Network Intrusion Prevention/Detection System: Implementation of Network TAPs and Monitoring Systems on Company X’s Wide Area Network

By

Robert Price & Troy Cooper

Submitted to
the Faculty of the Information Technology Program
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

University of Cincinnati
College of Education, Criminal Justice, and Human Services

June 2012
Network Intrusion Prevention/Detection System: Implementation of Network TAPs and Monitoring Systems on Company X Software’s Wide Area Network

By

Robert Price & Troy Cooper

Submitted to
the Faculty of the Information Technology Program
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

© Copyright 2012 Bobby Price and Troy Cooper

The author grants to the Information Technology Program permission to reproduce and distribute copies of this document in whole or in part.

_________________________________________  ______________
Troy Cooper                           Date
_________________________________________  ______________
Bobby Price                           Date
_________________________________________  ______________
Mark Stockman                Date
ACKNOWLEDGEMENTS

Special thanks to Tony Schutte and Nick Ritter, IT Managers at Company X, for giving us a great project to work on while we struggled to find one. Also, for their support in acquiring hardware and setting company time aside for us so that we could implement everything. This project wouldn’t have succeeded without them. And of course, thanks to the IT faculty and the University of Cincinnati. Without their guidance and support we wouldn’t have made it this far. And a very special thanks to Professor Stockman for guiding and advising us on this project.
TABLE OF CONTENTS

Signature Page................................................................................................................i

Acknowledgements...................................................................................................... ii

Table of Contents....................................................................................................... iii

List of Figures............................................................................................................. iv

Abstract..................................................................................................................... v

Project Description and Intended Use...........................................................................

  Problem Statement.................................................................................................. 1

  Description of the Solution...................................................................................... 2

  User Profile........................................................................................................... 6

Design Protocols......................................................................................................... 7

Deliverables................................................................................................................ 8

Project Planning.........................................................................................................

  Project Budget...................................................................................................... 9

  Project Schedule................................................................................................. 10

  Hardware............................................................................................................. 11

  Software............................................................................................................. 15

Proof of Design.......................................................................................................... 16

Testing....................................................................................................................... 28

Conclusions and Recommendations......................................................................... 29

References............................................................................................................... 31

Notes......................................................................................................................... 32
LIST OF FIGURES

Figure 1: Map of WAN (Wide Area Network)..........................3
Figure 2: Diagram of Milford LAN (Local Area Network).........4
Figure 3: Deployment of a TAP on a network.........................5
Figure 4: Use Case Model.............................................6
Figure 5: Timeline.....................................................10
Figure 6: Gantt Chart................................................11
Figure 7: VSS v 16x8 Distributed TAP..............................12
Figure 8: Dell R515 Server.........................................14
Figure 9: Network Tap...............................................16
Figure 10: VSS Login Screen.....................................17
Figure 11: Port Statuses............................................18
Figure 12: TAP Setup................................................18
Figure 13: User Screen..............................................19
Figure 14: Port and Port Monitoring.................................20
Figure 15: System Settings.......................................21
Figure 16: BASE home screen.....................................22
Figure 17: Detected Traffic.......................................23
Figure 18: Details about Signatures.................................24
Figure 19: IP address Reputation................................25
Figure 20: Instances of Snort.....................................26
Figure 21: Snort Rules..............................................27
ABSTRACT

Security on Company x’s network will be increased with the addition of mirrored traffic and IPS/IDS sensors. Each network between the public firewall will be mirrored, or tapped into, and sent to a Snort sensor. Snort is the world's leading open source IDS/IPS and will allow us to implement security based rule sets to detect and prevent security related risks.
PROBLEM STATEMENT

For security and confidentiality the company that we worked with during our project will remain nameless. Therefore, we will refer to the company as Company X throughout this paper.

Company X, in Milford - and other locations as well; did not have, or used minimum security detection and prevention systems. Company X wanted to be able to view all of the traffic that was coming through their firewall and also have security systems implemented so that malicious traffic could be caught before any damage was done. Company X, in Milford, was using SPAN (Switched Port Analyzer) ports to mirror and monitor the traffic on their switches. This created a variety of problems. First off, there was the functionality of the mirrored port. Mirroring forced the switch to either send all packets from across the switch, or packets from a specified port, to a specific SPAN/monitoring port in addition to delivering it to its intended recipient. This created a higher rate of packet collision, because twenty other ports on the switch continually sent packets to the mirror/SPAN port. The risk of packet loss is again increased again, because the mirror/SPAN port had the same amount of bandwidth as the other ports on the switch (2). Company X wanted to be able to mirror the traffic from each network to at least two monitoring systems. If they had two ports to mirror traffic on each switch, this would have tripled the rate of packet collision - per switch.

Another issue with the spanned port was how the ports were commonly configured. Switches dropped layer 1 (physical) and selected layer 2 (data link) errors depending on what was deemed as high priority. This caused info to be lost that could have been used to properly troubleshoot common physical layer problems (1).
Also, if Company X had decided to configure more mirror/SPAN ports, new switches would have had to been purchased to connect the monitoring devices to the network. These switches would have been a waste because not all ports would be used for this situation. Moreover, creating more mirror/SPAN ports would have created system downtime, because a system engineer would have had to configure each mirror/SPAN port.

System downtime would have produced decreased productivity - as systems would have been down and Company X employees would have not been able to work. Company X has 661 users in Milford and about 7500-8500 users worldwide. Not to mention the extra cost that would have incurred from paying an engineer to configure the mirror/SPAN ports.

Moreover, there was only the capability for one mirror/SPAN port on the routers that were being used by Company X. So there would not only have been the added cost of purchasing new switches to connect the IDS/IPS to but there would have also been the added cost of purchasing new routers if Company X would ever like to connect additional monitoring systems to any of the routers in the future.

Company X wanted like to add IDS/IPS to their wide area network (WAN), but faced the issue of purchasing unnecessary hardware and labor; along with using a technology that is known for dropping traffic. Therefore, we implemented a solution to this problem. Our solution required minimum configuration, down time and labor.

**DESCRIPTION OF THE SOLUTION**

Our solution was to install a TAP (Tunnel Addressing Protocol) on the internal network at the Company X Milford site. After a TAP was installed, packet sniffers and Snort were connected to the TAP to monitor the network. A packet sniffer allowed us to log the traffic that is passed over
the network. Snort is open source network intrusion prevention and detection system that will allow us to perform real-time traffic analysis.

Siemens has eleven sites worldwide that this project will eventually affect. Besides our location in Milford; other locations include Tokyo, Shanghai, and Frankfurt; among others.

Figure 1: Map of WAN (Wide Area Network)

Figure one shows the map of the Company X’s Wide Area Network. Each yellow cloud represents a site that has internet access. Each site that has internet access will eventually have a TAP installed on that site’s network. We will not be installing the TAPs at these sites, but our implementation at the Milford site laid the groundwork for the implementation at every other site. We documented our process so that in the future the networking and cyber security teams in Milford can follow our process to implement our solution at each site.
Figure 2 displays the local area network at the Company X Milford site. Each Ethernet connection that is coming off of the public firewall is highlighted with a black circle. Each of these connections coming off the public firewall was tapped. By doing this the TAP replicated all of traffic on each port so that it can be monitored through a packet tracer, and through Snort. We will be looking to purchase TAPs that have at least two monitoring ports, one for the packet capture and one for Snort. The TAP that we ending up choosing is a TAP from VSS Monitoring and it is a 16x8 tap. The network TAP plugs right in to a router or switch and no configuration is needed. For our solution, the tap was installed between the firewall and each highlighted network in Figure 2.
Figure 3: Deployment of a TAP on a network

Figure 3 shows an example of how we connected the TAP to the network and Company X. The TAP was placed inline, between the firewall and the switch. In our case, the router was connected to Network Port A, in the diagram, and the switch was connected to Network Port B. The full duplex traffic now passes through the TAP and is mirrored to the monitoring ports and sent to our monitoring tools. In our case the monitoring tools are Snort and Daemon Logger. No configuration was needed with TAPs – they are plug and play. They are also 100% failsafe.
USER PROFILE

There are two kinds of users of our solution: network analysts and security analysts (8).

Figure 4: Use Case Model

Figure 4 shows the use case model. Security Analysts are the only users of the monitoring systems. The majority of the security analysts are familiar with packet logging software and Snort. They log in to the systems to view traffic, view incidents, conduct investigations, and to
create rules in Snort –if need be. Network Analysts only interact with the physical TAP. The
Network Analysts are familiar with how the network is laid out and are responsible for the daily
network operations. They will remove and/or replace any TAPs if they happen to fail; and also
be responsible for the addition of more TAPs, if needed.

DESIGN PROTOCOLS

● Determine amount/type of Taps needed
First, we confirmed that each network diagram was up to date. Once this was
confirmed we were able to determine how many networks each site has that needed to be
monitored.

● Purchase TAPs from vendor
Our vendor of choice was VSS Monitoring. We selected to use the VSS v16x8 distributed TAP.

● Install server software (Red Hat, Libpcap, PCRE, Libdnet, Barnyard2, DAQ)
Snort was installed on a Red Hat server. Before installing Snort we needed to install the
following software packages: Libpcap, PCRE, Libdnet, Barnyard2, and DAQ.
Libcap. Used by Snort to capture the packets that is traveling over the network.
PCRE: A set of functions that implement regular expression pattern matching using the
same syntax is Perl 5.
Libdnet: A generic networking API that provides access to several protocols.
Barnyard2: The output system for Snort. Snort creates a special binary output format
called “unified”. Barnyard2 reads this file, and then resends the data to a database backend.
DAQ: The data-acquisition API that is necessary to use Snort version 2.0.0 and above.
The latest release of Snort is 2.9.2.1-1. Also we needed BASE to be able to view all of the
information that snort is picking up.
DELIVERABLES

● Updated Network Diagrams
Network diagrams were for the Milford site were updated in order for us to complete this project. The Milford diagram hasn’t been updated since 2008.

● TAPs on network
Company X now has an inline 16x8 VSS Monitoring TAP on their network mirroring all traffic off of the public firewall.

  ● PCap Appliances
Company X now has Daemon Logger as a PCap appliance for their network.

● Snort System
Snort was installed on a Dell server running RedHat Enterprise edition.

● Latest Snort rule-set
The latest Snort rule-set was downloaded and installed to deliver the latest detection capabilities. We also subscribed to the site to automatically download the latest rules.

● Real-time traffic analysis
Company X now has real time traffic analysis capabilities with the addition of a Snort system on their network.

● Packet-logging
Company X now has packet logging, with the addition of a Snort system on their network.
PROJECT BUDGET

The whole Snort, TAP, packet capture budget for Company X is $250,000. This is for the implementation on the entire WAN. The total cost for our implementation was $18,566.22. We estimated the entire future cost using our project cost to be $204,228.42. Table 1 details the budget for this project.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Budgeted Cost</th>
<th>Actual Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAPs</td>
<td>N/A</td>
<td>$12,566.22</td>
</tr>
<tr>
<td>Server</td>
<td>N/A</td>
<td>$5,500</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software</th>
<th>Budgeted Cost</th>
<th>Actual Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snort</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>B.A.S.E.</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>Red Hat</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other</th>
<th>Budgeted Cost</th>
<th>Actual Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sourcefire VRT Certified Rules</td>
<td>N/A</td>
<td>$500</td>
</tr>
</tbody>
</table>

| Total (Milford Site Only) | $18,566.22 |
| Total (All Sites)         | $204,228.42 |

Table 1: Cost Analysis
PROJECT SCHEDULE

We completed the project in the last week of April 2012.

Figure 5 details an organized timeline of the events we followed to insure a successful project outcome.

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Duration</th>
<th>Start</th>
<th>Finish</th>
<th>Predecessors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Project Selection</td>
<td>1 day</td>
<td>Tue 11/1/11</td>
<td>Tue 11/1/11</td>
<td></td>
</tr>
<tr>
<td>2 Research TAP Vendors</td>
<td>20 days</td>
<td>Mon 10/31/11</td>
<td>Fri 11/25/11</td>
<td></td>
</tr>
<tr>
<td>3 Write Draft Proposal</td>
<td>6 days</td>
<td>Mon 11/7/11</td>
<td>Mon 11/14/11</td>
<td></td>
</tr>
<tr>
<td>4 Write Final Proposal</td>
<td>11 days</td>
<td>Mon 11/21/11</td>
<td>Mon 12/5/11</td>
<td></td>
</tr>
<tr>
<td>5 Autumn Quarter Presentation</td>
<td>1 day</td>
<td>Tue 11/22/11</td>
<td>Tue 11/22/11</td>
<td></td>
</tr>
<tr>
<td>6 Winter Quarter Presentation</td>
<td>11 days</td>
<td>Mon 2/20/12</td>
<td>Mon 3/5/12</td>
<td></td>
</tr>
<tr>
<td>7 Present TAPs Vendor Results</td>
<td>1 day</td>
<td>Fri 12/2/11</td>
<td>Fri 12/2/11</td>
<td></td>
</tr>
<tr>
<td>8 Order TAP</td>
<td>1 day</td>
<td>Tue 1/31/12</td>
<td>Tue 1/31/12</td>
<td></td>
</tr>
<tr>
<td>9 Install Software and Configure Server</td>
<td>7 days</td>
<td>Thu 3/29/12</td>
<td>Thu 4/5/12</td>
<td></td>
</tr>
<tr>
<td>10 Create Project Plan</td>
<td>2 days</td>
<td>Fri 3/30/12</td>
<td>Sun 4/1/12</td>
<td></td>
</tr>
<tr>
<td>11 Install TAP on to Network</td>
<td>7 days</td>
<td>Mon 4/9/12</td>
<td>Mon 4/16/12</td>
<td></td>
</tr>
<tr>
<td>12 Test TAP</td>
<td>9 days</td>
<td>Wed 4/18/12</td>
<td>Fri 4/27/12</td>
<td>11</td>
</tr>
<tr>
<td>13 Assignment: Testing Data</td>
<td>5 days</td>
<td>Wed 4/18/12</td>
<td>Mon 4/23/12</td>
<td></td>
</tr>
<tr>
<td>14 Prepare Final Presentation</td>
<td>14 days</td>
<td>Thu 4/19/12</td>
<td>Sun 5/6/12</td>
<td>14</td>
</tr>
<tr>
<td>15 Present Final Presentation</td>
<td>1 day</td>
<td>Mon 5/7/12</td>
<td>Mon 5/7/12</td>
<td>16</td>
</tr>
<tr>
<td>16 Prepare Draft Report</td>
<td>14 days</td>
<td>Thu 4/19/12</td>
<td>Sun 5/6/12</td>
<td></td>
</tr>
<tr>
<td>17 Turn in Draft Report</td>
<td>1 day</td>
<td>Mon 5/7/12</td>
<td>Mon 5/7/12</td>
<td>18</td>
</tr>
<tr>
<td>18 Tech Expo Set-up</td>
<td>1 day</td>
<td>Mon 5/14/12</td>
<td>Mon 5/14/12</td>
<td>18</td>
</tr>
<tr>
<td>19 Tech Expo</td>
<td>1 day</td>
<td>Tue 5/15/12</td>
<td>Tue 5/15/12</td>
<td></td>
</tr>
<tr>
<td>20 Prepare Final Report</td>
<td>14 days</td>
<td>Wed 5/16/12</td>
<td>Sun 6/3/12</td>
<td>20</td>
</tr>
<tr>
<td>21 Turn in Final Report</td>
<td>1 day</td>
<td>Mon 6/4/12</td>
<td>Mon 6/4/12</td>
<td></td>
</tr>
<tr>
<td>22 Academic Paper Abstract</td>
<td>7 days</td>
<td>Mon 4/16/12</td>
<td>Mon 4/23/12</td>
<td></td>
</tr>
<tr>
<td>23 Academic Paper</td>
<td>16 days</td>
<td>Tue 5/1/12</td>
<td>Sun 5/20/12</td>
<td></td>
</tr>
<tr>
<td>24 Turn in Academic Paper</td>
<td>1 day</td>
<td>Mon 5/21/12</td>
<td>Mon 5/21/12</td>
<td>22,23</td>
</tr>
</tbody>
</table>

Figure 5: Timeline
The complete implementation of the network intrusion, prevention, and detection system required a collection of tools. These tools were used to mirror the network traffic, send the mirrored traffic to a monitoring system and to analyze the traffic through the system. These tools fall into two categories: hardware and software.

**HARDWARE**

**TAPs**

A network test access port (TAP) creates permanent access ports for passive monitoring. A monitoring device that is connected to a TAP receives the same traffic as
it would if it were located directly on the wire and sends traffic data to a monitoring device; by splitting or regenerating the network signal(12). There were six requirements for the TAP.

The TAP had to have:

- A minimum eight network ports and four monitoring ports
- Be low cost
- Require minimal configuration
- Be remotely accessible
- And have a transfer rate of 100/1000Mbs per port (10)

With the requirements in mind we decided to go with the VSS v16x8 Distributed TAP.

**Figure 7: VSS v 16x8 Distributed TAP**
The VSS v16x8 TAP has sixteen fix 10/100/1000 UTP ports. The fixed ports can be configured as either inputs or outputs. Each pair of the fixed ports can operate as a passive Ethernet tap, with fail-safe loop-through during loss of power.

As show earlier (Table 1), the cost of this TAP is around twelve and a half thousand dollars. During the vendor research phase we found VSS to have the most competitive pricing. And the purchasing of this TAP is also more cost effective than the alternative to our solution, which was to buy more switches for SPAN ports.

The VSS v16x8 TAP requires minimal configuration. The configuration consists of plugging the network connections in to the TAP. That’s it. Anything else that you want to configure can be done from the Web interface. The TAP has auto-MDI/X and auto-negotiation.

The auto-MDI/X feature allows the TAP to figure out for itself which pins in the network cable to send traffic on. And because of this, no cross-over cables are needed.

The auto-negotiation feature allows the TAP to self-configure the speeds of the ports during the link initialization.

These features make installing and configuring the TAP a cinch. Once the TAP is up and running the only thing to really configure is telling the TAP which monitoring device to send the mirrored traffic to.

The VSS v16x8 TAP is also able to be configured from anywhere within the Project X network via Web browser through the HTTP/HTTPS protocol.
Monitoring Systems

Additional server was purchased to use as Snort monitoring systems. The server that we purchased is figure 8. The server will be connected to the ports on the TAPs so that the packets can be viewed through the packet capture, and also so that rules can be created with the IDS, or Snort. The server that was purchased was a Dell R515. With having this server there won’t need to be any extra time maintaining and managing the server. This server also has automated updates so you won’t have to take time out of your day to do updates on the server and you are able to continue working on your projects. This server also has an interactive screen which makes it a lot easier to set up the server (17).

![Dell R515 Server](http://www.dell.com/us/enterprise/p/poweredge-r515/pd)
SOFTWARE

Snort

Snort is an open source network IDS/IPS developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide (14). With Snort, the Security Analysts will be able to view suspicious traffic that is flowing across the network and be able to create rules to block traffic from going to threatening IP addresses.

Libpcap

Libpcap is a required third party application for Snort. Pcap consists of an application programming interface (API) for capturing network traffic (14). This software is used as a plugin for Snort so that the traffic flowing across the network can be viewed.

BASE

BASE is a Basic Analysis and Security Engine. It is the interface of snort so you are able to see the intrusions on your network. It is a simple to use program so if some people are not comfortable editing files directly, this program makes it a lot easier for the user to do so. Another perk of using BASE it is free and it is supported by volunteers so you are able to get help easily for setting it up on your system or if you just had any other questions about using BASE (16).
PROOF OF Design

In figure 9 the blue piece of equipment that is in the middle is the network TAP that we installed on the rack. The blue cables that are all the way on the right of network TAP is the cables going to the monitoring system, which is the server with red hat on it.

Figure 9: Network Tap
In figure 10, this displays the login screen which accesses the TAP settings.

![Figure 10: VSS Login Screen](image)

Once you login into the VSS monitoring this is the page that appears. On this page you are able to see the status of all of the ports such as if the port is up or down. Also on this page it shows the speed of the port and how the port was set up, which all of ours we set up as auto. Another thing that is shown on this page is to protect the equipment this shows the temperature and the power supply and will show if everything is working properly. With using VSS Monitoring they sell other equipment like switches, so with this interface you have to set the class to the specific equipment that is being used and for this project it is a TAP.
Figure 11: Port Statuses

From the main screen above (Figure 11) there is a setting that allows you to go into the setup of each port. To enter the setup of the port, the button is all the way to the right in figure 11. Once that button is clicked then figure 12 appears and that is the TAP setup. In the TAP setup this is where we set that we were using TAPs instead of the other options there are at the top of figure 12. Also, there are different kinds of settings that can be set so the TAP can be exactly how it is supposed to be. For this project it was set to auto and everything is working properly.

Figure 12: TAP Setup
In figure 13 is the user screen which is nice because it has the capabilities to allow several different users to access the TAP. When different users are added restrictions can be set so they can only change settings on certain ports that they are given permissions to. For our project as of right now we only needed to have one user which is the admin user. This is setup for later down the road that if the company wants to add a different user they will be able to do that easy enough.

**Figure 13: User Screen**

![User Screen](image-url)
### Figure 14: Port and Port Monitoring

For figure 14 this shows where each port is getting monitored at. The first column is for if the project involved filtering which we are not doing. The next column is showing the port input and then the third column shows where the port input is going. So for an example port input 1A and 1B is going to the port output M1.
In figure 15 this shows all of the settings for the project. Have all of the network settings which we covered up for security reasons. Then we have the system clock which just shows the clock. Also we have it set up so that it will automatically log you out after 30 minutes. The next settings are the advanced setting which we have TAP port pairs that are connected through the TAP. The last thing is the information about VLAN tagging.
Figure 16 shows the home screen of B.A.S.E. (Basic Analysis and Security Engine) when we login into B.A.S.E. B.A.S.E. is the user interface for Snort so it will be easier to access the data that snort brings in without doing everything in command line. This is the interface that we will be using to make it easier for Company X to fix problems as they come up.
Below, in figure 17 we are showing all of the detected traffic that is being detected by snort. This traffic is being detected by the snort rules and also the rules that have been created. This will help out our problem because we will detect the traffic by the rules and it will alert us so that Company X will be able to fix the problem when they come up.

Figure 17: Detected Traffic
Figure 18: Details about Signatures

Figure 18 above is part of BASE where it allows you to click on one of the detected traffic that you were able to see in figure 7 and see more details about the traffic that was detected. You are able to see where the source address was trying to get to along with some information on what is happening to see if it is a real threat to the company and if you need to do anything about it. By
having this it will help the problem because you will be able to see if it is a real threat or not. If it is not a real threat then Company X won’t waste their trying to fix the problem and be able to focus on the ones that are causing problems.

Figure 19: IP address Reputation
Figure 19 isn’t actually part of the BASE interface but it is a useful tool that is part of MacAfee’s website that will show the reputation of that specific IP address and will show a map of where the attack is coming from. This is useful for our problem because Company X will be able to find out the most dangerous attacks and be able to fix them first.

Figure 20: Instances of Snort

Figure 20 above shows the instances of snort that are running and the host that are being monitored. This shows that we have snort running and monitoring certain host which is what we are working on for the project.

In figure 21 below shows the Snort rules that we have for snort. This helps solve the problems that company x is having because it will help protect the network from being attacked because it will let Siemens know if there is unusual activity for they are able to fix the problem.
Figure 21: Snort Rules
Table 2: Testing Scenarios

TESTING

Table 2 displays our testing scenarios.

For testing scenario 1 we were able to visually inspect that the network taps were connected to the right input and outputs and we also have the cables labeled just in case anything happens that they needed to be disconnected, that it would be easy to hook everything up again. We also were able to that the snort sensor is connected and hooked up to the tap. We were able to get results using BASE. For the last one with testing taps we were able to verify that the tap is working correctly from using BASE and getting results.

For testing scenario we connected to the snort system and brought up the configuration file. We were able to connect to snort and saw that all of the networks to be monitored were in the configuration file and were being monitored properly. We then opened up B.A.S.E and verified that packets were being captured and displayed through the web interface.

For testing scenario 3 we downloaded the latest rule set off of the internet so we know that it is the most current version. In order to make sure that it will always be the latest rule set we
purchased the version from snort to automatically download the latest rule sets when they are available. We also checked to make sure that the rule set was in the correct folder.

For testing scenario 4 we really couldn’t block traffic that was coming from within the same network that we were monitoring, we weren’t sure on how this would affect the system so we decided to test the sql injection warnings. We opened a site on the local intranet and entered a select statement in to a text box on a login page. We then opened B.A.S.E. and viewed that the traffic was correctly marked as a “Possible SQL injection” warning.

**CONCLUSIONS AND RECOMMENDATIONS**

In conclusion, Company X wanted a way to monitor all of the traffic on their internal network. One solution to this problem is to use SPAN ports, but with SPAN ports the risk of dropping packets because of collision is presented.

Our solution was to implement a VSS v16x8 TAP on the Company X network. The VSS Tap allows an inline device to mirror all of the network traffic coming off of the Company X public firewall without the risk of dropping packets.

Unlike a switch with SPAN ports, if the power on the TAP is lost the network TAP will still allow traffic to flow through it.

The VSS TAP also requires minimal configuration, which can be done by any employee with basic networking knowledge. There are no network engineers required to take the extra time to set up SPAN ports, like there would be with a switch.

The network TAP also allows the network to be easily expanded. There is no reconfiguration of switch ports as the network grows. And the TAP also has extra ports for expandability of monitoring systems.
The cost of a network TAP is higher than the managers at Company X first believed they would be. But this solution beats the cost of purchasing more switches to create SPAN ports – along with the other benefits discussed above. And VSS TAPS were the most cost competitive of all of the vendors that were looked at.

Our recommendation would be to implement network TAPs for any company that is looking to implement an IDS on to their network if it is feasible. Of course could be an issue, depending on the size of the company. There are various different models of network TAPs available on the market, and depending on the size of the network depends on how much will be spent.

Return on investment has traditionally been difficult to quantify for network security devices, in part because it is difficult to calculate risk accurately due to the subjectivity involved with its quantification (15,1). But can you really put a value on the network infrastructure of your company and the data flowing across it?

The answer to that question was easy for Company X. They have already felt the effects of having their network compromised and are already feeling the results of having an IDS on their network.
REFERENCES


