Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)
GSEC Certification Paper – Research on Topics in Information Security

All Sewn Up: Intrusion Detection in the Network Fabric

Adam D. Crooke
2002

Assignment Number: 1.4

Abstract

Even as far back as twenty years ago Intrusion Detection Systems were being used, albeit more log analysers than anything else. Since then, IDS has become an essential weapon in the security arsenal of any company wishing to conduct business on the Internet. There are two types of IDS: host and network. Both obviously have their advantages, but both equally have their shortfalls. The current popularity of switched networks has made network intrusion detection far more difficult, a switch limits the placement of the detection system and the amount of traffic it can see, decreasing the granularity of the analysis.

By combining the two onto the switch fabric allows monitoring of traffic directly to hosts, yet without residing on hosts, as well as encompassing overall network visibility. This can be achieved by integrating IDS within the network on the access layer – most typically nowadays a switch. This brings many benefits over the current host and even network based IDS. Notably speed, ease of use, and security becomes a part of the network, as opposed to an "add on". However, no matter how good an IDS solution is, it should not stand-alone, and should complement other security applications as well as build upon an understandable, supportable and realistic security policy.

Introduction

First build the network – then secure it. This has long been the traditional step; sometimes security is simply an afterthought, rather than a necessity to consider and build into a network design. Companies have realised that e-commerce is a business enabler and are now beginning to equally focus on securing the transactions and data stores, as well as increasing revenue through e-commerce.

Sadly, security has suffered at the hands of economics and many companies are reluctant to use amounts of their budget that is necessary to properly protect their network. Upper management are often blind to the need for adequate security measures to be implemented, until they are the focus of an attack and they realise how much revenue can and will be lost through malicious attacks on their network. Only when the balance sheet shows how devastating an attack can be do management give their blessing to adequate security measures.

The main protection that a network needs is from the Internet. Before the Internet was so prevalent in our homes and offices and was known as ARPANet computers were linked via standard voice telephone lines and as such attacks tended to be localised to the particular machine and also from a local source (after all, international calls were, and still are expensive). Now that the Internet consists of millions of computers connected via a network of high speed dedicated data lines the attack can from anywhere in the world and because of the depth of knowledge that can be accessed effortlessly even a disgruntled ex-employee with very little computer knowledge can search for "Hacking tools" and begin an assault on a companies network with devastating results. Attacks on a companies network can consist of many different types through many different access mechanisms, whether it is through email, web sites or social engineering, any of these methods can then propagate attacks such as worms, viruses, trojans, denial of service or even hoaxes. Any of these attacks can be devastating for a company from anything from loss of face, to loss of revenue, such is often seen in denial of service attacks. From this it is easy to see that there are so many different types of attacks to legislate and protect against and there are more and more appearing each day.

There are many approaches to information security and a complete solution would be to use a balance of all these technologies and practices. If a company does nothing else to protect its network it should at least implement a firewall. These do not alone make for secure networks; firewalls can, and often are circumvented by very trivial methods. They simply do not provide the whole solution. So, other technologies and methodologies are essential for a secure network.

A typical enterprise network consists of two attack vectors: the outside (a very large attack space), the other from the inside. While insider attacks can very effective because the attacker may know the systems and people involved and know how best to attack the system, an external attack can be just as devastating, if not more so, especially because the attacker can be so difficult to catch because of the anonymity of the Internet. Firewalls are a good way to prevent SOME external attacks by protecting traffic coming into the enterprise network from the outside. It is by no means a stand-alone solution to network security. One other such popular technology that complements firewalls is Intrusion Detection Systems (IDS). These applications

can perform one vital function (amongst others) firewalls cannot: protection from the inside. Not only this but prevention is better than cure – IDS are a big step to identifying an attack even before it has even begun. As Illena Armstrong says: "For the most part, the corporate world is generally acknowledging that intrusion detection systems of some sort must be deployed." [1]

There is no doubt that security is rapidly becoming not just a necessity, but also the prime focus within a company's information systems strategy. Fast spreading threats underscore the continued importance of not only detection, but also speed in minimising the impact of malicious code on e-business today. The LoveLetter worm, which hit in May 2000, quickly infected millions of email messages and was estimated by Computer Economics to have cost $8.7 billion. Next came Code Red in August 2001, which cost approximately $2.6 billion, followed by Nimda the following month, which infected more than 2.2 million servers and PCs in just 24 hours. This is just a small sample of attacks that gained high profile exposure due to the financial damage that they inflicted, but there are many types of attacks that an organisation could experience and many types of hardware that are targeted. IDS works on the host and network level and these form the basis for the most common attacks. A host is open to many different types of attacks, but so is the often-overlooked network. These can consist of *Address Resolution Protocol* (ARP) and *Media Access Control* (MAC) layer 2 attacks as well as *Distributed Denial of Service* (DDOS). It is just as essential to protect the way the network operates as well as the individual hosts themselves.

For any type of IDS to be effective it is important to remove "false positives" (alarms on legitimate traffic) as well as, of course: "false negatives" (attacks the IDS fails to see). It is important to configure and fine-tune the IDS for the particular application that it is required for. Obviously the boundaries blur somewhat when implementing IDS within the network fabric and this is an important consideration when examining this solution.

There are two steps to this threat mitigation – first is to identify the alert as a legitimate threat and then go on to take steps against it. This first step is perhaps the most important stage of choosing and configuring IDS, and those choices will depend on budget, application, time, and resource availability. The description of integrated IDS in this paper will take into account all these factors, and it is understood that this will not be suitable for all organisations while there are also other solutions and possibilities.

Twos Company…

Now we can see the importance and use of IDS it has traditionally become necessary for companies to choose not only the IDS vendor, but also the type. The dilemma faced by businesses, especially those with tight IT budgets is one of IDS choice. Two types exist: Network and host based. There are many different network based IDS software packages around, ranging in prices, and consequently – features. Two worthy of note due to their popularity are Snort [2] and ISS RealSecure [3]. Both are moderately easy to configure but they do have limited speed and traffic capabilities when compared to host based IDS such as TCP

[1] Armstrong, pp. 32
[2] http://www.snort.org/about.html
[3] http://www.iss.net/products_services/enterprise_protection/rsnetwork/sensor.php

Wrappers and TripWire[4].

Implementing a network based IDS in a switched environment is difficult because of the way a switch behaves. A switch sets up a virtual circuit between two hosts, and traffic designated for these hosts travels through this circuit and is not received by anybody else. This makes network IDS practically impossible because promiscuous network cards will sniff with no results. At present there are several solutions to this. The first is a "tap" which can intercept the traffic before it reaches the switch or host, which means that many taps may be needed depending on the network structure (e.g. four different VLAN's). Most switches have spanning ports that are used to carry traffic between VLAN's, an IDS could be attached to this, however only one port can operate as a spanning port on each switch and the port does not always send 100% of the traffic which could mean an attack could be missed. One other option is of course to use a hub, but that really negates all the advantages that come with using switched networks, as well as the fact that the ubiquitous switch is so well relied upon, and brings so many advantages to a network administrator that most of them would not wish to give them up!

It should also be noted that VLAN's by themselves are not suitable ways to secure internal networks and should not preclude the use of internal network or host IDS. Implications say that it is possible to inject 802.1q frames into non-trunk ports, and have data delivered to a destination by enabling traffic to "hop" from one VLAN to another, if a port belongs to the native VLAN of the trunk port (if source and destination are on different switches). As well as this, human error and the fact that VLAN's were not designed with security in mind, makes them inadvisable security methods for protecting an internal network.

Therefore it becomes apparent that switches and IDS are enemies - but not if they are built together.

A Proposed Solution?

Switches are becoming so prevalent within companies' networks – it is just not economical to purchase hubs instead of switches. They also bring with them many benefits for the network administrator, not least segmenting the network - reducing the collision domain and subsequently vastly improving the traffic speed and flow thus enabling devices to operate more efficiently – at least all those apart from a Network based intrusion detection system!

Network devices are becoming more intelligent – they can now control as well as authenticate and authorise. Why not build the security into the network and make it inherently more secure? One step towards this is the ability to monitor the network using the network itself. Without necessarily completely redesigning TCP/IP, it is possible to build IDS into the network fabric. More specifically IDS residing at the network and data link layer on access points such as the switch. The ubiquitous switch is so common that most network designers and administrators would be lost without one! It is therefore sensible to bring the IDS and switch together in the network environment to create a synergistic network enabling superior connectivity as well as high security.

There are however, factors to consider when integrating any devices together: "[companies]

[4] http://www.tripwire.com/products/servers/features.cfm

need to choose between using integrated functionality in a network device versus using a specialised functional appliance. The integrated functionality is often attractive because you can implement it on existing equipment, or because the features can interoperate with the rest of the device to provide a better functional solution." [5]. Decisions also need to be based on capacity and functionality – while it is possible to buy an integrated router and firewall it may not be practical from a management point of view, and can hamper the flexibility of the network. Having said that, by building IDS into the hardware itself, comes many advantages; the most notable is speed (this and other benefits are discussed in a later section). By building a switch chassis that can house IDS cards or modules would make a far neater unit aesthetically and from an administration point of view, as well as logical clustering of network devices.

Security considerations on the device:

Switches, like any network access point should always be secured, but in practicality are often neglected and can be used by attackers as a springboard for further attacks. Some points to consider and follow are outlined below, these are relevant whether an IDS resides on the switch or not!

Switch all trunking ports off that are not needed, rather than leave ports set to "auto". This will prevent a host from becoming a trunk port and receiving all the traffic normally apparent on a trunk port. In fact, why not configure the IDS to pick this up – this would certainly only be possible with an integrated solution. As well as this, it is also advisable to disable all ports that are not required for connectivity at all. Cisco also recommends [6], based on work from SANS to make sure the trunk ports that are configured, do not use the same VLAN number as anywhere else on the switch. This prevents the problem mentioned earlier in this paper with regard to traffic inadvertently crossing VLAN's without firstly crossing a layer 3 device (i.e a router).

A simple security device that is wroth considering is Private VLAN's (although this feature may not be available on older devices) – these allow restricted connectivity between hosts. This is an advantage such that if an attacker compromises a remote host, they are unable to then move onto to other hosts outside the private VLAN. Each host would typically be assigned their own private VLAN. IDS on the switch could still perform its operations by enabling ONE promiscuous port for which the IDS could use to scan all the individual VLAN's. This would of course the only port that has full access to all of the private VLAN's. This also means that only one IDS is required and an in-line solution would be that much more difficult for an attacker to comprises because of its virtual invisibility to any other devices on the network.

Current Implementations:

[7]There have been companies that have implemented IDS within the switch; one notable offering is the Catalyst 6000 Intrusion Detection System Module from Cisco. It works in a similar way to the Cisco Secure IDS Appliance Sensors - in that it detects unauthorised activity traversing the network. It is

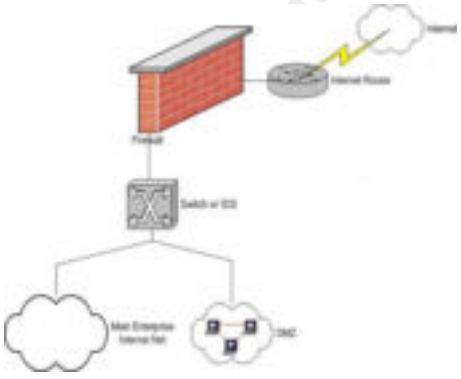
[5] Convery & Trudel, p 3.
[6] Convery & Trudel, p. 5
[7] Catalyst 6000 Intrusion Detection System Module

configured using the Catalyst OS and the VLAN access control list capture feature, or SPAN functionality and it does allow for quite granular traffic monitoring.

The card above is Cisco's only offering in the in-line IDS range but is still useful for benchmark tests and general comparisons with the more traditional IDS offerings not just from a logical but also a physical point of view. This is certainly one of the physically smallest IDS available. A traditional IDS system would require a hardware system such as a server that would be at least one or two "U" high and would then require the operating system and then the IDS software itself. With Cisco's offering the whole package is a one or two "U" system requiring no operating system or software installation whatsoever apart from the Catalyst O/S that is already running on the switch.

One of the problems with traditional IDS is not so much the level of detail; it is the speed in which the detail could be examined. Especially when monitoring heavily utilised services such as e-commerce web sites. Should a denial of service attack occur with a service like this, it could realistically cost companies millions in revenue, it is because of this that it is very important to maintain the availability of services like this. Integrated cards within the switch - monitoring the network traffic real time can be considerably faster than their static rivals. "The Catalyst switch family, for example, enables the use of up to eight 150-Mbps IDS line cards for gigabit-per-second traffic monitoring." [8] It has over 300 signatures (patterns of known network misuse) and uses these analyse the traffic that it copies before it leaves the switch meaning that users do not experience a slow down when connecting to these particular services that are being monitored. Using the Cisco integrated IDS gives some concrete performance results that are only possible with an integrated solution. The IDS line cards in a Catalyst 6000 can monitor 100 Mbps of traffic at approximately 47,000 packets per second, with a new flow arrival rate of 1000 per second. Compare this to current network IDS boxes, which limit to about 80 Mbps fully loaded[9]. This speed requirement will clearly be even more necessary for an enterprise network as companies begin to roll out high speed switched networks of 1GB or more.

Benefits



The diagram on the left shows a typical simplified small enterprise network, and shows how an integrated switch/IDS solution fits into the architecture. The switch could of course be sited anywhere desired within the network depending on the type and amount of coverage required, however it is certainly better to site the equipment at the distribution or access layers (to quote Cisco network architecture). In this example the integrated switch/IDS is being used to monitor both the DMZ (which most likely contains public/Internet facing web servers, mail servers etc) and the private corporate network (most likely consisting of internal infrastructure services and end user nodes) on different segments. Obviously this setup is very flexible and demonstrates a major benefit of using an integrated solution. It is

[8] Wexler, p. 61
[9] SANS – Security Essentials 1.1, p. 85

completely independent of the platform(s) it is monitoring because it simply analyses the traffic, and does not run as a process on an individual host. It is also important to note that the IDS visibility to an attacker becomes less clear, and coupled with the use of honeypots (a decoy server designed to attract the attacker away from the production server) can mean an attacker will find it almost impossible to locate and disable the IDS and to evade detection. With this forming part of an integrated end-to-end solution forms an effective, defence in depth security strategy to complement other deployed security mechanisms (firewalls, encryption, authorisation etc.). As well as conserving rack space, the integrated solution provides uniformity across the network and is completely end node platform independent.

Bandwidth on a typical corporate network (such as the one in the example above) will probably always exceed the network detection and processing speed of traditional network and host based IDS. But a significant speed gain is realised with an integrated solution allowing less dropped packets and an increase in attack recognition. This provides a transparent IDS operation to the end user, network administrator and the attacker! Not only this but an integrated switch solution provides a platform to monitor multiple VLAN's simultaneously (both ISL and 802.1q), which enables a very granular view of network traffic patterns, while there is only one box to look after. The box can of course be managed and monitored with the usual tools by using SNMP or any desired protocol, as well as the IDS unit logging to syslog, or any other logging utility. This helps to bring down the total cost of ownership of an integrated switch/IDS box to the point that enables companies to deploy many throughout their switched network.

Other applications

As network access and carrier technology gets faster and more advanced, the switch may be replaced just as it has overshadowed its predecessor: the hub. Within the next few years we will certainly begin to see more wireless LAN (WLAN) access points. This brings more interesting challenges for the IDS – a full investigation of which is outside the scope of this paper. As WLAN's become more prevalent, so the doors to the network become bigger and the wider those doors can be opened. Many within the security domain have seen WLAN's as a huge security risk, especially since the many stories in the press of drive by hacking or war chalking* simply for something as relatively harmless as free Internet access! Because of this WLAN's have been rather unfairly given a bad press. Like most security lapses and holes it is due to company and/or personnel mis-configuration and an uneducated use of the technology. Using encryption and non-advertising network ID's make the wireless network impossible to even detect, let alone connect and decrypt traffic.

While WLAN's do increase the complexity of the network, their wireless access points do make a logical location for IDS, and a natural synergy between access points and switches. As WLAN's become more prevalent I think we will begin to see a harmonious mixture of integrated WLAN access points and switches working together as access mediums for end users as well as the first stop for security and attack detection.

So it is possible to see that as network access and carrier technology progresses, so does the software and hardware that monitors and guards against attacks. Whatever access

* Marking a geographical area where unauthenticated WLAN access can be obtained.

technologies are adopted, the ubiquitous IDS will almost certainly be ever present in the armoury of weapons in the war against hackers.

Conclusion

An integrated switch/IDS solution certainly has many benefits as discussed, it should be noted that it doesn't replace host based intrusion detection (which are still certainly useful for "low and slow" attacks), but with newer and faster technology it will certainly improve, and perhaps replace both IDS approaches that are used now. This can only happen by better support from vendors and suppliers who are willing to push integrated solutions, and of course on whether companies see the benefit in real terms to their network strategy as well as, of course economic viability.

Should a company decide that an integrated solution offering is suitable for them by examinig the factors above, they would find that there are currently very few offerings and choice in integrated IDS solutions. This is in the major part the reason why they are so uncommon within the enterprise. This is a vicious circle, the only major vendor that provides a solution is Cisco through their catalyst range of switches, and it is only a very limited range that supports the in-line IDS cards. The problem is also proprietary hardware, which can dissuade companies from investing in technology, especially if the support infrastructure isn't available. With lack of choice there is no competition, and so no motivation to improve. And for companies to seriously consider purchasing these systems they need choice, and most of all they need to be cheap, at least comparatively when looking at host based IDS, which can be prohibitively expensive, as well as a logistical nightmare (time and resources) when deploying many nodes. It is also important that this integrated approach does not lead to proprietary technology. For technology to mature and advance, an open system is needed. For this to happen standardisation is required. There is already some work in this area in the form of "The Intrusion Detection Exchange Format Working Group" from the IETF that has been setup for this purpose. They are responsible for the creation, regulation, and advancement of standards on the Internet (initially in the form of an RFC document) for protocols for exchange of information between Intrusion Detection Systems. This is beneficial for the advancement of IDS in general, and specifically with regard to communications between different systems, this will certainly facilitate the growth of IDS and specifically, integrated IDS within the enterprise.

Another problem for IDSs is that historically "signature update" has always been logistically difficult, and yet paradoxically is essential for adequate pattern matching to take place, and for the IDS to be of any real use. This does mean that an integrated solution needs to accessible and easily configurable like many existing systems this is a priority for some companies with limited resources and skill sets. While a signature update utility is essential and is usually facilitated via a front end, it is synonymous with host based IDS, but could be more problematic with an in-line integrated solution. Clearly a distributed model would be preferred, more of a client/server architecture delegating the configuration front end duties to a management station where the configuration would take place and then be "pushed" to one or many client IDSs running on one or many switches in the enterprise. This is a popular approach and can be seen with many appliances, such as Checkpoint's Firewall-1/VPN-1 packages. Built into this, strong authentication is needed, not only at the management station for connection and configuration, but also for pulls/pushes with signature updates and configurations to the client IDSs (which could come from local servers within the enterprise or from a vendors Internet site).

This type of architecture would free human and network resources. This is particulary important in continually overstretched IT/IS departments. Normal IDS requires system resources of the box that it runs on, which of course so does an integrated solution. The difference however is that the IDS is implemented within the hardware, which in itself shows massive speed increases, while the signature updates are stored, and updated (via the network) in firmware (see Current Implementations section). Regular IDSs are dependent on a dedicated (usually) server that requires an operating system and software, which requires a larger initial investment than an integrated solution. Not only this, but because the solution sits directly on the network and examines the traffic at the network and data link layer it does not affect the speed of the network or add load to the systems it monitors, and yet it regains an extremely granular level of inspection without needing many network interface cards (like a firewall), it simply utilises the network points that are already present on the switch!

It can be seen then that integrated solutions certainly have many advantages over regular IDS and yet companies have not adopted this approach due to lack of vendor interest and support. If we examine the timeline of IDS technology we can see that the same basic technology has been used for years (signature and pattern matching). Perhaps the time is coming for a new approach, and with that a new method for deploying the IDS. No matter what happens within the field of IDS it is an unfortunate reality that attacks will continue to take place, and subsequently millions of pounds will be lost each year due to the lack of commitment of vendors, implementers, and above all, companies as well as the persistent pest that is the attacker.

There is of course no substitute for attack mitigation through an adequate security policy, as well as secure management and reporting. This is the first stepping-stone towards a secure infrastructure; a security policy must be in place, well defined and championed at a high level. Having achieved this, then the manpower can be utilised to implement, maintain, and oversee a secure network infrastructure using IDS. This has been traditionally a popular and successful approach, and will continue to be so no matter what technology or techniques are to be used in the future.

Whether IDS will be the next computing paradigm and enjoy as large a footprint in organisations that anti virus software has now, will remain to be seen. The future holds many problems for IDS, especially with the advent of IPv6 and the rapidly approaching reality of universally encrypted traffic – payload analysis tasks will become increasingly more difficult, without another dimension of difficulty with wireless networking. However, as always the hardware will adapt, but will come at a price.

Whatever is in store for IDS in the future, the technology is beginning, and will continue to aggregate within the existing network infrastructure. Perhaps by following the steps of integrating switches and IDS together to weave into the network fabric. Network and host based systems boundaries will continue to blur and embrace each other in the fight against network attacks. This view being shared by Security Focus: “Ultimately, I think that future IDS will merge all of the independent network components and tools which exist today, into a complete and cooperative system, dedicated to keeping networks stable…. as always, the

ultimate authority will be our own judgement." [10]

[10] Tanase, p.4

Appendix A: Sample Cisco Catalyst Switch Secure Configuration (preparation for integrated IDS in-line card)[11]

```
!
!Turn on NTP
!
set timezone GMT
set summertime BST
set summertime recurring
set ntp authentication enable
set ntp key 1 trusted md5 -UN&/6[oh6
set ntp server 192.168.254.57 key 1
set ntp client enable
!
! turn off un-needed services
!
set cdp disable
set ip http server disable
!
!turn on logging and snmp
!
set logging server 192.168.253.56
set logging server 192.168.253.51
set logging timestamp enable
set snmp community read-only Txo~QbW3XM
set ip permit enable snmp
set ip permit 192.168.253.51 snmp
!
!Turn on AAA
!
set tacacs server 192.168.253.54 primary
set tacacs key SJj)j~t]6-
set authentication login tacacs enable telnet
set authentication login local disable telnet
set authorization exec enable tacacs+ deny telnet
set accounting exec enable start-stop tacacs+
set accounting connect enable start-stop tacacs+
!
!set passwords and access restrictions
!
set banner motd <c>
This is a private system used for testing for SNS GIAC IDS Testing purposes
<c>
!console password is set by 'set password'
!enter old password followed by new password
!console password = X)[^j+#T98
!
!enable password is set by 'set enable'
!enter old password followed by new password
!enable password = %Z<)|z9~zq
!
!the following password configuration only works the first time
!
set password
X)[^j+#T98
X)[^j+#T98
set enable
cisco
%Z<)|z9~zq
%Z<)|z9~zq
!
!the above password configuration only works the first time
!
set logout 2
set ip permit enable telnet
set ip permit 192.168.253.0 255.255.255.0 telnet
```

[11] Adapted from Convery & Trudel, p. 40

References:

Armstrong, Illena. "Detecting Intrusions: Problems and Solutions". InfoSecurity News Magazine. September 2002 – West Coast Publishing.

Cisco. "set spantree root through set vtp". 14 June 2002. URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/rel7_2/cmd_ref/set_s_z.htm#16861 (29 Aug 2002).

Cisco. "Catalyst 6000 Intrusion Detection System Module". 5 Sep 2001. URL: http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/6kids_ds.htm (02 Sep 2002).

Convery, Sean & Trudel, Bernie. "Cisco - SAFE: A Security Blueprint for Enterprise Networks". 18/06/02. URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm (25 Aug 2002).

Internet Security Systems, Inc. "Enterprise Protection". URL: http://www.iss.net (17 Sep 2002).

McAlerney, Joe. "SILICON DEFENSE – Snort Support Intrusion Detection Research". IDWG – Intrusion Detection Exchange Format. URL: http://www.silicondefense.com/idwg/ (29 Aug 2002).

SANS. "Security Essentials 1.1". Booklet to accompany SANS GIAC Course (10 Sep 2002).

Sipes, Steven. "Why your switched network isn't secure". Intrusion Detection FAQ. 10 September 2000. URL: http://www.sans.org/newlook/resources/IDFAQ/switched_network.htm (29 Aug 2002).

Snort.org. URL: http://www.snort.org/about.html (17 Sep 2002).

Tanase, Matthew. "The Future of IDS". 4 December 2001. URL: http://online.securityfocus.com/infocus/1518 (3 September 2002).

Taylor, David. "Are There Vulnerabilities in VLAN Implementations?". VLAN Security Test Report. July 12 2002. URL: http://www.sans.org/newlook/resources/IDFAQ/vlan.htm. (15 Aug 2002).

Tripwire, Inc. "Tripwire for Servers for Security & Network Management". URL: http://www.tripwire.com/products/servers/features.cfm (22 Sep 2002).

Wexler, Joanie. "Security Blanket". Packet Magazine – Volume12, No. 1. January 2001. URL: http://www.cisco.com/warp/public/784/packet/jan01/pdfs/packet_jan01.pdf (01 August 2002).