Interested in learning more about security?

SANS Institute
InfoSec Reading Room

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

Intrusion Prevention - Part of Your Defense in Depth Architecture?

The tools available to IT security professionals are becoming more proactive by attempting to prevent, rather than only detect, exploits from damaging critical assets. Intrusion prevention, in particular, has received a lot of attention in the IT press in the last several years. This paper will explore Intrusion Protection Systems (IPS) from the perspective of using IPS as part of a Defense in Depth strategy. First we will describe Defense in Depth. We will then explore various components of a traditional Defense in De...

Copyright SANS Institute
Author Retains Full Rights

AD

Intrusion Prevention – Part of Your Defense in Depth Architecture?

Bobbi Spitzberg
GSEC Practical, v. 1.4 b
April 3, 2003

© SANS Institute 2003, Author retains full rights

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

Abstract

The tools available to IT security professionals are becoming more proactive by attempting to prevent, rather than only detect, exploits from damaging critical assets. Intrusion prevention, in particular, has received a lot of attention in the IT press in the last several years.

This paper will explore Intrusion Protection Systems (IPS) from the perspective of using IPS as part of a Defense in Depth strategy. First we will describe Defense in Depth. We will then explore various components of a traditional Defense in Depth architecture. This paper will explain the various technologies of IPS. We will conclude with a discussion of what these tools can and cannot do in a comprehension security program.

Defense in Depth

Just as a fundamental cornerstone of IT security is protecting an organization's data confidentiality, integrity and availability, there is a triad to describe how to protect your environment from cyber attacks. This triad is prevention, detection and reaction/response. Defense in Depth is a commonly used approach in IT security to address these principles. The underlying assumption is that no single mechanism offers adequate protection. Defense in Depth utilizes multiple "layers" to protect an organization's critical assets. In other words, an attack that is not stopped by an outer layer will be stopped by an inner layer. Any exploit will have to break through multiple defense layers for it to be successful. Having a Defense in Depth architecture does not assure an organization that it won't be attacked. It does make it as difficult as possible for the attacks that inevitably will occur to succeed. As attacks get more numerous and more complex, organizations need to develop more complex defense strategies.

The first steps in developing a Defense in Depth architecture are to determine what assets to protect, the sensitivity of those assets, and the confidentiality, integrity and availability requirements of the identified assets. In other words, the organization needs to identify its "crown jewels" and how to protect them. Once this has been completed, a risk assessment identifying known vulnerabilities is necessary. This assessment will help to prioritize and target the protection mechanisms to be employed at the various layers of the mitigation plan.

A determination then needs to be made which risks are to be accepted, transferred or mitigated. It is important to note that not all the risks identified in the risk assessment need to be mitigated. Remember that a risk is the "product" of a vulnerability and a threat. For example, a vulnerability may have been identified in the risk assessment, but little or no threat exists to the organization. It is always possible to accept risks if a business case can be made for this action. Once this analysis of the risks to the critical assets has been done, a

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

security plan should be developed detailing the vulnerabilities and threats found in the risk assessment and which ones are to the actions to be taken for them.

If well-defined, well-communicated security policies do not exist, the next step would be to create them. As Bob McKee recommends in his Computer World article (http://www.computerworld.com/securitytopics/security/story/0,10801,78169,00.html) on developing a Defense in Depth architecture, these policies must clearly define the acceptable use of the organization's computer resources as well as helping to assuring that users understand the threats to these assets.

The underlying principle to keep in mind when designing a security program is that something can and will go wrong. Each layer is important. One layer cannot do the job itself. Many organizations think that their perimeter firewalls will do the entire job of protecting the critical assets. A firewall is a good way to implement an organization's network security policy, i.e. what service is allowed to what server. But a firewall does not stop malicious traffic on the allowable ports. Firewall rules are "holes" in the perimeter wall. The more ports (holes) that are allowed through the firewall, the more vulnerable the internal services become.

The layer immediately inside the perimeter firewall in a typical defense in depth architecture would be the Intrusion Detection System (IDS). The typical IDS provides notification that an attack may have occurred. It does not prevent them. But as Eric Cole teaches in the SANS Institute Security Essentials course, "prevention is ideal, but detection is essential."

Intrusion Detection Systems have been around a long time. There have been several distinct approaches – primarily signature analysis and protocol anomalies. These approaches have been evolving to the point where there is currently much overlap (Tanese).

As well as identifying possible attacks, an IDS can help the organization to assess the effectiveness of the firewall rule sets and policies. The typical IDS monitors traffic on the network. They can detect such attacks as SYN floods, port scans, and IRC based attacks. They compare network traffic to know attack signatures and normal traffic structures. Alerts are formulated which require further investigation by the network engineers and systems administrators to determine if an attack has occurred.

Matt Tanese's article explains the ability of signature based IDS to be very specific about the attack. Because of this, they can convey very accurately what the attack is and what it can do. However, this specificity is also a disadvantage. If an attack does not have a signature, the IDS will not detect it, even if the attack is a minor variation of a known attack.

There are known weaknesses in IDS. There are many false positives, which require a lot of resources being used. For example, an alert may be issued for

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

an attack that utilizes known vulnerabilities in the Unix remote procedure call (rpc) services. However, no Unix servers are running in the targeted environment. The typical IDS does not have the intelligence to determine that a host has been patched to prevent the identified attack. If the IDS is dependent on having current signature files, the ability to identify as large a number of attack signatures as possible is dependent on good IDS maintenance procedures. As the number of signatures increases, they may miss attacks on busy networks because of the time spent analyzing packets.

Protocol analyzer IDS can be very slow. This is because of the complexity of the rules and the time to takes to analyze the packet. An advantage of their ability to analyze packets, even though it can be slow, allows them to detect zero day attacks. Since they are looking for generic violations within the protocol (e.g. TCP, IP, UDP, ICMP), they can identify attacks by what they do. This analysis does not depend on knowing exactly how they do it.

The trend in IDS systems is to blend both approaches. This means combining the strengths of each to create more robust intrusion detection. This is also leading to IDS that are becoming similar to prevention offerings.

IDS depend on the network interface of the IDS appliance running in "promiscuous" mode. This means that the device must be able to see all the packets on the wire. Devices that run in "promiscuous" mode are referred to as sniffers. Switched networks are not as easy to "sniff" as non-switched. As Steven Sipes explains in the SANS FAQ on switched networks (http://www.sans.org/resources/idfaq/switched_network.php), switched networks typically do not broadcast the majority of frames on the wire. This means that a network interface running in promiscuous mode, as most IDS do, will only be able to see the traffic between a node and switch. There are methods that are available to pick up traffic on a switched network, such as arp-spoofing.

The defensive layers interior to the IDS may include firewalls placed between externally facing servers such as web servers and email servers and critical assets such as databases. This zone between the 'external' and 'internal' firewalls is often referred to as a DMZ. It is often thought of as an isolated network segment that provides services to the externally facing untrusted systems.

There are multiple ways to protect the host itself. The first line of defense for the host is a standard configuration that is sensitive to security considerations. This is emphasized in the SANS Institute courses on Securing Windows and Securing Windows (www.sans.org). The operating system should be hardened from the time of installation. There are many guides available for installing specific operating systems, e.g. Windows and various flavors of Unix, in a secure manner. Keeping patches up to date is another good practice. There are also various host intrusion detection systems (HIDS). Like network intrusion detection systems (NIDS), host based IDS are reactive rather than proactive. They

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

commonly detect anomalies in login attempts, change in user privileges, changes in critical files, and unauthorized access to applications or files. Typically, they involve analysis of the host log files or determine if critical files have been changed. Like NIDS, they detect the possible attack after it has occurred. They also can use a database of known attack signatures. And as with NIDS, there may be a high level of false positives. Host based intrusion detection systems are the last line of defense. As more and more organizations require external users to connect to their networks using Virtual Private Networks and other encrypted connection methods, the importance of protection of the host at the host becomes more and more important. Access methods that travel the Internet encrypted prevent analysis of the payload at the perimeter. It is only at the host that the majority of the methods decrypt the payload. Only if it is decrypted can the payload be analyzed as a possible carrier of an exploit. Also, by increasing the emphasis on protecting the host, we recognize that most security breaches originate within the perimeter and will, therefore, not be prevented by perimeter firewalls and IDS sensors.

Another important component in an organization's Defense in Depth architecture should be an anti-virus strategy. Protection against viruses can begin at the perimeter with viruswalls, which are analogous to firewalls. Most users are familiar with anti-virus software that runs on their desktop. Antivirus software is also available that runs on servers such as email servers and web servers.

However, as pointed out in a recent Government Computer News article (http://www.gcn.com/vol1_no1/security/21439-1.html), one of the major problems in security today is people and not the technology. Tim Grange of the National Institute of Standards and Technology's Computer Security Division has pointed out that there are many security problems that could only be resolved by training IT administrators to better secure systems. Part of this would include an effective vulnerability assessment policy and associated procedures. Patch management must also be included. These efforts would help to markedly reduce the risks associated with cyber attacks by decreasing the vulnerability component of the risk equation.

It is clear, therefore, that a robust security program should include strong management commitment to assure that systems administrators are trained in cybersecurity best practices. In addition, they need to support and fund programs that will continually assess threats and vulnerabilities to determine the vulnerabilities that need to and can be mitigated. It is important to remember that an organization should not skip the essential steps in protecting itself from cyber attacks. These include: formulating security policies, identifying the critical assets (crown jewels), assigning roles and responsibilities, identifying appropriate network and host controls – including database controls, appropriately utilizing encryption. And let us not forget the importance of patching, training, auditing, logging, and virus protection throughout the enterprise. All of these need to be part of an organization's Defense in Depth strategy.

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

It sometimes appears easier to invest in the latest technology solution than to perform the steps we have articulated. Currently that technology is intrusion prevention.

Intrusion Prevention

Behavior Blocking versus signatures

Most anti-virus and IDS systems use signatures (patterns) associated with known attacks to determine if incoming traffic is malicious. This means that the attack must be known before it is stopped. The advantage of blocking traffic based on its behavior is that an organization's critical assets can be protected on zero day when the attack mechanism is still unknown. Behavior blocking involves allowing what appears to be legitimate traffic while blocking malicious traffic. Rules are formulated that define this legitimate traffic. Traffic that does not match the rules in the profile is considered to be atypical and probably malicious. This will trigger a reaction from the product using behavior rules. For example, a rule may have been formulated that says that the only process that is allowed to access web server files is the web server process itself. If any other process attempts to access a file, such a rule would trigger a response from the tool.

The specificity of signatures is their distinct advantage. This not only helps to eliminate false positives and negatives, it also helps the administrator to determine the course of action to be followed. The disadvantage of signatures is that they cannot protect against unknown attacks. Their effectiveness is dependent on the vendor supplying new signatures quickly and accurately. Of course, the user must have a means for updating signatures.

The main advantage of behavior blocking is the recognition of previously unknown attacks. Attacks can be recognized by the methods used to gain control of a targeted host. Also, because attack behaviors are more generic and much more of a known, they require less maintenance from vendors and users.

Users of behavior blocking tools must be aware that even though they do not have to be concerned about regularly updating signatures, they need to be aware that rules need to be evaluated regularly for their appropriateness and effectiveness. It is important to know that this method is not as accurate as signature analysis because it is less specific. The biggest advantage of behavior blocking is that this approach protects assets on unpatched hosts from attacks when they are not still unknown and before signatures have been formulated. Many organizations cannot patch production servers frequently.

Why not combine the two methodologies? As would be expected, this approach combines not only the advantages, but also the disadvantages of signatures and behavior blocking. In theory, a combined approach should help in eliminating false positives and negatives.

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

Having both signature and behavior rule formulation in one tool requires a lot of knowledge from both the tool vendor and the user. Although many of the behavior tools such as those from Intruvert and Okena have been reported to have successfully prevented SQL Slammer from affecting customers, it would be premature to view these tools as a panacea. Also, only one major vendor, Entercept, offers a combined product at this time.

At the perimeter

It is easy to assume that Intrusion Prevention Systems (IPS) are proactive IDS and work mostly at the perimeter as an NIDS would. As we explore the various tools that are classified as IPS, we will see that IPS appears at all the layers in the Defense in Depth model.

IPS at the perimeter use multiple methods as they operate in the data path. They can drop packets that they identify as being part of an attack. Some IPS products at this layer use protocol analysis, even creating a virtual TCP/IP stack that will reassemble packets in order to determine to allow or disallow the traffic. ISS Real-Secure Guard is an example of this (http://www.iss.net/products_services/enterprise_protection/rsnetwork/guard.php).

IntruVert Networks' products provide signature, protocol anomaly and denial-of-service protection. They claim that they were able to successfully block SQL Slammer before a signature for this attack was available (http://www.intruvert.com/products/index.htm .

The products in this category all appear to combine attributes of both firewalls and NIDS sensors. The greatest challenge for this class of tools is to allow legitimate traffic while blocking attacks and do this without adversely affecting performance. These products are typically appliances.

Present day attacks spread at tremendous speed. These fast moving attacks can infiltrate a network before conventional tools such as anti-virus software have time to formulate a signature to prevent infection. IPS appliances, with their behavioral analysis and speed, operate fast enough to detect such attacks without performance degradation.

Web Server IPS

An organization's web servers are not only the way an organization portrays itself to the Internet world, but also a major Achilles heel. Many attacks use port 80, the standard HTTP port. Since a web server is often a conduit to the backend database server, it is essential that it be protected. There are two types of Intrusion Prevention Systems specifically designed to protect web servers. These are web server shields and web application firewalls.

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

With web server shields, you can customize how you control the components and functionality of the web servers you choose to "wrap". Most of the tools in this category either plug into the server or monitor its activity. They are designed to protect against buffer overflows as well as specific attacks associated with web servers such as parser evasions and directory traversal. Another method used is to lock down files that allows the application to run as a "virtual root" account that has limited access to the server.

Another type of IPS used to protect web servers is a web application firewall. These are deployed at the perimeter. Web application firewalls look for possible attacks that are specific to attacks on browsers and web servers. Such potential attacks would include, for example, attacks on data, which might employ special characters or wild cards to change data; logical content attacks on command strings or logic statements; and attacks which might target files or accounts on the server hosting the web application (Bar-Gad). They are designed to protect the applications and data in addition to web servers. These tools need to have what it is referred to as "session awareness" so that they can protect the server from cookie poisoning, attacks against the database itself from the web application. These tools are capable of automatically learning and building rules to increase the protection provided to the server. There are many tools in this category.

Host Based Intrusion Protection Systems (HIPS)

The following sections will give an overview of several types of IPS that are host-based. We will not provide a detailed product analysis. Examples of commercial HIPS are given only to illustrate the variety of HIPS that are commercially available.

HIPS -- Trusted Operating Systems

Trusted Operating Systems (OS) are nothing new. The concept dates to the early 1980's. There are four requirements or principles that comprise a Trusted OS. PitBull has an excellent White Paper on Trusted Operating Systems (http://www.argus-systems.com/product/white_paper/pitbull/oss/2.shtml).

The requirements for a Trusted OS are:

- Information compartmentalization. This is also referred to as Mandatory Access Controls (MAC). It restricts the information that any one user can access. Normally Unix uses Discretionary Access Controls (permission bits and access control lists). The key point here is that root is **not** exempted from these controls. The premise is that compromise in one application cannot be utilized to compromise another.

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

- Role compartmentalization. This is Role Based Access Control (RBAC). This restricts the functions that any one user can perform. No one user has full control. There is no superuser (root) in a Trusted OS.
- Principle of least privilege. This restricts what processes can do. A mail server could not access the database engine's configuration files, for example. The process has only the privileges it needs for its particular function.
- Kernel level enforcement. This ensures that security is performed at a basic enough level that it cannot be bypassed at the user level. Access decisions will precede the application's actually accessing anything.

Trusted OS can be a special version of the Operating System. Examples of this are Sun Microsystems Trusted Solaris (http://wwws.sun.com/software/solaris/trustedsolaris/index.html) and Hewlett-Packard's VirtualVault. Implementations such as PitBull Foundation can exist with commercial Operating Systems.

Trusted OS vendors claim that by compartmentalizing applications malicious attacks are prevented from gaining control of multiple applications, even when they control one application on the attacked host. This is because they use sensitivity labels, which are independent of the user ID and cannot be overridden by root. It should be noted that Trusted OS can make administration very difficult. An administrator who did not have access to a particular component might think it had crashed because (s)he couldn't see it (Scheier).

HIPS -- System Call Blocking - Okema

Okena's StormWatch (http://www.okena.com/areas/products/products.html) protects Windows NT/2000 servers and desktops by intercepting system calls. Okena, which has recently been purchased by Cisco Systems, Inc., uses behavioral rules to determine if the system call represents appropriate or acceptable behavior for a particular application. The fact that Cisco has entered this market and purchased Okena is significant information about how positively IPS is viewed by established IT corporations.

The product consists of four modules that individually intercept four types of system calls. These modules are the file interceptor, network interceptor, COM interceptor and registry interceptor. It has about dozen out-of-the-box policies for such common servers as Microsoft IIS, Microsoft SQL Server, DNS and DHCP.

For standard applications as well as custom applications, StormFront uses data collected by StormWatch on the application's behavior. This behavior is analyzed in order to develop operating security policies. In other words, StormFront "learns" an application's normal behavior and develops an initial policy based on behavior that has been learned previously. This initial policy should still be reviewed and modified by the appropriate staff. Through this

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

mechanism it is, therefore, possible for an organization to develop policies for custom applications as well as applications that are not provided by Okena. The Okena architecture is called INCORE (INtercept COrrelate Rules Engine). The architecture is purely behavioral. No signature analysis is done, nor is access based on user or group identification. Policies can be updated by means of a management console, which interfaces with the rules engine. The rule engine, in turn, can communicate alerts and log data back to the management console.

System Call Blocking - Entercept

Entercept's products use a combination of both behavioral rules and signatures (http://www.entercept.com/products/entercept/index.asp). Also, it supports more platforms than does Okena (http://www.entercept.com/products/entercept/prodinfo/requirements.asp), most notably Unix platforms such as Solaris and HP-UX. The web servers supported are IIS as well as Unix based web servers such as Apache. Entercept's products are primarily for the protection of servers, including specific products to protect web servers and Windows database servers. Although it supports more Operating Systems and web servers than the Okena products, Entercept is actually more limited. A user is limited to the supported applications. In order to support commercial and custom applications, you would need to contract for professional services. It is, however, possible to change certain automatic protections by creating exceptions to established rules. This is done by using a rules wizard. Users and groups can be defined that are allowed to do modifications to the support servers. For those supported applications, it is easy to install and configure.

Entercept (http://www.entercept.com/whitepaper/vulnerabilities/), which uses both signatures and behavior blocking, claims in a White Paper on its products that they address the majority of the Top 20. Host based IPS can indeed protect critical hosts from attacks that utilize such well-known vulnerabilities as those in Windows systems from the SANS Top 10 for Windows – Internet Information Services (IIS), Microsoft Data Access Components (MDAC), weak hashing, unprotected shares (NETBIOS), protect against null sessions, buffer overflows.

Entercept also can protect against buffer overflows on Unix systems. This would prevent buffer overflow exploits, for example, in rpc (remote procedure calls) services, sendmail, bind, the printer daemon, and sadmind/moutd. Entercept can also protect hosts from vulnerabilities introduced by default installs of operating systems and applications. Its use of behavioral rules to define accepted and prohibited behaviors can prevent even root exploits that target these default settings. CGI exploits are also prevented.

What these tools can and can't do

Many of the SANS Top 20 vulnerabilities (http://www.sans.org/top20)

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

can be easily mitigated by comprehensive security policies that clearly articulate the required procedures including the ability to track that the procedures are indeed followed. If systems were configured securely from the start, patched regularly, and had strong authentication, most of these common vulnerabilities would be eliminated within the organization. The SANS Institute in its introduction to the Top 20 List states that most successful attacks against operating systems can be attributed to a few vulnerabilities. These vulnerabilities appear again and again on the Top 20 list because organizations continue to fail to mitigate them and consequently, attackers continue to exploit them. Indeed attackers rely on the fact that organizations are not fixing these well-known problems. SQL Slammer is the most recent example of this. The widespread attack that occurred the weekend of January 25 through January 26, 2003, took advantage of vulnerability that was not well known, but for which a patch had been issued six months previously. Another factor that contributed to the large number of servers that went down is that many sites fail to cover up such vital information for the attacker as the operating system and the web server software that is installed.

How many of these tools an organization chooses to incorporate into a Defense in Depth strategy is dependent on the financial resources available as well as how these tools fit into the existing security program. They should not be a substitute for security best practices.

Conclusion

Perhaps the biggest contribution of the attention that these tools are receiving is that they are raising the issue of better protection of the host. Too many organizations have assumed for too long that they are adequately protected because they have installed a firewall at the perimeter. The attention that Intrusion Prevention Systems are getting help to draw attention to the “soft center” behind the crunchy outer shell represented by firewalls.

IPS tools can address and prevent intrusions resulting from most of the common vulnerabilities. These continue to be the “Top 20” because hackers know that most organizations have not fixed them. Hackers continue to scan the Internet for organizations and hosts that may be vulnerable.

As part of a strong Defense in Depth policy, organizations must still formulate policies and procedures to ensure that accounts have strong passwords, that full backups are taken regularly, that only necessary ports are open as well as assuring that only properly addressed packets leave and enter through the firewall. IPS cannot make up for not having proper logging and auditing.

Which tools should we use and where should we use them if money were not a factor?

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

Certainly some blocking features should be employed at the firewall or within an IDS system. Integrating an IPS tool and/or incorporating blocking capabilities into an organization's existing IDS architecture is desirable as well as being a relatively inexpensive hardening of this layer in the Defense in Depth strategy of the organization.

These products are complicated and will work well if configured well. An organization cannot eliminate the hard work of knowing what they do, how they do it and what they need to protect. This technology should also not be viewed as firewalls have been viewed in the past. In other words, once an organization has an IPS, or even multiple Intrusion Prevention Systems in place, they can omit review and reevaluation of what they do to protect their "crown jewels."

Malicious code is designed to run on hosts. Their mission is to make a request to the Operating system on the targeted host. IPS, with their behavior blocking designs, will intercept and block these malicious requests. This blocking can be done at the perimeter, the host, or in between – wherever the IPS is running. As we stated earlier, as more and more organizations move toward encrypted access, e.g. Virtual Private Networks (VPN), Secure Server Layer (SSL) and secure shell (ssh), the importance of analyzing traffic within the perimeter becomes more important. Some of these access methods are only decrypted by the application.

Intrusion Prevention Systems offer great promise. Before they are widely accepted and deployed, several improvements need to be made. They, like their Intrusion Detection precursors, generate false positives. For an IPS, this means more than investigating extraneous alerts. It means blocking legitimate traffic. These systems still remain difficult to administer and are not yet fully scalable. There is also the performance problems introduced by the IPS that intercept system calls on the host themselves. This causes an additional load on the Operating System that translates into decreased performance. Also, it still needs to be determined if the vendors of these products are targeting the majority of the threats that are most likely to occur.

Securing an organization's critical assets is not easy. No magical, easy solution for eliminating today's risks exists. An organization still needs to have a security plan, risk assessments, vulnerability assessments, penetration testing, and patch management in order to identify its specific risks and to mitigate them or accept them. Intrusion Protection System can certainly assist in protecting you from zero day attacks and give you time to further harden your environment. It is important not to rely on these tools to the point where Security Best Practices are not followed.

William Jackson's recent article in Government Computer News says that security is fundamentally a people problem. Security breaches, even with the most accurate Intrusion Prevention Systems, will continue to occur. The majority

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

of security problems are management issues. Those issues will not be solved by technology – no matter how sophisticated it becomes. Trained security professionals remain the best intrusion protection investment that an organization can make.

© SANS Institute 2003, Author retains full rights

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

References

Argus Systems PitBull Foundation Product White Papers. "OS-Level Security: Trusted OS Security: principles and practice". URL: http://www.argus-systems.com/product/white_paper/pitbull/oss/2.shtml. (April 3, 2003).

Bar-Gad, Izhar. "Web application firewalls protect data". NetworkWorldFusion Magazine. June 3, 2002. URL: http://www.nwfusion.com/news/tech/2002/0603tech.html. (April 3, 2003).

"Cisco Systems to Acquire Okena, Inc.: Acquisition Extends Cisco's Network Security Portfolio with Next-Generation". January 24, 2003. URL: http://newsroom.cisco.com/dlls/corp_012403.html. (April 3, 2003)

Cummings, Joanne. "The People Side of Prevention". NetworkWorldFusion. September 23, 2002. URL: http://www.nwfusion.com/buzz/2002/intruderside.html. (April 3, 2003).

Entercept Security Technologies. URL: http://www.entercept.com/products/entercept/index.asp. (April 3, 2003).

Harrington, Chad. "Defense in Depth: Combining Behavioral Rules and Signatures". URL: http://www.entercept.com/products/entercept/whitepapers/downloads/defenseindepth.pdf (April 3, 2003).

IntruVert Networks. "IntruShield Product Family". URL: http://www.intruvert.com/products/index.htm. (April 3, 2003).

Hulme, George V. "Intrusion-prevention tools prove themselves by stopping worms like Slammer in their tracks". Information Week. February 3, 2003. URL: http://www.informationweek.com/story/IWK20030202S0002 (April 3, 2003).

Jackson, William. "Experts repeat: Security is a people—not technology—problem". Government Computer News. March 18, 2003. URL: http://www.gcn.com/vol1_no1/security/21439-1.html. (April 3, 2003).

Karagiannis, Konstantinos. "Get Real Intrusion Prevention". PC Magazine. February 1, 2003. URL: http://www.pcmag.com/print_article/0,3048,a=35232,00.asp. (April 3, 2003).

McCormick, John. "'Naked' federal sites are open to attack". Government Computer News. February 24, 2003. URL:

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

http://www.gcn.com/22_4/security/21214-1.html. (April 3, 2003).

McKee, Bob. "What it takes to develop defense in depth". Computerworld Magazine. February 04, 2003. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,78169,00.html (April 3, 2003).

OKENA INCORE (INtercept COrrelate Rules Engine) ARCHITECTURE. URL: http://www.okena.com/Areas/Products/products_incore.html. (April 3, 2003).

Rudzonis, Brian C. " Intrusion Prevention: Does it Measure up to the Hype?". GIAC/GSEC practical. October 24, 2002. URL: http://www.giac.org/practical/Brian_Rudzonis_GSEC.doc (April 3, 2003).

SANS Institute. URL: http://www.sans.org/. (April 3, 2003).

"SANS Institute: SANS/FBI Top 20 List". Version 3.22 March 3, 2003. URL: http://www.sans.org/top20/. (April 3, 2003).

Sipes, Steven. "Intrusion Detection FAQ: Why your switched network isn't secure". September 10, 2000. URL: http://www.sans.org/resources/idfaq/switched_network.php (April 3, 2003).

Tanase, Matt. "The Great IDS Debate: Signature Analysis Versus Protocol Analysis" Security Focus ™. February 3, 2003. URL: http://www.securityfocus.com/infocus/1663 (April 3, 2003).

"The SANS Institute's Top Twenty Most Critical Internet Security Vulnerabilities: Coverage Analysis by Entercept Security Technologies". URL: http://www.entercept.com/whitepaper/vulnerabilities/ (April 3, 2003).

"Trusted Solaris Operating Environment". URL: http://wwws.sun.com/software/solaris/trustedsolaris/index.html (April 3, 2003).

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

Last Updated: June 18th, 2013

Upcoming SANS Training

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

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**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**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 Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**