then too, no matter how much you filter, users will often find ways to circumvent. Downloading ActiveX objects, multi-media using unknown proprietary protocols, and installing new software may all introduce new avenues for threats thru the firewalls that need to be monitored. And of course, in many or most environments,

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

the *biggest* threat may actually be the people who are already on the "inside"-they need to be monitored, too.

All of these filters and changes again open the possibility that the IDSes do not allow the analyst the information to draw a conclusion.

Raghudharan attempts to make a case for tailoring in a layered design, stating, “the advantage that could be taken is that the tailoring of NIDS attack signature database can be done to consider only those attacks that are applicable to the systems in the DMZ; at the same time the firewall will have blocked all other traffic.” However, this places emphasis on the security of the FW. The network expects that there will never be a misconfiguration on the FW, that the Firewall will never be vulnerable to a malicious attack, or that an authorized FW user will never attempt to access resources through the DMZ without proper processes followed. Better design allows overlap between all devices, allowing the possibility for one device to fail, and still have a secure, functioning system.

Analyst Mistakes

Skilled analysts are arguably the most important part of any Intrusion Detection System. The Analyst must make connections and correlations from disparaging pieces of information. Tailoring removes the amount of information presented to the Analyst. As Phung states, the analysts “only need samples of the data in order to generate profiles, but there will also be the argument that analyzing anything, especially network traffic, without all the data could lead to false conclusions.” These false conclusions can cause resource waste, eliminating the benefits of signature tailoring.

David Curry, from IBM, makes the best case for not tailoring in the CSI roundtable, “Most of the time you can't reduce false alarms without the risk of missing a real one, so you have to be able to immediately separate the wheat from the chaff.” The impetus for evaluating and identifying these real attacks falls on the *skilled, well-trained analyst.* The more information that is provided through the IDS, the better capable the skilled analyst is to perform their duties.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Chapter 3

Network IDS:

To Tailor or Not to Tailor

Tailoring in "Off-The-Shelf" IDS Products

There are many questions surrounding tailoring within commercial, signature-based network IDSes. According to Boeckman and Northcutt, "The fundamental problem is that most existing IDS products are signature-based systems. In the most literal sense, signatures are 'indicators of known attacks'." This places the IDSes in a reactive rather than proactive position. As each "indicator" changes, the IDS rule sets must be changed.

These signature changes are not always smooth. Problems still occur even with the regression testing and QA mentioned above. This is especially true of tailored COTS products. As Jansen notes, "Tailoring detection mechanisms specifically to the system in question and replacing them over time with improved detection techniques is also problematic with many IDS implementations. Often the IDS needs to be completely restarted in order to make changes and additions take effect." If tailoring changes are expected to happen on the fly, an attacker's window of opportunity opens as the IDS is restarted. Dependent upon the frequency of change, the windows of opportunity may constitute a significant risk.

Products such as Cisco's Secure IDS (formerly Net Ranger), Symantec's NetProwler, Intrusion.com's SecureNet, ISS's Real Secure, the Navy's Shadow project, and the open source community's Snort can all limit system resource utilization through signature-based filters. The following paragraphs discuss tailoring in different commercial rule-based Intrusion Detection System products.

Navy's Shadow

"Most 'script-savvy' administrators can easily put together a set of parsing programs that can make the auditing data from a firewall very valuable for performing intrusion detection by tailoring it for a specific environment. This is the kind of capability that, unfortunately, is not readily available in most COTS IDS products," states Boeckman, pointing out, again, the value of a well-trained staff.

The well-trained staff's scripted parsing of data is similar to the beginnings of the Government's "Off-The-Shelf" Shadow product. The later versions of Shadow capture the packet headers of *all* network traffic. This traffic is examined through scripts to produce an hourly correlation of the network's communications.

Lee Sutterfield, from Wheelgroup mentions problems with early IDS designs, similar to Shadow's:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

> Early IDS prototypes did keystroke capture on the network with sniffers. The data was stored on local hardrives and then uploaded to a central facility at night for processing the next day. It worked, but it wasn't operationally effective given the real-time nature of this business.

In its current release, Shadow performs the same uploading to a central facility, but instead of nightly correlation, the data is analyzed hourly. Shadow requires tailoring in order to be effective. In any large environment the Shadow log sizes, data storage requirements, and processing power needed to complete the IDS tasks easily become unmanageable. Tailoring in this instance typically examines TCP/IP packet headers and excludes collecting well-known traffic, such as DNS zone transfers between internal DNS servers or encrypted VPN traffic between gates.

In a perfect forensic world, every packet and its payload would be stored for the offline analysis performed by Shadow. Cost constraints eliminate this possibility and force the network administrator to limit storage and trim packets to "events of interest". These events may come from the SANS top 20-attack list, known malicious Internet Service Providers, or multiple TCP Syn packets from one IP address to another.

Symantec's NetProwler

Symantec's NetProwler product is a unique Intrusion Detection System. Instead of being a typical Network IDS that monitors all network traffic, it is designed to only watch specific machines. NetProwler is designed to accomplish this task by auto tailoring the attacks watched for to the Operating Systems on the machines. The network designer deploys NetProwler sensors on a network segment he wants protected. The designer gives the sensor a specific range of machines to watch, or submits the IDS to auto-detect the machines that are within its broadcast domain. The sensor fingerprints the OS's on the network, and then applies attack signatures that are applicable to that Operating System. If an OS cannot be accurately defined, it is given an unknown status. This typically occurs with network hardware, such as switches and routers. The benefits of saving resources are documented in the above sections that refer to the benefits of tailoring . Unfortunately, the unknown OS's have very minimal attack signatures applied to them. Secured configurations and newer revisions of some software can prompt the NetProwler fingerprinting to apply an unknown moniker to very well known operating systems; these resources are thus unprotected.

SecureNet

Intrusion.com's product literature labels SecureNet as a fully tailorable solution, touting, "You can even choose which signatures are string-matched and which are analyzed in context, tailoring the system to the unique attributes of your network traffic." Yocom demonstrates poor performance on SecureNet's PDS 5545 100 Mb/s appliance, showing the device's performance degrading above 40 Mb/s. According to Intrusion.com's literature, their Gigabit sensor's performance tails off over 600 Mb/s, giving rationale to tailor the rule sets in both instances.

Real Secure

Christopher Klauss, Internet Security Systems in the CSI Roundtable notes, "A good IDS will be extremely configurable-attack signatures can be turned on and off and fine-tuned; the response options of the product can also be configured. This customization allows you

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

to control what the product reports and how it reports it." All of these features are available in the ISS Real Secure product.

Cisco's Secure Intrusion Detection System

Cisco's Secure IDS product was originally named Net Ranger. It was formerly a Wheelgroup asset prior to its purchase by Cisco. As Lee Sutterfield, from Wheelgroup details, the "bottom line, to do ID at 100Mbps+ you have to analyze and collect a great deal of data." Currently, Cisco's 4230 Fast Ethernet sensor appliances run on Dual Intel 600 MHz PIII processor boxes with 512 MB RAM and SCSI mirrored hard drives. The sensor is based on Sun's Solaris 8 for x86 and includes two fast Ethernet network interface cards. This configuration is capable of Intrusion Detection at TX line speed and according to Yocom's tests, operates as well at 90 Mb/s as it does at 30 Mb/s. This was while supporting "the largest database of attack signatures" amongst any of the products tested. Tailoring through signature removal is not necessary in instances, such as this, where the product (in this case an appliance) is designed to handle full line speed.

Overall

All of the products tested by Yocom missed alerts. The vendor's own product literature in many instances defines deficiencies in higher-level stress testing. Current Off-The-Shelf IDS products cannot keep up with network demands, as demonstrated by the lack of providers ready with a 10Gb scalable solution, and network vendor proprietary 10Gb solutions already in place. The above products are a sampling of the current state of network IDSes. As Yocom states, the products still need to work on "their ability to support speeds beyond 100M bit/sec."

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Chapter 4

Network IDS

To Tailor, or Not to Tailor

Conclusions

If anyone has the confidence, or naiveté to assume:

- Firewall and network boundaries will block all unwanted network access attempts,
- Users will never attempt to access resources which are guarded through means which may break policy,
- And intruders will never obfuscate, manipulate, or adjust network traffic in an effort to reach resources which are protected,

then by all means tailor Intrusion Detection signatures to account for only the design originally architected. The fact is, the network will change, users will wish to access new hardware or install new software without examining the security implications, and intruders will operate by any means necessary to gain entrance to a network.

Recall that IDS vendors have a great interest in their product performing as efficiently and effectively as possible. The vendors themselves tailor these signature sets to eliminate wasted processor cycles and duplicate rules. However, they also have an obligation to the end analyst to provide a detailed description of what is happening. This allows the analyst to make the most informed decision possible and attribute the success of the attack aversion to the IDS.

Provided the network IDS is capable of operating at full network-load capacity, IDS tailoring through signature removal is a poor idea. The term blindsided stems from not having information to avoid an attack. Tailoring signatures limits the amount of information. Signatures match known attack patterns that allow skilled analysts to determine if a network penetration is eminent. Tailoring allows valuable information regarding reconnaissance to be missed, or actual attacks to be ignored. If tailoring is required to occur due to legacy product selection or unexpected network growth, be forewarned of the consequences. When this tailoring occurs, make sure a process is set in place to review as completely as possible any changes that need to be made. This process must include reviewing these changes regularly. Remember, the analysts can separate “the wheat from the chaff”, only if they have both to begin with.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Network IDS

To Tailor, or Not to Tailor

Internet References

Arnold, A. "Kernel Based Anomaly Detection." Intrusion Detection Systems, Machine Learning Group. Columbia University. Apr 2001.
URL: http://www.columbia.edu/~aoa5/ids/aoa5_Kernel_042601.htm (6 Mar. 2002).

Australia. Defense Signals Directorate. "Handbook 13, Intrusion Detection and Audit Analysis v. 1.0." Australian Communications-Electronic Security Instruction 33 (ACSI 33).
URL: http://www.dsd.gov.au/infosec/acsi33/HB13.html (6 Mar. 2002).

Bace, R. & P. Mell, "NIST Special Publication on Intrusion Detection Systems", Feb. 2001
URL: http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf (6 Mar. 2002).

Boeckman, C. "Getting Closer to Policy-Based Intrusion Detection." Information Security Bulletin. May 2000.
URL: http://www.chi-publishing.com/isb/backissues/ISB_2000/ISB0504/ISB0504CB.pdf (6 Mar. 2002).

Jansen, W., P. Mell, et al. "Mobile Agents in Intrusion Detection and Response." National Institute for Standards and Technology. June 2000.
URL: http://csrc.nist.gov/staff/mell/maidr.pdf (6 Mar. 2002).

McCullagh, D. "Routers Blamed for Yahoo Outage." Wired News. Feb 2000
URL: http://www.wired.com/news/business/0,1367,34178,00.html (6 Mar. 2002).

"Manhunt Product Literature." Recourse Technologies.
URL: http://www.recourse.com/product/ManHunt/ (6 Mar. 2002).

Miercom Labs, "Recourse Man Hunt Performance Testing." Nov 2001.
URL: http://www.mier.com/reports/recourse/ManHunt.pdf (6 Mar. 2002).

"NetProwler 3.51 Product Literature." Symantec Corporation.
URL:
http://www.symantec.com/techsupp/enterprise/products/netprowler/netprowler_351/manuals.html (6 Mar. 2002).

"Network Intrusion Detection System Product Overview." SecureNet Series. Intrusion.com Corporation.
URL: https://www.intrusion.com/products/downloads/nids_01-0716.pdf (6 Mar. 2002).

Phung, M. "Data Mining in Intrusion Detection." Sans. Oct 2000.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

URL: http://www.sans.org/newlook/resources/IDFAQ/data_mining.htm (6 Mar. 2002).

Power, R. "CSI Roundtable: Experts discuss present and future intrusion detection systems." Computer Security Journal vol XIV, #1. 2001
URL: http://www.gocsi.com/roundtable.htm (6 Mar. 2002).

Raghudharan, R. "Intrusion Detection Systems: Beyond the first line of defense." Network Magazine. Sept 2001.
URL: http://www.networkmagazineindia.com/200109/security1.htm (6 Mar. 2002).

"Real Secure Product Literature. " ISS Corporation.
URL: http://www.iss.net/products_services/enterprise_protection/rsnetwork/index.php (6 Mar. 2002).

Romascanu, D., D. Harrington. "IEFT Ethernet Interfaces and Hub MIB WG Update." July 2001.
URL: http://www.ieee802.org/3/efm/public/jul01/presentations/romascanu_1_0701.pdf (6 Mar. 2002).

"Secure IDS Release 2.2.1 Product Literature." Cisco Corporation.
URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/netrangr/nr221/index.htm (6 Mar. 2002).

"Shadow 1.6 documentation." Naval Surface Warfare Systems – Dahlgren Lab.
URL: http://www.nswc.navy.mil/ISSEC/CID/index.html (6 Mar. 2002)

'"Stick'- A Potential Denial of Service Against IDS Systems." Internet Security Systems Security Alert, Mar 2001
URL: http://xforce.iss.net/alerts/advise74.php (6 Mar. 2002).

Additional Sources

Northcutt, S., J. Novak. Network Intrusion Detection: An Analyst's Handbook, 2nd ed. Indianapolis: New Riders, 2000.

Yocom, B., K. Brown, D. Van Derveer. "Intrusion Detection Products Grow Up." Network World. Oct 2001.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced