Global Information Assurance Certification Paper

Intrusion Prevention: Taking IDS to the Next Step

SANS GIAC GSAE Assignment #1 Option #1

Tom Ginn

Version 1.1

August 18, 2003

Table of Contents

Abstract

Malicious attacks against a computer or network of computers in any organization represent a serious threat to the confidentiality, integrity and availability of the system's information resources. The rapid growth and use of networked information systems has created a crucial need for organizations and individuals to determine how best to protect that information. Intrusion Detection Systems (IDS) are a valuable tool in identifying, and providing important information about intrusion attempts. They enable the system owner to take action to repair and recover from any damage that may have occurred or been caused by such an attack. Security Analysts can also use this information to configure their networks such that damage from future attacks can be reduced or avoided. This is the basis for Intrusion Prevention.

Some current methods of Intrusion Prevention exist in the form of firewalls, router ACLs and physical limitations (such as disconnecting a system from the Internet entirely). One of the most current and commonly discussed forms of Intrusion Prevention stems from today's Intrusion Detection Systems. Using the same tools found in current Intrusion Detection Systems, antivirus technologies and firewalls, Intrusion Prevention Systems (IPS) place emphasis on stopping a network attack automatically, without the need for analyst review or response. However, Intrusion Prevention Systems can experience significant obstacles when implemented. This paper will examine these limiting factors, discuss the benefits of implementing an IPS, and compare IPS technologies with current IDS tools in order to present the reader with a clear understanding of Intrusion Prevention Systems and their use in today's IT environment.

Introduction

With the increase in the number of network attacks over the past several years, organizations have not only sought to protect their resources, but are tunring their attention to monitoring events occurring in their systems, in order to detect, analyze and safeguard against malicious attacks.[1] The systems responsible for performing these tasks are called Intrusion Detection Systems or IDS.

Recently, a new approach to threat security has been developed. This solution promises to not only detect and report on security threats across a network or system, but to actively prevent those attacks from being successful the first time. While an IDS can alert System Administrators and security analysts to potential attacks and allow a response to occur, IPS systems will block such attacks automatically. These new IPS systems suffer a number of problems, not the least of which is the quantity of false positives that are triggered. The security industry is currently struggling to employ an IPS device that will be able to automatically provide the same analysis and response employed by a security analyst.

Why Use an IDS?

Intrusion Detection Systems offer a level of protection that has become increasingly necessary in today's computer-networking environments. The increase in the number of malicious attacks and network breaches has made the use of IDS systems a must. Most organizations are no longer considering whether or not they should use an IDS, but rather, which IDS to use.

There are several convincing reasons to implement an IDS solution. According to the NIST publication on Intrusion Detection Systems[1], some of these reasons are:

1. Increase perceived risk of discovery among those who would seek to attack a network, limiting the chances of someone actually carrying out such an attack,
2. To detect suspicious activity on the network, specifically those activities that were not prevented by other security measures,
3. To detect and report on the initial stages on an attack, allowing time for such an attack to be prevented by the System Administrator,
4. To document current threats,
5. To monitor attacks that do occur and provide helpful information on the nature of the attack, for future reference and prevention.

According to the most recent Computer Security Institute survey (2002), which was conducted with the participation of the San Francisco Federal Bureau of Investigation, cyber crime has resulted in increasing financial costs for the third

[1] Intrusion Detection Systems, Rebecca Bace and Peter Mell

year in a row.[2] Of those surveyed, 223 respondents were able to quantify their combined financial losses at over $455,000,000. As well, 90% of those who responded (primarily large corporations and government agencies) "…detected computer security breaches within the last twelve months."[2]

It would appear from such statistics, that no organization is safe from being a target of information theft and computer crime. Therefore, it has become more important than ever for large organizations to have the ability to detect possible attacks, monitor the method in which such attacks are conducted and use this 'footprint' information to secure their systems and networks from similar attacks in the future.

Intrusion Prevention – The Next Step?

IDS solutions have become a successful addition to many network security infrastructures. Information gathered by Intrusion Detection Systems have allowed organizations to safe-guard their information and networks against known and suspected attacks. However, while most Intrusion Detection Systems are capable of detecting and monitoring suspicious activity, they are generally not configured to stop such activity. Organizations rely on experienced security analysts to respond to alerts generated by the IDS and react accordingly. It is these analysts who are able to quickly review the information produced by the intrusion detection system and determine the nature of any suspicious activity. The analyst can then deploy a pre-determined response plan based on the review of information. Intrusion Prevention Systems seek to automate this function, returning most, if not all, intrusion detection and response to the IDS itself.

The aim of Intrusion Prevention is to stop an attacker cold, before any malicious activity can be performed. Using rules, usage models and correlation engines, IPS systems can help ensure appropriate network usage by automatically preventing unauthorized use from occurring.[3] The benefits of such technology are obvious. If an organization can not only detect suspicious activity, but also automatically prevent that activity from penetrating the network's defenses, they can more effectively safeguard their information resources against malicious attacks and ensure continued confidentiality, integrity and availability of those resources.

An effective IPS also provides a great deal of efficiency by significantly reducing response time. With automated security analysis and response, an IPS can quickly prevent unauthorized activity from taking place and take measures to provide information on the nature of the attack itself, i.e.: the source of the activity and its intent. This information can then be used to track the attack to a specific individual, or be used in a legal response. While it may take several minutes (or

[2] Golubev, Dr. Vladimir A. "2002 Computer Crime and Security Survey"
[3] Vijayan, Jaikumar. "Intrusion prevention touted over detection"

longer) for a professional security analyst to be alerted to a potential attack, and formulate a response, an Intrusion Prevention System could perform the same actions immediately. The quick response time of an IPS will greatly reduce the risk of damage to the network and company information.

IDS and IPS Problems

Although the IT Security industry has been working hard to strengthen and improve the effectiveness of Intrusion Prevention Systems, several common problems still remain; the most substantial problem is that of false positives. A false positive in the IDS world is suspicious activity detected by the system that is in fact legitimate network traffic. A common example is that of an IDS raising a "SYN Flood" alarm due to a large number of SYN packets being sent to a busy web server. The IDS determines this traffic to be the result of an attack, when the condition is indeed genuine.[5]

False positives are costly in terms of manpower and resources. False positives generate alarms that must be examined and reviewed by Security Analysts, who in turn must have the expertise and experience necessary to accurately identify these false positives. In the case of a large network with many servers and devices, the number of alarms being generated may even warrant the need for additional human resources, increasing company costs. This has lead several industry authorities to conclude that IDS systems have outlived their usefulness, citing unjustifiable costs as reason to abandon the IDS approach to network security and instead rely on more 'traditional' methods found in firewall application. This topic is explored briefly at the end of this report.

While false positives are a time consuming trouble for Intrusion Detection Systems, they can cause much greater harm in an Intrusion Prevention environment. Instead of simply generating an alarm when suspicious network activity is detected, an IPS will stop such activity automatically. Considering the number of false positives detected by today's security systems, this problem can quickly transform a network IPS into a brutally effective denial-of-service device. Several new IPS products have touted that they are capable of removing, or at least reducing this problem, however it appears that many companies are choosing to continue to rely on the human factor; allowing their security analysts to review and respond to alarms generated by current IDS systems. Ted Julian, president of Arbor Networks Inc., a network anomaly detection vendor, suggests that "…the need for better filtering and detection methods is patently obvious".[6]

The other serious problem plaguing Intrusion Prevention (and some Intrusion Detection Systems) is that of network bottlenecks. Due to the tremendous traffic loads placed on IPS devices, significant speed is required in order for these systems to remain efficient. If the IPS does not work quickly enough, it can begin

[5] Ranum, Marcus J. "False Positives: A User's Guide to Making Sense of IDS Alarms"
[6] Vijayan, Jaikumar. "Intrusion prevention touted over detection"

to drop packets. Combined with the problem of false positives, it is possible for an Intrusion Prevention System to become a single point of failure for those organizations that rely too heavily on them.

With these problems in mind, it is important for any business to carefully review their IT security and business needs in order to determine how best to implement an IDS or IPS security device. To accomplish this task, it is best to understand the features that work well in an IPS system, and those that require further research.

Implementation of IPS

A number of companies have already released promising IPS products. Entercept Security Technologies has created an "…updated version of a host-based intrusion-prevention software tool"[7] that takes advantage of virus signatures and behavioral rules to track suspected attacks before those attacks have a chance to affect a targeted application. As well, Teros Inc. has created a new module for one of their Intrusion Prevention systems that uses predetermined norms to assess and direct traffic passing through to individual servers or applications.[1] Other companies have designed IPS products that provide real-time alerts and on-the-fly revisions and updates to existing firewall rules.

While each of these implementations seem to provide solid security, it is important to realize how IPS systems are limited, and where their main strengths lie. This understanding will allow Security Analysts to implement an IPS solution in such a way that it takes advantage of IPS benefits, while avoiding the pitfalls that are associated with too much reliance on automatic response.

The most successful implementation of an IPS will be one that uses the most solid parts of current intrusion detection systems. Before an IPS is configured to drop suspicious packets, there must be near-100% certainty that the packet is in fact bad. If the likelihood of the IPS producing a false positive is greater than 1%, for example, an organization may wish to consider continued use of current intrusion detection systems, rather than rely on the IPS to block this traffic. However, problems such as Protocol Anomalies or single packet kills, where the IPS is less than 0.001% likely to generate a false positive or mis-detection, can be successfully implemented in intrusion prevention software and devices.

An IPS' ability to properly handle specific types of suspicious activity has been referred to as an IPS "…spectrum of competence."[8] Table 1 below, taken from a SANS Webast on Intrusion Prevention Essentials, by Joel Synder, is an excellent example of measuring the competence of IPS systems. Security analysts will

[7] Vijayan, Jaikumar. "Intrusion prevention touted over detection"
[8] Snyder, Joel. "Intrusion Prevention Essentials" SANS Webcast. 4 Dec. 2002

need to carefully research and review this kind of information when considering how best to implement an IPS solution.

Class of Problem	Likelihood of False Positive	Likelihood of Mis-Detection
Protocol anomaly	<0.001%	0%
DoS Attack	<10%	<0.001%
HTTP Attack	50%	<0.001%
Port Scan	25%	5%
Information Gathering	25%	5%
Single Packet Kills	0%	<0.001%
Backdoor Access	<1%	10%
Trojan Horse	<1%	10%

Table 1[9]

Gartner – The End of IDS?

On June 11, 2003, Gartner Inc. declared that intrusion detection systems would be obsolete by the year 2005. The Gartner Information Security Hype Cycle indicates that current Intrusion Detection Systems fail to provide a level of security equal to the costs of implementation and maintenance. The report not only claims that there is no value in IDS technology, as promised by vendors, but further cites that such technologies have "…proven to be costly and an ineffective investment."[10] Instead, firewalls operating on both application and network levels will be able to take on the role of intrusion detection and prevention by 2005.

Not surprisingly, this report has generated heated debate in information security circles. Although it is not within the scope of this document to discuss the validity of the Gartner report, it is important for all information security professionals to understand the implications of the Gartner declaration. The future of intrusion prevention systems would appear to rely heavily on the legitimacy of Gartner Inc.'s findings.

When considering the implementation of an intrusion prevention system, Security Analysts must not only consider those areas of current IDS technologies that could benefit from the automation of an IPS, but must also carefully consider the current effectiveness and value of their existing IDS application. Diligent research and testing will reveal the overall effectiveness of a network's ability to detect and respond to suspicious activity, and further analysis will indicate where the addition of intrusion prevention will increase the level of protection provided. Security Analysts and Network Administrators will have to carefully compare the abilities of an IDS with the cost of their implementation.

[9] Snyder, Joel. "Intrusion Prevention Essentials" SANS Webcast. 4 Dec. 2002.
[10] Haines, Allison. "Gartner Information Security Hype Cycle Declares Intrusion Detection Systems as Market Failure"

Conclusion

Intrusion Detection Systems are an important aspect of many organizations' security infrastructures. In the past few years, the number of attacks against information networks has increased not only in volume, but also in the severity of damage caused by those attacks. IDS has become an effective protection against such malicious activity and has laid the groundwork for Intrusion Prevention, a more efficient method of network security. Intrusion Prevention Systems offer a level of protection that is both automated and immediate. IPSs can give an organization the ability to greatly reduce response time and minimize or eliminate the damage that may be caused by a network attack.

Today's IDSs are continually being improved as the need for faster and more reliable detection increases. Problems such as false positives, mis-detection, and network bottlenecks require further research and improvement. But as these improvements are made, the security protection that will be offered through Intrusion Prevention should make the IPS a mainstay in most organizations. IT Security professionals will require a detailed understanding of how these systems work and how they can be best configured and operated. Successful implementation of Intrusion Prevention will greatly improve the ability to protect the confidentiality, integrity and availability of information resources.

List of References

1. Northcutt, Stephen. Novak, Judy. Network Intrusion Detection, An Analyst's Handbook, Second Edition. Indianapolis: New Riders Publishing, 2000.
2. Proctor, Paul E. The Practical Intrusion Detection Handbook. Upper Saddle River: Prentice-Hall, Inc, 2001.
3. Njemanze, Hugh S. "Centralized Security Management Provides Foundation for Effective Intrusion Prevention". Information Systems Control Journal. Volume 4, 2003 (2003): 47 – 48.
4. Vijayan, Jaikumar. "Intrusion prevention touted over detection". 11 April 2003. URL: http://computerworld.com/securitytopics/security/story/0,10801,80260,00.html (3 June 2003).
5. Sundaram, Aurobindo. "An Introduction to Intrusion Detection". Intrusion Detection. 23 Jan. 2001. URL: http://www.acm.org/crossroads/xrds2-4/intrus.html (12 June 2003).
6. Cummings, Joanne. "From intrusion detection to intrusion prevention". The Buzz. 23 Sept. 2002. URL: http://www.nwfusion.com/buzz/2002/intruder.html (12 June 2003).
7. Mimoso, Michael S. "Gartner declares IDS obsolete by 2005". Security News & Analysis. 12 June 2003. URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci905961,00.html (12 June 2003).
8. Haines, Allison. "Gartner Information Security Hype Cycle Declares Intrusion Detection Systems as Market Failure". Gartner. 11 June 2003. URL: http://www3.gartner.com/5_about/press_releases/pr11june2003c.jsp (12June 2003).
9. Ranum, Marcus J. "False Positives: A User's Guide to Making Sense of IDS Alarms". Feb. 2003. URL: http://www.icsalabs.com/html/communities/ids/whitepaper/FalsePositives.pdf (3 June 2003).
10. Bace, Rebecca. Mell, Peter. "Intrusion Detection Systems". NIST Special Publication on Intrusion Detection Systems. SP 800-31. November 2001. URL: http://cs-www.ncsl.nist.gov/publications/nistpubs (14 February 2003).
11. Golubev, Dr. Vladimir A. "2002 Computer Crime and Security Survey" Computer Crime Research Center. 2002. URL: http://www.crime-research.org/eng/library/Cybercrime_Stat.html (6 June 2003).
12. Hulme, George V. "Attacks Averted" InformationWeek. 3 Feb. 2003. URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=6512063 (7 May 2003).
13. Snyder, Joel. "Intrusion Prevention Essentials" SANS Webcast. 4 Dec. 2002.

High Level Intrusion Detection Audit

SANS GIAC GSAE Practical Assignment #2

Tom Ginn
Version 1.1
August 18, 2003

Table of Contents

Background

ThisCompany relies extensively on Information Technology to support critical, day-to-day business activities. The IT infrastructure is exposed to security threats and vulnerabilities that can potentially compromise its functionality, or lead to loss of data confidentiality, integrity, and availability. Many of these threats and vulnerabilities relate to unauthorized activities conducted on the network or servers.

Given the broad scope and nature of security threats in today's IT environment, it is recognized that perfect protection is not possible; however, there are measures that should be taken to provide reasonable safeguards. To adequately protect the Company's information assets and ensure continuing availability of IT resources, a multi-layered approach to information security should be employed. One layer of security control is the ability to detect, respond to, and recover from unauthorized activity. This is commonly referred to as Intrusion Detection.

Increased reliance on the Internet magnifies the need for this control layer in the IT environment. Without the ability to detect and respond to unauthorized activities, there is increased risk that Company data will be viewed, copied, changed or deleted, and that IT components may be compromised.

SCOPE

The primary scope of this audit will be to review the current IDS implementation and management in use at ThisCompany and compare against industry best practice. The audit will focus primarily on IDS procedures in use and will include:

- Review of IDS solution, its use and configuration,
- Review of monitoring, logging, and analysis procedures,
- Review of response procedures, supervision and control.

A detailed review of the technical configurations of the Intrusion Detection System and tools remains outside the scope of this audit. This audit is intended to ensure that IDS management and implementation adhere with industry best practice and that response procedures effectively safeguard the security of the Company's data. Based on the results of this audit, a more thorough and detailed examination of the Intrusion Detection System may be required.

Audit Objectives

The objective of this audit is to determine the completeness, appropriateness, and effectiveness of ThisCompany's ability to detect and respond to unauthorized activities through the use of network intrusion detection and related response procedures and processes. This audit will also determine whether

ThisCompany's incident response procedures are sufficient to allow for timely resolution of problems and protection of corporate data.

Audit Procedures

All items in the following Audit Checklist will be addressed and reviewed by the following audit procedures:

- Gather and review relevant documentation
- Conduct interviews with appropriate personnel
- Observe network intrusion detection technologies and processes in operation, or the evidence of such operation
- Compare against recognized IDS 'best practices'
- Analyze results
- Make observations and recommendations as appropriate

The key to completing the audit successfully and on time is the availability of necessary client-area staff and documentation.

Audit Checklist/Questionnaire

The following audit checklist/questionnaire will be used to evaluate IDS in use in ThisCompany's system environment. The Checklist is divided into four (4) sections: General, Information Sources, Analysis and Response. A fifth section is added as an optional checklist to review additional tools that may be used in conjunction with the IDS.

This checklist should be used as an aid when interviewing Security Analyst personnel and those people associated with the operation and management of the IDS. Interviews will also determine which sections and questions of the checklist are appropriate and where further information could be gathered.

Examples of evidence are included with the checklist. These are the auditor's suggestions on where and how potential evidence can be found. Possible sources of information and evidence are not limited to those indicated by the checklist.

General		
Topic	**Questions**	**Evidence Examples**
General	What type of IDS is in use for the detection of security breaches?	List of IDS(s) used.
	How are system administrators alerted when intrusions or unusual activity is detected?	Procedure information or samples (screenshots, etc).
Logging	How are IDS processes, including monitoring, detection, notification and response recorded?	Samples of incident response documentation.
	Do recorded activities include event type, date and time of event, user identification, workstation identification, and security actions?	IDS Activity logs.
	Are all logs stored in a secure location with read-only access by authorized personnel?	List of personnel with access to logs.
Usage	How is the IDS configured or used to increase the perceived risk of discovery and punishment of attackers?	Configuration files.
	How is the IDS configured or used to detect problems that are not prevented by other security measures?	Configuration files.
	How does the IDS detect the preambles to attack?	Configuration and signature files.
	What information does the IDS provide on actual intrusions?	Sample documents containing information on suspicious activity.
	What kinds of reports and detailed information documents are produced by the IDS?	Reports and detailed information produced by IDS
	Are IDS statistics and logs generated in formats suitable for inclusion in database systems or for use in report-generating packages?	Sample of IDS formatting or database report.
	What forms of failsafe features are used to hide the IDS from attackers and prevent the IDS itself from becoming the subject of an attack?	IDS product features/implementation.

Goals	Is the overarching goal of the IDS one of accountability or response?	Personnel interviews.
	How is the IDS used to provide accountability (i.e., link a given activity or event back to the party responsible for initiating it)?	Personnel interviews, IDS configuration.
	How is the IDS used to recognize a given activity or event as an attack and then take action to block that attack?	IDS signature files, configuration.
Control Strategy	Does the IDS employ a centralized, partially distributed, or fully distributed control strategy?	Personnel interviews, implementation.
Timing	Does the IDS employ an Interval-Based (batch mode) or Real-Time (continuous) timing mechanism?	Configuration, interviews.

Information Sources		
Topic	**Questions**	**Evidence Examples**
Network Based IDS	Is a Network Based IDS used in the current intrusion detection implementation?	Network architecture diagram, configuration.
	How is the IDS configured to ensure that all packets are processed, especially during periods of high traffic?	Configuration, logs.
	How are monitoring ports configured to ensure that all network segments are included in the monitoring range of the IDS?	Configuration files, list of network segments, log files.
	How does the IDS analyze encrypted information (VPN)?	Sample documentation.
	How are attacks classified as successful or not? Is this process automated or manually investigated by an administrator?	Analyst procedures, logs.
	How is the IDS configured to prevent it from becoming unstable when dealing with network based attacks that involve fragmenting packets?	Configuration files.

Host Based IDS	Is a Host Based IDS used in the current intrusion detection implementation?	Network architecture diagram, configuration files.
	How is it ensured that the IDS is configured and managed for every host monitored?	List of monitored hosts, IDS configuration files, logs.
	How is the IDS itself protected from attack?	Configuration, additional security devices.
	How are network scans and other such surveillance that target an entire network detected and dealt with?	Logs, response procedures and example documents.
	How is the IDS protected against denial-of-service attacks?	Configuration, additional devices, firewall.
	Does the IDS use operating system audit trails as an information source?	IDS settings, additional tools.
	How is this information stored on the system?	Storage location, format, accessibility.
	What is the performance cost on the monitored systems?	Performance analysis, logs.
	How is this performance cost justified or managed?	Business case documentation
Application Based IDS	Is an Application Based IDS used in the current intrusion detection implementation?	IDS architecture.
	How is the IDS itself and the application logs protected against attack?	External security devices, ACLs.
	Is the IDS used in conjunction with a Host Based or Network Based IDS to prevent Trojan Horse and other software tampering attacks?	IDS architecture and configuration.

IDS Analysis		
Topic	**Questions**	**Evidence**
Misuse Detection	Does the IDS employ misuse detection in its approach to analyzing events?	IDS configuration, signature files, security analyst interview.
	How is the IDS regularly updated with the most current signatures of new attacks to ensure the highest level of efficiency?	Automatic update procedure, logs, version/file numbers.
	How are variants of common attacks detected, despite the tightly defined signatures of misuse detection?	Application of signature rules, configuration settings.

	Is a state-based misuse detector used to overcome the problem of variant attacks?	Configuration, security analyst interviews.
	How is the state-based misuse detector configured to detect variations of known attack signatures?	IDS Configuration, signature files, logs.
Anomaly Detection	Does the IDS employ anomaly detection is its approach to analyzing events?	IDS Configuration, architecture.
	How are false alarms separated from actual attacks?	Response procedures, documentation.
	How is anomaly detection used in conjunction with misuse detection in order to define attack signatures?	Security analyst interviews, procedures.
	How are "training sets" of system event records used to characterize "normal" behavior patterns?	IDS log files, analyst procedures.

IDS Response		
Topic	**Questions**	**Evidence Examples**
Active Response	How is additional information gathered during intrusion detection?	Log files, sample documents of detection.
	How is this information used to resolve detection of an attack?	Response procedures, security analyst interviews.
	How is additional information used to support investigation and apprehension of the attacker, and to support criminal and civil legal remedies?	Relevant legal documentation or legal procedures, log files, sample of information gathered.
	What actions are taken by the IDS to change the environment during an attack, thus deterring or stopping a would-be attacker from accessing or affecting vital information?	IDS configurations and automated responses.
	Do these actions include reconfiguration of routers and firewalls or the insertion of TCP reset packets into the attacker's connection?	Security analyst interviews, response procedures, change control processes.
	Is the IDS configured to take action directly against a suspected attacker?	IDS configuration, response procedures, samples.

	How is this process supervised and controlled to ensure damage is not caused to innocent sites or users?	Security analyst interview/procedures, safeguards.
	How is this process supervised and controlled to ensure an innocent attack is not escalated to more aggressive action by the user?	Response procedures, processes.
	Have the legal ramifications of these "strike-back" options been adequately reviewed and approved?	Formal policy on approved response(s). Legal personnel interviews.
Passive Response	Does the IDS system rely solely on passive responses?	IDS configuration settings, response types.
	How and when are alarms generated?	Sample alarm, IDS settings.
	To whom are these alarms displayed?	Security analyst interview, sample alarm display.
	What form of alarm is used to notify appropriate personnel that a potential attack has occurred, or is occurring?	Alarm/response procedures, IDS settings.
	What types of information are displayed in the alarm messaged?	Sample alarm message.
	What forms of remote alarm notification are used?	Alarm procedures, IDS settings.
	Is email used an alarm notification channel?	Sample email, security analyst interview.
	How are emailed alarm notifications protected from monitoring and blocking by the attacker?	Alternate notifications, encryption, security analyst interview.
	Are generated alarms and alerts reported to a network management system?	IDS settings, sample alerts.
	Are SNMP traps and messages used to post alarms to central network management consoles?	IDS configuration, sample alarms.
	How do network operations personnel service these messages?	Interviews with operations personnel, procedures.
	How is the network infrastructure adapted to respond to a detected attack?	Infrastructure diagram, procedures, configuration.

Additional Tools (optional)		
Topic	**Questions**	**Evidence**
Vulnerability Analysis or Assessment Systems	How are vulnerability analysis systems used to complement the effectiveness of the IDS?	Infrastructure configuration, configurations, application information.
	How is the vulnerability analysis system configured to gather information and provide an accurate "snapshot" of the security state of the system?	Documentation on vulnerability analysis system, sample output, configuration settings.
	How are processing loads split in order to optimize the analysis process?	Configuration settings, interviews.
	Are multiple assessment engines run in parallel to further optimize the process?	Infrastructure diagrams, procedures, personnel interviews.
	How are cryptographic mechanisms used to perform very sensitive and reliable tests of whether particular files or objects have changed unexpectedly?	Configuration, description of mechanisms used, samples of tests.
	Is the vulnerability system host-based or network-based?	Security analyst and personnel interviews.
	How are network-based checks configured to prevent system crashes on the systems they are testing?	Configuration settings, documentation from previous tests.
	How is the vulnerability assessment configured to prevent the IDS from blocking subsequent assessments?	Configuration settings, personnel interviews, procedures.
	How is the vulnerability assessment configured to prevent the IDS from becoming "trained" to the assessments, thus ignoring real attacks?	Configuration settings, personnel interviews, procedures.
File Integrity Checkers	How are file integrity checkers used to complement the effectiveness of the IDS?	Interviews, list of file integrity checkers used.
	Are file integrity checkers used to help determine whether vendor supplied bug patches or other desired changes have been applied to system binaries?	Interviews, system settings, procedures.

Honey Pot and Padded Cell Systems	How are honey pot and padded cell systems used to complement the effectiveness of the IDS?	List of additional tools used, security personnel interviews.
	Have the legal implications of these devices been reviewed thoroughly?	Legal documents, legal personnel interviews.

Deliverables

Deliverables from this audit will include:

1. A summary report with an opinion of the network intrusion detection control environment.
2. Detailed findings with recommendations on addressing areas of residual risk.

Assumptions and Risks

1. It is assumed that all information required for this audit will be made available to the auditor, with client assistance provided as required.

2. Although this audit covers risks identifiable at this time, it is not possible to provide assurances about future control issues in this area.

Key Results

Within the scope of its current architecture, ThisCompany's implementation of IDS has been well planned, executed and monitored. Appropriate standards and guidelines have been utilized for key components such as incident response. The company's use of the technology is relatively new; as such, it is still evolving and undergoing fine-tuning. The results of this audit show that the following points need to be addressed to contribute to an improved control environment within the IT security infrastructure:

- Host Based IDS is not used, which makes it difficult to detect compromises that are not initiated external to the firewall, or those that may have gone undetected by the network IDS.
- The IDS in use is dated and does not provide the functionality and protection of newer tools.
- The incident response procedures do not undergo scheduled testing.

Further detail is provided in the "Detailed Findings" Section of this report.

Priority

Each recommendation has been assigned a priority: critical, high, moderate or low. The priorities have been assigned to provide an indication of relative risk and potential impact. The priority represents an opinion of the Auditor.

Detailed Findings

Subject: Implementation

Observations:

1. The current IDS architecture is network based (NIDS). Monitored hosts are determined by their ability to connect externally through the DMZ, which does not allow for monitoring of servers that are on the 'trusted' internal network. It is not practical to employ NIDS for such purposes. Further, NIDS is not adequate in all cases to detect compromise of systems.[1,2]

2. The current IDS in use at ThisCompany is Netprowler. This tool relies primarily on pattern matching. As such, it is dated and lacks the capabilities of newer systems. It is also somewhat limited in its analysis and reporting functions.

3. IDS is relatively new at ThisCompany. Therefore, not all processes and functions have matured, or have been fully implemented. For example, automated notification is not part of the response procedures.

Recommendations

1. Employ Host-based Intrusion Detection (HIDS) on critical servers.
   Priority: *Critical*

2. Consider upgrading to an IDS that has more powerful capabilities such as stateful matching, protocol analysis and intrusion prevention.
   Priority: *High*

3. Continue to enhance procedures in accordance with established guidelines, such as SANS, within a reasonable timeframe.
   Priority: *Moderate*

[1] Bace, Rebecca. Mell, Peter. "Intrusion Detection Systems"
[2] Northcutt, Stephen. Novak, Judy. Network Intrusion Detection

Subject: Incident Response

Observation:

ThisCompany's IT security team has based its response procedures on respected sources, such as the SANS institute, and has tied them to existing corporate processes like the Major Incident response process. A simulation has been run to test the response process. However, there is not a schedule for periodic tests. Given staff turnover and other variables, it is important that the response procedures are tested on a regular basis to promote familiarity, identify shortcomings, and ensure preparedness in the event of a real incident.

Recommendation:

Establish a schedule for periodic testing that involves all relevant parties.
Priority: *High*

Auditor Observations

This audit was conducted over a period of six (6) weeks to allow sufficient time to interview all relevant personnel and gather information. The high level nature of this audit allowed interviewed parties to provide valuable insight into the structure of the Intrusion Detection System and response procedures. We were able to consult with several levels of authority and responsibility within the company, which allowed us to verify our findings and determine the root cause of our final observations.

Supporting documentation and interview notes have been copied and bound in the Intrusion Detection Review binder (not included with this report). All documentation was referenced with each procedure and observation to ensure completeness. This method was beneficial in ensuring that the full scope of the audit was achieved and that the final results are accurate and supported.

Management has reviewed this audit and agrees with the observations. They will perform analysis to allow appropriate decisions to be made around the issues raised.

Conclusion

The overall audit assessment shows that reportable items identified have control impacts that require action by management to mitigate risk. While the present IDS implementation provides reasonable security, there is room for significant enhancements.

To improve upon the issues identified, we recommend management implement the following:

- Employ HIDS on critical servers.
- Consider upgrading to an IDS that has more powerful capabilities such as stateful matching, protocol analysis and intrusion prevention.
- Establish a schedule for periodic testing that involves all relevant parties.

List of References

1. Northcutt, Stephen. Novak, Judy. Network Intrusion Detection, An Analyst's Handbook, Second Edition. Indianapolis: New Riders Publishing, 2000.

2. Bace, Rebecca. Mell, Peter. "Intrusion Detection Systems". NIST Special Publication on Intrusion Detection Systems. SP 800-31. November 2001.

3. "Information technology – Code of practice for information security management" ISO/IEC 17799:2000(E), First Edition. 12 Dec. 2000.

4. Smith, Gordon E. Network Auditing, A Control Assessment Approach. New York: John Wiley & Sons, Inc. 1999.

5. Proctor, Paul E. The Practical Intrusion Detection Handbook. Upper Saddle River: Prentice-Hall, Inc, 2001.