Global Information Assurance Certification Paper

The Next Step in Securing Our Network:

A study in analyzing our risks
and implementing Intrusion Detection
Phase 1

SANS GIAC Security Essentials Practical Assignment
v1.4b, Option One

Steve Crow
January 28, 2004

Abstract

Ours is a small sized medical clinic that does not host a web site. We provide multiple services for thousands of patients and naturally must keep their information confidential, accurate and highly available. The Doctors, nurses and a handful of users require Internet access for business purposes. Some of those users require email and where possible those users are on a different network than the production servers. As the only System/Network Administrator, my challenge is to assess what our immediate security needs are, and to continually improve upon our defenses. This paper will have a beginning (Risk Assessment), a middle (Implement Safeguard), but not an end. There is no end to implementing security. It is a continuous process. A phased approach will be used. This paper covers Phase 1: installing and testing a network based Intrusion Detection System on the smaller more email intensive network before implementing it on the main network.

The Beginning: A Risk Assessment

In order to provide better security for our clinic, we have to understand what the "Current State of Affairs" is. In other words, what are the assets, how are the assets at risk, and what are we currently doing to protect those assets. After that we can come up with a plan for improving the defenses.

Our Assets: What is it we want to protect?

I) Our Information:

The information we need to protect is all of the data that pertains to patient records, billing records, schedules, financial info, and employee information. We must maintain the confidentiality of our information; the integrity of that information; and the ability to create, modify, and process our information at any moment in time (availability). The loss of confidentiality could damage patient confidence and mean significant monetary damages. The loss of integrity could delay or cause improper treatment for patients. The loss of the availability of our information would cause delayed and impaired treatment as well as have an impact on revenues. All of these possibilities are considered extremely serious.

II) Our Systems:

Our computers, network equipment, and software also need protecting, as these are the infrastructures that make the confidentiality, integrity, and availability of our information possible in the first place. The basic pieces are:

A) Servers: AIX and Windows 2000.
B) Workstations: Windows XP, 2000, and 98
C) Dumb Terminals
D) Firewalls: A Cisco Pix and a Sonicwall SOHO
E) Switches, Hub, and a Bridge

The Risks: What are they?

In order to figure out what other steps should be taken to improve the security of our Information, a Risk Analysis is in order. I thought the SANS training on Risk Analysis was very helpful. SANS taught the classic Risk = Threat X Vulnerability equation and that a Risk Analysis Matrix measured those risks in the context of Severity of Consequences and Probability of Likelihood [1]. That training provided me with a starting point for examining our risks, the likelihood of compromise, and the possible extent of damage.

This Risk Assessment will focus primarily on the threats posed by Internet access and the vulnerabilities those threats can exploit. There are other threats posed such as fire, flooding, tornados, malicious employees, thieves, or accidents. These threats are managed mostly by physical security, password policies, backup strategies, and disaster recovery plans.

I) What are the Threats?

There are all kinds of threats to information, which ones are most serious?

A) Internet Browsing.

Internet Browsing is a risk because links and visits to Web sites can be the source of the likes of Blaster, Code-Red, or Nimda; "Blended Threats" that then use you to spread the attack via email or network shares. Symantec's Glossary page defines these as: "Blended threats combine the characteristics of viruses, worms, Trojan Horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. By using multiple methods and techniques, blended threats can rapidly spread and cause widespread damage,"(Symantec)[2]. If a user goes to an unauthorized web site, or even to a legitimate site that has been compromised, it could do serious harm. Valuable information could be damaged, stolen, or changed. In the case of Blaster, it was a pretty effective Denial of Service attack by preventing users from working until the systems were fixed. I personally experienced this one at my home and I got it via dialup!

B) Email.

Email is a huge threat because not only have viruses been able to execute while just being read, many users are just not computer literate enough to recognize dangerous attachments. Users have all too often been the victim of social engineering and tricked into opening an attachment that then embeds itself in their system and begins its nefarious work. It then seeks other victims. We don't host an Email server, so each email user has an account with an ISP and uses an email client such as Outlook, Eudora, or an online account such as Yahoo. Some ISPs are getting better at catching the viruses, but way too many still get through. Malware has become so common now that even national news media carry stories about the dangers.

For example while writing this paper, the New York Times web site carried an article about the so-called Bagle.A worm that may compare to the Sobig worms. [3] Even when I went to research that worm on the Symantec web site, there were other, newer, threats listed! [4]

C) Attackers.
Just because we have a broadband connection to the Internet, there are attackers out there that are consciously trying to violate our systems. They are aggressive and diligent. Whether they do it by actively scanning for open ports and vulnerabilities, or by war dialing to find systems available through modems, or by sending malware through email; they are seeking weaknesses to exploit.

II) What are the Vulnerabilities?

As I see it, the vulnerabilities can be divided up as: Software related, User caused, and Configuration issues. I will rate the particular items, as I understand the consequences of what could happen if a vulnerability were exploited in our situation, and the likelihood of the exploit happening. The ratings are: 3 High, 2 Medium, and 1 Low. The Net Risk Rating is the total of the Seriousness and Likelihood of an exploit occurring.

A) Software Related
Software flaws, issues, and vulnerabilities are discovered just about daily. I read the email newsletter "@RISK: The Consensus Security Vulnerability Alert" by SANS. [5]. It is astonishing to see week after week how many software problems there are: buffer overflows, elevated privileges, command execution, and poor to no security. It seems impossible to keep up with, yet we have to remain diligent.

The Software we have that could cause us trouble and therefore must stay updated is:

Software:	Seriousness	Likelihood	Net Rating
IBM AIX	3	1	4
Unix Medical Application	3	1	4
Windows98	3	2	5
Windows2000 Srvr	3	2	5
Windows2000 Wrkst	3	2	5
WindowsXP	3	2	5
MS Internet Explorer	3	3	6
Microsoft Outlook	3	3	6
MS Word & Excel	1	1	2
Eudora	3	3	6
AOL	3	3	6
Corel WordPerfect	1	1	2
Symantec Corporate AV	3	1	4
Accounting Application	3	1	4
Proprietary Medical SW	3	1	4

B) User Caused Problems

I have a job because of users. It's my job to help them fulfill the requirements of the business. However those same users can so very easily click on a malicious link or an attachment that legitimately passes through the firewall. Even with user training, it only takes one mistake to delete a file or execute the damaging Malware. Most users in my experience are very good at what they do, but they are not computer literate enough to spot social engineering designed to trick them. Hence the "Mydoom" or "Novarg" [6] mass emailing worm that caused so much trouble in late January. Another issue is user passwords. So important to keep secret, yet almost universally found beneath the keyboard. I'm trying to get my users to understand something that I read somewhere (I have no idea where!). Passwords are like toothbrushes: Use 'em, change 'em often, and don't share them.

The user may:	Seriousness	Likelihood	Net Rating
Mistakenly execute malware	3	3	6
Reveal sensitive information	2	2	4
Purposely cause damage	2	1	3
Accidentally cause damage	2	2	4

C) Configuration Issues

Configuration issues are sort of a user caused problem, but I think they deserve their own mention. For example: I don't have managed switches at this point. But I do have items that require careful set up and configuration. For example, firewalls do a great job, when they are configured correctly.

Items to Configure:	Seriousness	Likelihood	Net Rating
Firewalls	3	2	5
Bridge	3	1	4
Modems	3	1	4
Network Shares	3	2	5
Access Control Lists	3	2	5

Obviously, as I look at that potential causes of damage and the likelihood of occurrence, I find the highest Net Risk Rating to be with associated with Internet Access.

III) Our Security Infrastructure: How are we doing so far?

A) Firewalls

Our network is divided into two segments: A larger network for most of the users who don't require email and only limited Internet browsing. The other smaller segment is for users who do require email. Their access to the 'main' network is provided through a bridge. Since Firewalls are an absolute

necessity for anyone hardwired to the Internet, a Cisco Pix 506E [7] protects one segment and a Sonicwall SOHO3 [8] protects the other. The access control lists are as tightly set up as possible, although this is reviewed on a regular basis, as are the logs.

B) Antivirus Software
Antivirus software has been a must for most Internet users for several years especially for email users. At first I was able to keep up with the needs by purchasing and installing Symantec's Norton Antivirus [9] on each workstation. However making sure that each machine was getting updated properly became cumbersome. Symantec Corporate Edition [10] is now used to keep the users updated and protected. I can monitor the status of the definitions from a central location, and I am paged if any virus activity is caught.

C) Operating System and Software Updates
Keeping current on software updates and patches for the Operating Systems and Applications is a large challenge, and a centralized management method is fast becoming a necessity. We are using tools like Shavlik's free HfnetChk utility [11] to help in the endeavor, and I also make sure Email clients and Office applications are kept current.

D) Server and Workstation Security
Securing existing Servers and Workstations is currently an on-going project. NTFS is used everywhere possible. Units are secured using the Win2k Gold Standard [12] before going into production. Unneeded services are disabled. User permissions and Local Security Policies are carefully setup. Vulnerability scanning is done periodically to test for problem areas. System logs are examined on a regular basis. Since most of these procedures cannot be implemented on the Windows 98 platforms, those machines are being replaced by newer ones as opportunity and finances allow. The dumb terminals use serial connections to AIX, so the main security for these is provided by physical security and password policies. The AIX O/S is also scrutinized for needed updates, rogue users, improper activity, unneeded services etc….

E) Physical Security
Physical access to the Servers is controlled by lock and key. About half of the workstations are in areas not easily accessible by the public, the other half are located in areas where clinic personnel are present at all times.

F) Backups
Backups are considered very very important. Tapes are rotated on a regular basis and are stored off site. Backup Logs are also kept on and off site.

G) Passwords
Passwords are the foundation of security in many ways. Without good passwords, many good security features can easily be by-passed. User training is an ongoing project and more comprehensive user training is being planned for the near future.

H) Applications
Applications are an area that will need future work with the software vendors. Some have good password schemes and others do not. This will be an ongoing effort.

Risk Analysis Conclusion:

I have been involved with installing and maintaining lots of Practice Management systems in Doctors offices since 1991. I covered a large geographic area with both large and small cities. I've had the opportunity to help clinics recover from: failed hard drives, employee caused damage (a jealous wife purposefully knocked over a server), and even lightning damage. These incidents really were few and far between considering how many users and servers were out there. Confidentiality, Integrity, and Availability of Information was fairly easy to accomplish, that is, before Internet access came into the picture.

Now as I analyze the dangers posed by the various threats and vulnerabilities that are inherent in having information systems connected to the Internet; and as I look at how likely an incident is to occur, the conclusion I come to is that Internet connectivity poses a great risk. There are malicious people that want to harm my stuff and it is very easy to give them an avenue of attack. Even software vulnerabilities and configuration errors would not be as significant if it weren't for the threat posed by Internet access.

I judge that we are doing fairly well at protecting our assets at the current time. I make sure we are protected by firewalls; I have a good anti-virus system in place; and I update and patch our software. I endeavor to properly setup network shares, maintain the access control lists, strive to train the users, and we have disaster recovery procedures in place. But, new vulnerabilities are discovered daily, configuration errors are easily made, and even if periodic vulnerability scanning shows that things are safe, a well trained user can still inadvertently click on a malicious email attachment or visit and get infected by a compromised web site that can then lead to other exploits. As the authors of Hack Proofing Your Network say, "You cannot design a client-side security mechanism that users cannot eventually defeat, should they choose to do so," (Russell 14)[13].

Therefore, I think the best way I can take our level of security to a higher level is through Intrusion Detection. I need to know if anything is happening on the network that I should be aware of.

The Middle: Implementing the Safeguard.

In order to put an Intrusion Detection System into operation, I had to decide which kind to put in first. Host based or Network based. I chose Network based as the first kind to implement for several reasons. Working on the servers is tricky because of the proprietary nature of the various medical applications. Getting vendor approval and testing for a host-based system would be a lengthy process. I also think installing a host-based system on the each workstation would initially cause a lot of user confusion, increased support calls, and be more difficult to monitor, fine tune and keep updated. But as we grow in our experience with Intrusion Detection, a centrally managed host-based product will definitely be considered so we can have both kinds of Detection in operation. For now, a Network based IDS will let me monitor the network immediately while evaluating the next security steps to take. “Because they are constantly monitoring the network, IDSs help to detect attacks and abnormal conditions both internally and externally in the network, and provide another level of security from inside attack,” (Russell 27)[14].

For a Network based Intrusion Detection System (NIDS) to be implemented effectively some guidelines must be established. The NIDS must be fairly easy to use, must be updated regularly, the rules must be tunable to our needs, the alerting capabilities must be robust, and support must be available in case problems arise.

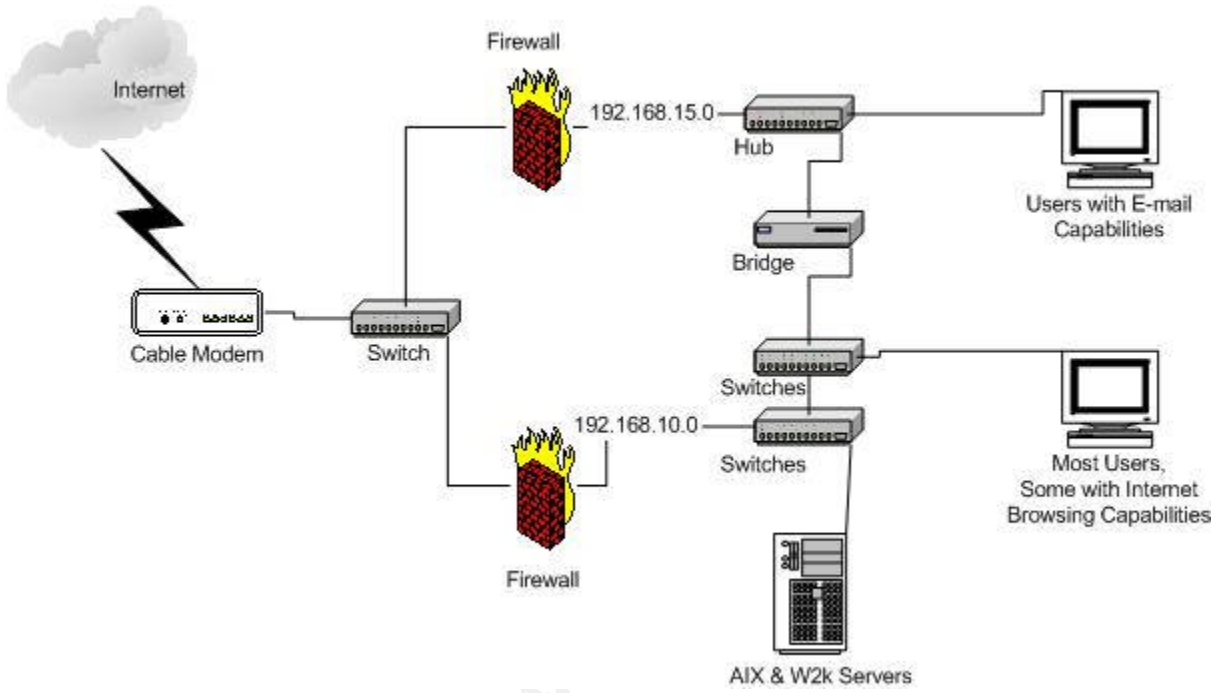
Snort [15], the free, open source NIDS was chosen as a beginning point for those reasons and because of a few others. It was featured in the SANS “Security Essentials Hands on Training” [16], which I took as an endorsement, and Snort has been mentioned several times over the years on the TechRepublic [17] web site. TechRepublic is a great resource for IT information. I have been on their mailing lists for years now and highly recommend them. Since snort is free, it is also a great tool to experiment with to become familiar with Intrusion Detection features, principles, and problems, before delving into other vendors and solutions.

Getting Started:

The machine that I have available to start with is a PIII 500mhz unit with 256mb of RAM. It has two network cards configured for different subnets (I’m hoping to monitor one network, while accessing the machine from another network). I could’ve installed and used the Linux OS, but I chose Windows 2000 to eliminate the additional learning curve that I would’ve had with Linux. I brought the machine up to the latest Service Pack and security patches. I also used the benchmarks and tools from the Center for Internet Security [18] to further measurably secure the unit following the recommendations from the SANS Gold Standard Training[tm] [19] that I received in Aug. of 2002. I also disabled NetBIOS,

unneeded services, File and Printer sharing; and restricted anonymous users. Also the security properties was changed from 'Users' to 'Authenticated Users' on the C:\ drive, and subfolders.

This is our network before implementing a Network Intrusion Detection System:

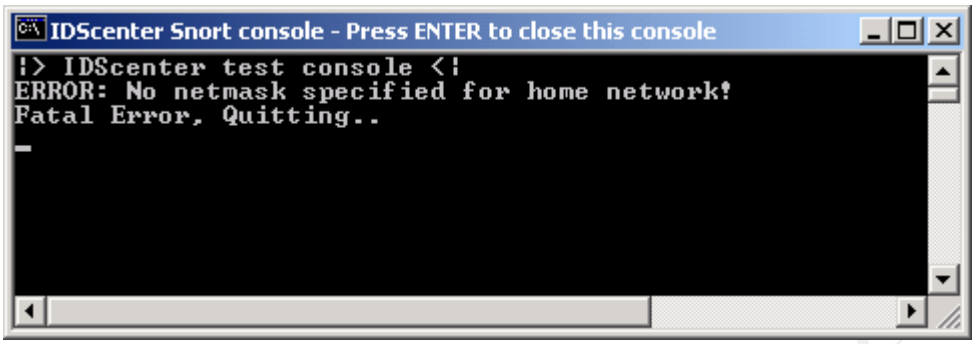


Before I began installing any software I researched the Snort website: www.snort.org [20] to find out what was needed to run Snort on Windows. The article: "Snort's Place in a Windows 2000 Environment" by Jon Bull [21] was my starting point. I downloaded the Snort 2.1.0 binary and then obtained WinPcap 3.0 [22] for the packet capture driver. I also decided to use Engage Security's IDScenter 1.1 RC4 [23] as the front end GUI after rereading Chapter 10 in the SANS Security Essentials Hands-On Workbook. [24]

How and Where to Monitor: Hub, Tap or a Switch? A very big question! I settled on a hub since my initial test network is fairly small, and the hub was already in place. In the future more research will be done on finding a switch with spanning capabilities or finding a network tap for working with the larger network. For this initial phase of implementing and testing a NIDS, the hub works great.

The Installation:

All of the software downloaded and installed without a hitch. I used the SANS Security Essentials Hands-On Workbook [24] and the IDScenter 1.1 Manual [25] as my guides. I went through all of the recommended settings and felt I was ready. However, when I tried to run the "Test Settings" button on IDScenter, I encountered my first problem, a "Fatal Error!"



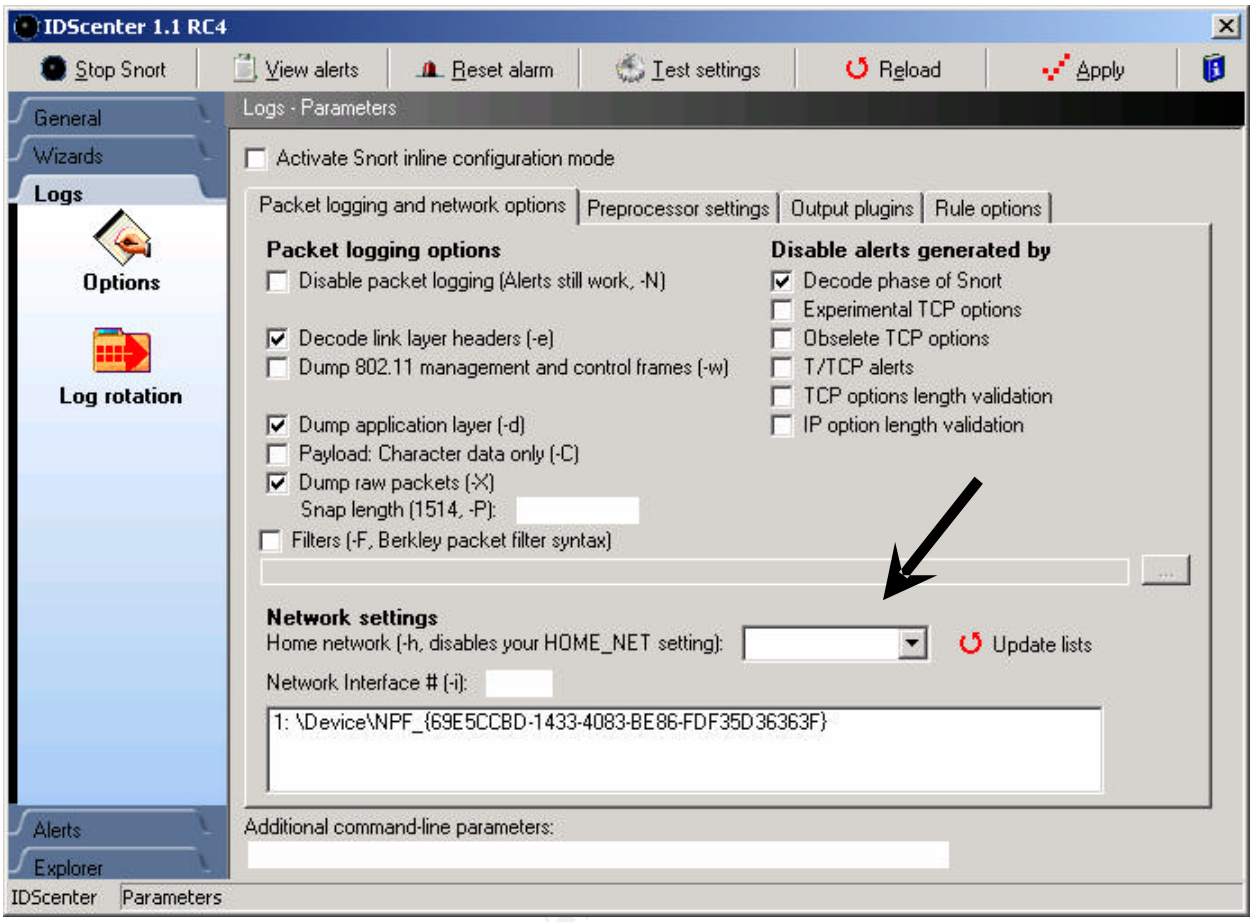
For some reason, Snort and IDScenter don't think that I have a Netmask configured!

I spent a day trying to figure this one out; I used forums and web searches. Found a lot of good information, but nothing pertaining to my problem. I reconfigured the snort.conf file repeatedly using the proper CIDR naming convention. I made sure over and over again that when I pulled up the Wizards tab and selected the 'Network Variables', that my IP address was correct. I made changes to this area and made sure they were reflected in the snort.conf file, but still I came up with the same error. In the Logs -> Options panel -> Network Settings, the IP address was correct here too. Note: for some reason I couldn't get registered with the Snort support forum; I couldn't get my confirmation email back to them, so that was a closed door for answers on this particular problem.

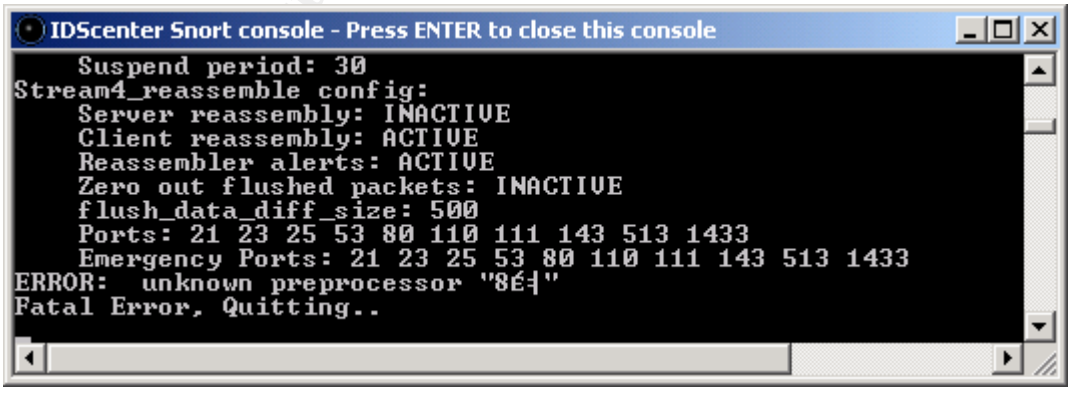
Finally I emailed Ueli Kistler, the IDScenter author and Webmaster. He was very very gracious to write back and tell me where to look. He said to go to the Logs -> Options panel, then to the "Network settings" and an edit box for "Home Network". He then said to remove what is written in this edit box. It's not clear to me but it seems this box is for disabling the HOME_NET setting, I thought the note in the parenthesis was telling me I could use the –h if I wanted to.

A big 'Thank You' to Ueli, for helping me to resolve this!

Please see the next page for a screen shot of the Options panel that I'm talking about.



I immediately made the change and his instructions got me past that initial error to my next challenge. The next problem that came up was obviously in the preprocessor area:



I tried taking out various preprocessor options and retesting. The point at which the error occurred would change, and the garbled characters would change slightly, but obviously there was something I wasn't doing right. After carefully examining the snort.conf file and reading the Snort manual I found this section:

```
# http_inspect: normalize and detect HTTP traffic and protocol
# anomalies.
# lots of options available here. See doc/README.http_inspect.
# unicode.map should be wherever your snort.conf lives, or given
# a full path to where snort can find it.
preprocessor http_inspect: global \
   iis_unicode_map unicode.map 1252

preprocessor http_inspect_server: server default \
   profile all \
   ports { 80 8080 }
#
#  Example unqiue server configuration
#
# preprocessor http_inspect_server: server 1.1.1.1 \
# ports { 80 3128 8080 } \
# flow_depth 0 \
# ascii no \
# double_decode yes \
# non_rfc_char { 0x00 } \
# chunk_length 500000 \
# non_strict \
# no_alerts
```

Section 2.8.10 of the Snort manual says this HttpInspect area “is a generic HTTP decoder for user applications,”(Roesch, Green)[26]. This sounded like an area for customized setups so I commented out both of these preprocessors and was able to begin testing again. Once I had figured out which preprocessor caused the problem, I cleared all preprocessors, and then added them back in one at a time, testing them as I went. I came up with a configuration very similar to the Hands on Workbook and the IDScenter manual.

Further testing brought some more fatal errors referring to various types of server functions. Further investigation revealed that other Server variables had disappeared from the configuration file, so I added those back in:

```
var DNS_SERVERS $HOME_NET
var SMTP_SERVERS $HOME_NET
var HTTP_SERVERS $HOME_NET
var SQL_SERVERS $HOME_NET
var TELNET_SERVERS $HOME_NET
var HTTP_PORTS 80
var SHELLCODE_PORTS !80
var ORACLE_PORTS 1521
var AIM_SERVERS [64.12.24.0/24,64.12.25.0/24,64.12.26.14/24,64.12.28.0/24,
        64.12.29.0/24, 64.12.161.0/24,64.12.163.0/24,205.188.5.0/24,205.188.9.0/24]
```

At last the configuration tester worked and Snort seemed to be running. I was excited to begin testing it with a port scanner. Then….

Yet one more problem cropped up! I was getting absolutely no logging activity! After going through the different settings a thousand times, I remembered seeing a question about problems with having multiple network cards on Windows computers on the Engage Security IDScenter forum site.[27] As an experiment I took the other NIC out and the alert log finally started working. The answer in the forum says that multiple instances of Snort can be run to support multiple NICs, but no answer was given on how to do it. This will be a great project for another day.

The Testing:

Finally I could begin testing the Intrusion Detection System. I used 2 different tools: NmapWin v1.3.1[28] and Superscan v3.0 [29] Both worked well, and I ran several different types of scans such as: SYN stealth, FIN Stealth, Null scan, Xmas Tree, and ACK scans. Snort immediately picked up on the scans and reported them, usually as something similar to this:

```
[**] [1:469:1] ICMP PING NMAP [**]
[Classification: Attempted Information Leak] [Priority: 2]
01/24-19:06:01.422581 0:B:DB:16:1D:D3 -> 0:40:5:D:D3:D0 type:0x800 len:0x3C
0.0.0.0 -> 192.168.15.186 ICMP TTL:50 TOS:0x0 ID:55152 IpLen:20 DgmLen:28
Type:8  Code:0  ID:51031   Seq:0  ECHO
[Xref => http://www.whitehats.com/info/IDS162]
```

I set Snort to start playing an alarm sound when it alerts, so anytime I hear that sound, I can investigate. By hooking up a modem I could even have it ring my cell phone as well.

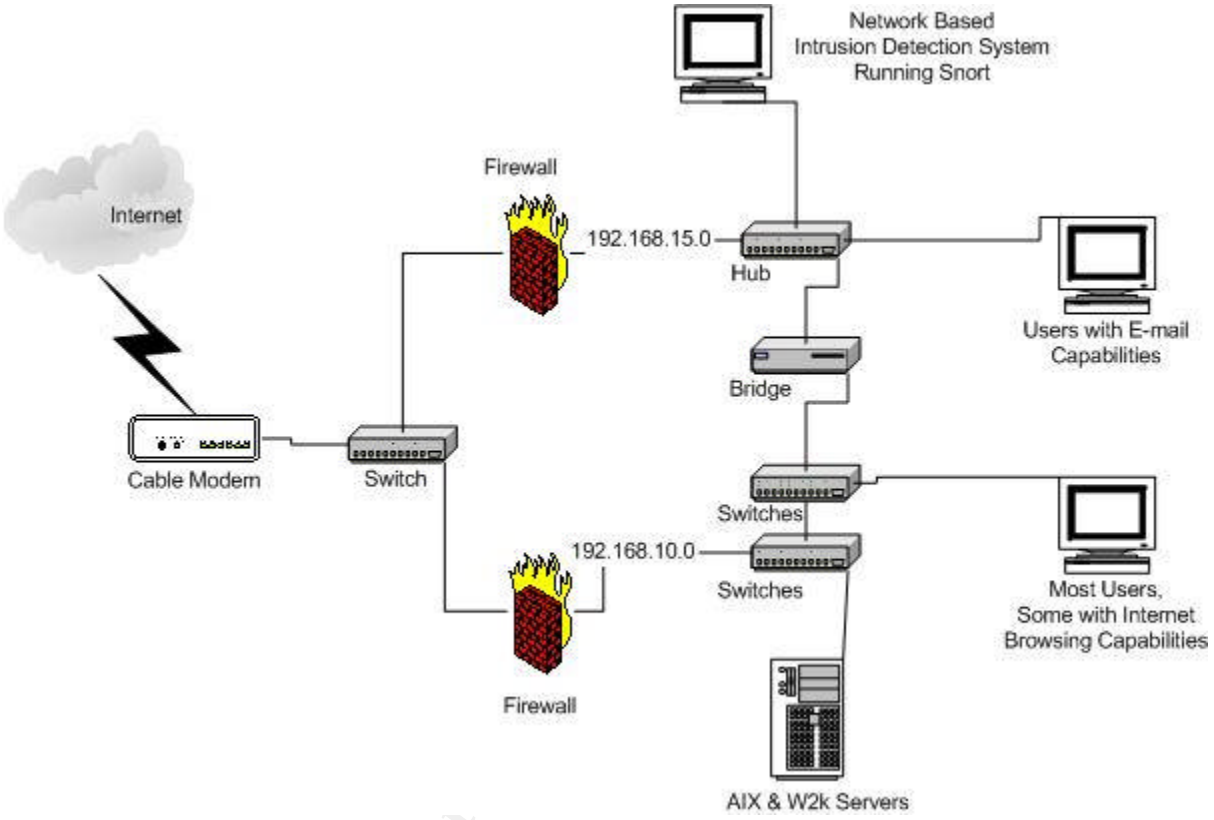
The only false positive I've encountered so far is that the system alerts me when users simply browse the Internet. Snort sees that as a scan:

```
Portscan detected from 192.168.15.30: 6 targets 6 ports in 20 seconds
```

By turning off the Portscan2 preprocessor I no longer get the false positives, and testing with Nmap shows that I'm still getting alerted for scans. However the Superscan testing isn't setting off the alarms. So I will continue to fine tune and test the system in order to make sure it is accurate and ready for the other production network. Tim Crothers in his excellent book talks about the daunting task of handling false positives, "The single biggest challenge faced when administering intrusion detection is all of the false alerts," (Crothers 128) [30] Now the real work can begin!

Not the End: Where to go from here?

Phase 1 Installation and testing is now complete and this is what the network looks like now:



Well, how have I done? Have I met my goals? I have taken a further step in securing our information by implementing a Network Based Intrusion Detection System on a network that hosts email users. I will have a better view of what is happening on that network. Did it meet the guidelines I had set? Mostly, I found Snort to be:

Easy to Install:	Fair, I thought it would be easier.
Easy to use:	Yes it is easy to use.
Updated regularly:	Yes it is updated regularly.
Tunable rules:	Yes the rules are flexible.
Good alerting:	Yes, I can be alerted in a number of ways.
Available Support:	Fair, but my experience is clouded by the inability to get registered with the support forum.
Good learning tool:	Yes, a great way to jump in and learn.
Effective:	Yes, it is effective at monitoring the network.

I am now at the threshold of taking the next steps of fine-tuning the IDS system and doing much more extensive testing so that I can implement it on the other network segment. After that, plans are in the works for more thorough vulnerability assessments and better user training.

As I stated in the beginning, security is a constant ongoing process.

The training I received at the SANS GSEC course taught me the principle of "Defense in Depth". This comprehensive way at looking at security challenges me and enables me to continually review and evaluate the many ways that security must be provided for. I now know that I have to examine all of the layers of an Information System. Layers such as policies, passwords, network components and shares, operating systems, Host based Intrusion Detection, applications, Internet browsing, e-mail, auditing, user training, services, physical security, disaster recovery, detection and incident handling, scanning, testing and retesting configurations.

Every aspect must be thought of and the appropriate measures taken for the protection of our information. I definitely feel like I couldn't do any of this without the SANS Institute, and I definitely look forward to receiving more training from them to further enhance my abilities to secure our environment.

References:

1. Cole, Fossen, Northcut, Pomeranz. SANS Security Essentials with CISSP CBK. SANS Press, Feb. 2003.

2. "Glossary." Symantec Security Response. http://securityresponse.symantec.com/avcenter/refa.html#b (Jan 2004)

3. Colley, Andrew. "New Internet Virus Draws Comparison to Previous One." The New York Times**.** CNET News.com. January 19, 2004. http://www.nytimes.com/cnet/CNET_2100-7349_3-5143115.html?ex=1075870800&en=7715b2071fc4834b&ei=5004&partner=UNTD (Jan 2004)

4. "Latest Virus Threats." Symantec Security Response. http://securityresponse.symantec.com/ (Jan 2004)

5. "@RISK: The Consensus Security Alert." Computer Security Newsletters and Digests. http://www.sans.org/newsletters/ (Jan 2004)

6. "Wily E-Mail Worm Spreading Fast." Jan. 27, 2004. The Associated Press. http://www.cbsnews.com/stories/2004/01/27/tech/main596296.shtml

7. "Cisco PIX 506E Firewall" http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps4336/index.html (Jan 2004)

8. "Sonicwall SOHO3" http://www.sonicwall.com/products/soho3.html (Jan 2004)

9. "Symantec Antivirus" http://www.symantec.com/nav/nav_9xnt/ (Jan 2004)

10. "Symantec Antivirus Corporate Edition" http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=155&EID=0 (Jan 2004)

11. "FNetChk.exe." Shavlik Technologies, LLC. Copyright © 1997-2004. http://www.shavlik.com/pHFNetChkEXE.aspx (Jan 2004)

12. Bower, Farrington, Weber. Securing Windows 2000 HANDS-ON. SANS Press, 2002.

13. Ahmad, Russell et al. Hack Proofing Your Network. Rockland: Syngress Publishing Inc., 2002. 14.

14. Ahmad, Russell et al. Hack Proofing Your Network. Rockland: Syngress Publishing Inc., 2002. 27.

15. Caswell, Brian; Roesch, Marty. “Snort, The Open Source Network Intrusion Detection System”. Jan 2004. www.snort.org

16. Cole, Eric. SANS Security Essentials Hands-On Workbook. SANS Press, 2003

17. TechRepublic. CNET Networks, Inc. http://techrepublic.com (Jan 2004)

18. “Benchmarks/Tools.” The Center for Internet Security. 2003 http://www.cisecurity.com/bench_win2000.html (Jan 2004)

19. Bower, Ben; Farrington, Dean; Weber, Chris. Securing Windows 2000 HANDS-ON. SANS Press, 2002.

20. Caswell, Brian; Roesch, Marty. “Snort, The Open Source Network Intrusion Detection System”. Jan 2004. www.snort.org

21. Bull, Jon. “Snort's Place in a Windows 2000 Environment”. 4/15/02 http://www.snort.org/docs/snort-win2k.htm (Jan 2004)

22. Viano, Varenni, Risso, Degaioanni. “WinPcap: the Free Packet Capture Architecture for Windows” 09/16/2003. http://winpcap.polito.it/install/default.htm (Jan 2004)

23. Kistler, Ueli. “IDScenter - Snort IDS configuration and management front end.” v. 1.1 RC4. Mar 2003. http://www.engagesecurity.com/products/idscenter/

24. Cole, Eric. SANS Security Essentials Hands-On Workbook. SANS Press, 2003 Chap.10

25. Kistler, Ueli. “Snort IDScenter 1.1 manual” 2003. http://www.engagesecurity.com/docs/idscenter/ (Jan 2004)

26. Roesch, Martin; Green, Chris. Snort™ Users Manual 2.1.0. Jan 6, 2004. http://www.snort.org/docs/snort_manual.pdf (Jan 2004)

27. “IDS Center Forum” Engage Security Forums. 2003 http://www.engagesecurity.com/forum/viewforum.php?f=2&sid=214c31b3dcbf559925f1ad4c4cf6f80a (Jan 2004)

28. Vogt, Jens. “nmapwin” v. 1.3.1 Nov. 19, 2002. SourceForge.net http://prdownloads.sourceforge.net/nmapwin/nmapwin_1.3.1.exe?download (Jan 2004)

29. “SuperScan 3.0” Foundstone, Inc. 2002 http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/freetools.htm (Jan 2004)

30. Crothers, Tim. Implementing Intrusion Detection Systems. Indianapolis: Wiley Publishing Inc, 2003. 128.

Last Updated: May 29th, 2017

Upcoming Training

SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event