Global Information Assurance Certification Paper

ASSIGNMENT 1 Describe the State of Intrusion Detection

Strategies for a New Intrusion Detection System - Avoiding Pitfalls

In the course of planning for and implementing an Intrusion Detection System (IDS), several pitfalls can slow or completely stop forward progress, especially in large agencies or corporations. Some of these problem areas can be avoided and others can be mitigated with foreknowledge and proper preparation. This paper identifies several important issues and provides possible solutions at a greater depth than some single-topic point papers. The intended audience is the up and coming IDS Program Manager or Team Lead who needs his/her agency to get serious about computer defense.

HELP SENIOR MANAGEMENT UNDERSTAND

Sometimes the client or senior project manager, referred here after as "the boss", may not have a complete understanding of the whole information assurance/computer security problem. Worse, the boss may think that he/she knows enough to tell you how to do your job when he really does not. In either of these situations, you must concurrently work your program while educating your boss. If you and your boss are not seeing the same problems or agreeing on a common solution, it is very likely the program will fail or new people will be brought in to start over.

Several items will help you and your boss gain a common understanding of the program. Developing a clear concept of operations (CONOPS) with simple but complete diagrams is very important. As with good software specifications, your CONOPS should be clear and understandable by a non-computer specialist. Your boss should feel comfortable enough in his understanding of the program so he can brief the concept to his boss. Providing a little more background in each of your communications (e.g., email, progress reports, program reviews) will also be beneficial. Getting the boss to attend a managers track at the next GIAC conference may or may not help, depending on his/her technical background. For those located near larger cities, free product demonstrations or mini-technical seminars are frequently put on by IDS product vendors.

You should avoid information overload but ensure that you and your boss cover a complete IDS deployment scenario. Engineers easily slip into design details that bore or intimidate the boss. Provide the details at the rate at which you feel they can be absorbed. Think about the rule of thumb of no more than five to seven objects on a briefing slide. Make a personal list of your major program elements (e.g., CONOPS, schedule, hardware/software procurement, staffing) and make sure that you get some time up-front to brief and reach consensus with your boss. Remember, when the boss understands your program, he can more easily defend his budget requests and new procurements or staffing requirements.

The CONOPS should reinforce three primary points to senior management: topography of the sensor network, staffing needs and data retention. First, the IDS needs to see everything that is important. Placement of sensors is critical. Secondly, the IDS will not be functional without trained engineers and analysts. Personnel must be on-site in order to respond to events as they occur. Without around-the-clock staffing that is experienced and empowered to respond to threats, you are simply looking at day old history reports. IDS staff will also need to be available during operations to support forensic analysis and to tweak sensor settings/rules as the threat continues to change. Additional comments are made about personnel costs in the next section. Finally, the IDS must be able to store everything it sees. The amount of data retained can be tiered based on its age. For example, keep a week or month of full-packet data on-line. Everything older than that can be reduced header data, possible moving it to off-line tape or CD/DVD storage for use in post-event analysis or long-term trending.

DEVELOP A CLEAR CONCEPT OF OPERATIONS

It is very important that you help the boss visualize what the complete IDS will look like and what it will be able to accomplish once it is setup. Managers get uncomfortable when the are waiting for something to be delivered that they can't anticipate or track. By default, it is your job to provide the following items to the boss: software list (including license requirements and costs); hardware list (with major component specifications: cpu speed, RAM, disk capacity); logical data flow from sensor to back-end visualization tool or database

Few IT managers understand the full range of information that can be obtained from an IDS. A variety of presentations or diagrams will help the boss understand what all this new system will be able to provide. These same presentations will provide a starting point for discussions when developing external report formats for customers. External reports cover the gambit of analysis data for the CIRT/CERT, CIO executive summary, excerpts for the IA/Accreditation team or complementary reports for the network enterprise monitoring System Analysts. Snapshots of sample screens are a major help, though sometimes people can get stuck on a certain button or layout. Inform your reviewers whether certain items are customizable or not.

The boss needs to be aware of the data management strategy you are developing and how much storage, both on-line and off-line, will be required to support the IDS. Develop some estimate of data volume to be captured each day. Build that into an equation that illustrates the monthly data capture. Translate the data flow into storage units and quantify how much rack or shelf space will be required for a year's worth of data (including disk arrays and off-line tape storage). The data volume estimates may also translate into increased LAN/WAN bandwidth utilization, depending on the network path used between sensor and data collector.

HOW MUCH DOES IT COST?

There are many quick responses to the question of cost. "You get what you pay for", "Anything good is worth the money", and so forth. It is important to establish the fact that the cost of a quality IDS program is NOT free. However, it can be done without tremendous expense and it can be done in stages as your IDS team matures in its ability to handle more responsibilities.

Probably the greatest single expense in establishing an IDS is people. Free, open-source sensors exist, as do firewalls, scanners, databases and back end visualization tools. See Deploying Open Sourced Network Intrusion Detection for the Enterprise, TJ Vanderpoel, March 4, 2001 http://www.sans.org/newlook/resources/IDFAQ/open_source.htm . However, competent staff is needed to put it all together and operate it. Unqualified or untrained staff will cost more in the long run, as they learn on-the-job, than those with more experience (and usually with higher salaries). Even the fantastic graphical user interfaces (GUIs) and help pages that come with more expensive commercial IDS products cannot make up for the efficiency of a well trained operator/analyst or the productivity of experienced programmer. This does not mean that everyone on the IDS team must have a minimum of ten years of experience. However, a wise manager will invest in a core of well-qualified staff that is capable of training the junior team members.

Some managers incorrectly assume that the IDS will run itself after the high-priced engineers set it all up. Kill this thought as quick as you can. Make it known that the IDS program will require expertise in the construction phase as well as competent 7x24 staff to sustain operations. This staffing profile should have been established back in the CONOPS.

Hardware is likely to be the second greatest expense. The focus on sensor hardware should be fast CPUs, fast disk drives and fast network interface cards (NICs). Take time to consider the IDS vendors recommendations on minimum hardware configurations. Go ahead and ask the technical representative what environment the IDS tools perform with best.

HOW LONG WILL IT TAKE?

Before signing up to an installation deadline, be sure that you have fully scoped out the size of the job and assure yourself that there is a method in place to quickly resolve engineering issues. Possible hindrances to bringing a new IDS on-line include, but are not limited to: hardware acquisition delays, stringent organizational configuration management practices and review boards for new software to be added to the corporate baseline.

Work with the boss to outline whatever review/approval/acquisition cycle will be needed. Look to see if any temporary authorizations could be obtained for a “proof of concept” IDS installation. Build every contingent (e.g., funds available at the beginning of the fiscal year) into some type of schedule dependency.

A simple prototype will provide you with many benefits. An inexpensive setup with SNORT capturing data can use SnortSnarf or other tools at little or no cost. This in-turn will allow you to review traffic and begin normalization (canceling out background alerts from local traffic). Data collected here can form the initial sizing estimates and can be formatted for sample reports.

WHICH IDS TO CHOOSE?

Of course, this is the million-dollar question isn’t it? Actually, that figure is not too far off if multiple sensor/console licenses are purchased for a large corporation that wants to effectively

protect it's critical networking infrastructure and corporate data from loss. In a nutshell, the ideal IDS works with heterogeneous sensors from multiple vendors, ports to all operating systems, talks through the firewall, integrates common sys-log files from non-sensors for correlation, comes with just the right default reports that your customers need and is free. In reality, this system does not exist, though many salesmen will tell you different. You have to prioritize the features that are important to your customer. The features listed above are suitable "goals" that could be used as selection criteria.

The size and complexity of the network will help determine the number and variety of sensors that are required. In a large organization, both network and host-based sensors would be the norm. Depending on the manpower available for monitoring, some sensors may be setup to provide alerts, while others keep filling the log files with full data capture. Non-IDS systems, such as routers and firewalls, also have log data that could be correlated with intrusion events. An IDS that can collect data from many different vendor IDS' as well as commonly used perimeter routers and firewalls would provide maximum flexibility and would be a wise investment.

Operating systems must be assessed if optimum IDS performance is desired. Most commercial IDS' consoles operate on the usual NT, Win2K or Solaris platforms. But sensor performance will vary greatly based on system components that are not usually scrutinized so closely when buying normal desktop support machines. A little time should be spent reviewing minimum system requirements and optimum system requirements (e.g., Snort really likes BSD and Compaq NICs really scream). Ask the vendors if any particular components, like CPU clock speed, disk access time, network interface speed and backplane speed, are particularly important to their product.

Before making that final IDS selection, get some assurances from the vendor that their product will operate in your network environment. For instance, not all IDS' are "proxy-firewall friendly", so you may have to locate a console and database outside your perimeter if the sensors cannot be polled from behind the firewall. If possible, try before you buy. If there is time for demonstration, by all means, do so. Invite each vendor to show how his or her system could operate in your network architecture. Have them bring an engineer, not just the sales person. However, be painfully clear with them on the target network architecture.

HOW DO YOU MANAGE ALL THIS DATA?

Effective knowledge management will make the difference in having a usable IDS or having a useless report generator. Your IDS will have reams of data to serve up, but it will be ineffective if it is not easily digested by the end-user – your analysts.

There are a couple of data fusion concepts that you should become familiar with to see if they have any applicability in your situation [http://www.silkroad.com/papers/html/ids/n1.html]. A working knowledge of the IDS data integration problem is becoming as important as knowing the exploits and vulnerabilities. It is also important since the current state of IDS visualization is not quite as mature as it could be.

Several commercial products are making very good strides to pull heterogeneous sensor and system log information together into useful formats. Automated Intrusion Detection Environment, Advance Concept Technology Demo is being worked through DISA to support data integration for the Defense Department [http://www.acsac.org/1999/papers/wed-c-1030-prc.pdf]. ISS has developed its detection and scanner tools with a decision tool called Safe Suite Decisions [http://www.iss.net/securing_e-business/security_products/security_management/decisions/]. This application provides some capability of correlating non-sensor system logs and integrates scanning reports to help prioritize administrative efforts to secure high value systems. The SilentRunner® application, from Raytheon Company, http://documents.iss.net/literature/SilentRunner/sr10_ps.pdf allows administrators to rapidly overlay large security data sets – including RealSecure™ log data – from disparate sources. It uses advanced analysis algorithms to identify anomalous or suspicious events for further investigation. Intrusion Vision is a visualization and data management tool developed by General Dynamics that can be used with commercial and public domain intrusion detection systems. Alerts are analyzed in near-real time by the Intrusion Vision Event Manager, graded by severity and categorized by type. http://www.gd-decisionsystems.com/intrusionvision/main.html.

Itemize the capabilities your candidate IDS systems have for source IP or event-time correlation. Go through the product reviews or demos at a trade-show or at the vendor facility to see what reports come out of the box and what interface programming language is available. Check to see what file formats can be exported and imported and whether the basic data storage system is a commercial database or proprietary file format. The former provides for local tailoring of queries and reports while the later usually means you are stuck with what they give you.

STAYING ON THE CRITIAL PATH

At some point you must select the product(s) you are going to use. Once you do, stay on track and avoid being dragged into a new product review every week. Unless some unforeseen roadblock arises, get your solution in place as soon as possible. If you are not part of the ongoing operations and maintenance, encourage the customer to establish an engineering/review team. This team can periodically review products to see what new technology should be inserted into the established baseline.

Beware of falling into a trap of starting IDS reports before the system is fully on-line. If you do set up a prototype, or get an initial network sensor operating, there will be a tendency (or a request from management) to report what you have. Once you do that, your engineering and integration staff will effectively be reduced in size because someone will constantly have to generate reports and respond to management questions on IDS events. While it would be prudent to keep an eye on any data that is being generated, don't let it be circulated to widely that there is an operational system before you are ready to staff it full-time.

Additionally, you will need some time to normalize the network traffic. That is, there will be detects that are not attacks but 'normal' traffic. If there are load-balancing switches on your networks, they most likely employ some ICMP Ping or other health check that might appear to

be a ping flood to the IDS. Other network enterprise monitoring systems (NEMS) will also be sending frequent packets to their subordinate systems to ensure health and to measure network efficiency. All of this must be filtered out of your detects or minimized so your team can focus on the real threat.

The bottom line is that the CND effort can succeed with minimal delays when there is a clear understanding of the overall program, by all levels of management. This common understanding, fostered by clearly articulated CONOPS, requirements definition and proposed architectures will sustain the project through final tool selection and implementation. Finally, the sprint to the finish must be well focused to avoid terminal distractions.

References

How to guide – implementing a Network Based Intrusion Detection System
http://www.snort.org/docs/iss-placement.pdf

An Introduction to Intrusion Detection and Assessment for System and Network **Security Management, Prepared by Rebecca Bace from Infidel, Inc. for ICSA, Inc.**
http://www.icsa.net/html/communities/ids/White%20paper/Intrusion1.pdf

Network Intrusion Detection – An Analyst's Handbook, Second Edition, by Stephen Northcutt and Judy Novak

"Distributed Intrusion Detection with Open Source Tools" Sys Admin magazine, August 2001, Volume 10, Number 8, pp 20 - 25

Automated Intrusion Detection Environment, Advance Concept Technology Demo
http://www.acsac.org/1999/papers/wed-c-1030-prc.pdf

SilentRunner®, from Raytheon Company, http://documents.iss.net/literature/SilentRunner/sr10_ps.pdf

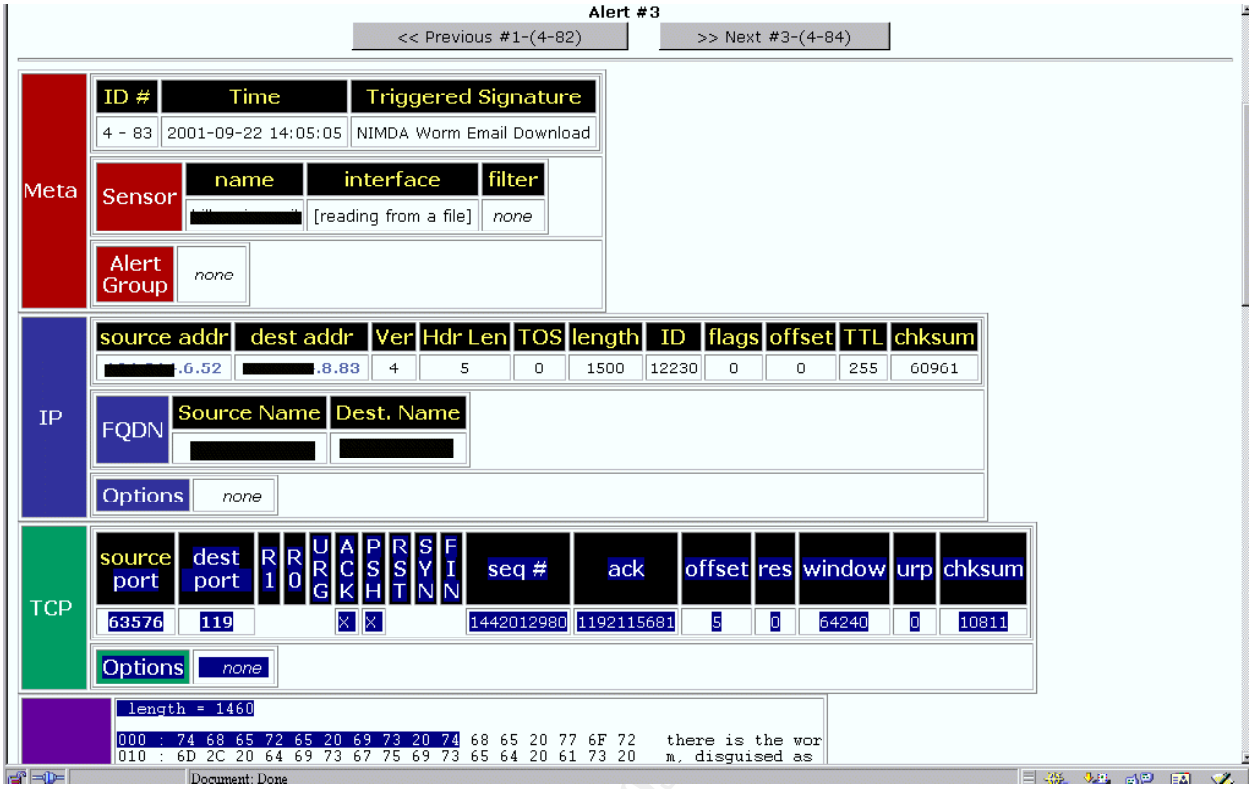
Intrusion Detection Systems & Multisensor Data Fusion: Creating Cyberspace Situational Awareness, byTim Bass, Communications of the ACM (accepted for publication February 26, 1999) http://www.silkroad.com/papers/html/ids/n1.html

Intrusion Vision from General Dynamics http://www.gd-decisionsystems.com/intrusionvision/main.html

ASSIGNMENT 2 Network Detects

Detect #1 Internal Network Detect of NIMDA via News Feed

Screen snapshot of ACID summary



length = 1460

```
               000 : 74 68 65 72 65 20 69 73 20 74 68 65 20 77 6F 72   there is the wor
               010 : 6D 2C 20 64 69 73 67 75 69 73 65 64 20 61 73 20   m, disguised as
               020 : 22 72 65 61 64 6D 65 2E 65 78 65 2E 22 20 20 4F   "readme.exe."  O
               030 : 75 74 6C 6F 6F 6B 0D 0A 3E 20 77 69 6C 6C 20 74   utlook..> will t
               040 : 68 65 6E 20 61 75 74 6F 6D 61 74 69 63 61 6C 6C   hen automaticall
               050 : 79 20 72 75 6E 20 69 74 2E 0D 0A 3E 20 0D 0A 3E   y run it...> ..>
               060 : 20 54 68 65 20 55 52 4C 73 20 6C 69 73 74 65 64    The URLs listed
               070 : 20 62 65 6C 6F 77 20 6D 69 67 68 74 20 68 65 6C    below might hel
               080 : 70 20 73 6F 6D 65 20 70 65 6F 70 6C 65 2E 20 20   p some people.
Break…
               4f0 : 0A 3E 20 0D 0A 3E 20 41 20 6E 65 77 20 63 6F 6D   .> ..> A new com
               500 : 70 75 74 65 72 20 77 6F 72 6D 20 63 61 6C 6C 65   puter worm calle
               510 : 64 20 4E 69 6D 64 61 20 73 74 61 72 74 65 64 20   d Nimda started
               520 : 63 69 72 63 75 6C 61 74 69 6E 67 20 74 68 65 20   circulating the
               530 : 77 6F 72 6C 64 20 74 68 69 73 20 77 65 65 6B 2C   world this week,
               540 : 0D 0A 3E 20 69 6E 66 65 63 74 69 6E 67 20 62 6F   ..> infecting bo
               550 : 74 68 20 65 6D 61 69 6C 20 61 6E 64 20 69 6E 74   th email and int
               560 : 65 72 6E 65 74 20 77 65 62 20 73 69 74 65 73 2E   ernet web sites.
               570 : 20 20 44 75 65 20 74 6F 20 74 68 65 20 68 69 67     Due to the hig
               580 : 68 20 69 6E 66 65 63 74 69 6F 6E 20 72 61 74 65   h infection rate
               590 : 0D 0A 3E 20 6F 66 20 74 68 69 73 20 6E 65 77 20   ..> of this new
               5a0 : 77 6F 72 6D 2C 20 69 6E 74 65 72 6E 65 74 20 74   worm, internet t
               5b0 : 72 61 66 66                                       raff
```

1. Source of Trace: This detect occurred on the internal corporate network. The specific sensor was located immediately inside the corporate firewall to monitor traffic that makes it through, whether by design or not.

2. Detect was generated by: Snort intrusion detection system (http://www.snort.org) based on the rule below. - Analysis Console for Intrusion Databases (ACID http://www.cert.org/kb/acid/) was used for correlation and analysis. This tool provides a very easy query and retrieval mechanism for SNORT data.

#local rules
alert tcp $HOME_NET any <> any any (content: "readme.eml";nocase;msg:"NIMDA Worm Web Download";)
alert tcp $HOME_NET any <> any any (content: "readme.exe";nocase;msg:"NIMDA Worm Email Download";)

3. Probability the source address was spoofed: Unlikely. Due to the nature of the proxy firewall, the source IP was correct

4. Description of attack: The trace shows a normal NNTP packet going to destination port 119. The payload shows text of an email message that would be expected from news groups. What triggered the alerts was the key words of the infecting files "readme.exe". However, in this case, the file was not an attachment, but simple being talked about in the email narrative. This was a false alert.

(NIMDA attack description from SANS) The worm attempts to propagate itself to new victims via four distinct mechanisms:

(1) The worm scans the Internet looking for web servers and attempts to exploit a number of Microsoft webserver vulnerabilities to gain control of a victim host. Once in control of a victim IIS/PWS server, the worm uses TFTP to transfer its code from the attacking machine to the victim. The file transferred via TFTP is named "Admin.dll". IIS 3.0, 4.0, and 5.0 are all affected, as are Personal Web Server (PWS) 1.0 and 3.0.

(2) The worm harvests email addresses from the Windows address book, user's inboxes/outboxes, and local HTML/HTM files [3,4] and sends itself to all addresses as an attachment named "readme.exe". Note that any x86 email software that uses a vulnerable version of Internet Explorer to display HTML messages [1] will automatically execute the malicious attachment if the message is merely opened or previewed [4]. This happens because the worm MIME encodes the attachment to take advantage of a known vulnerability called "Automatic Execution of Embedded MIME Types" (see CERT advisory CA-2001-06 [1]). Microsoft's Outlook and Outlook Express are the most typical victims. Every ten days the worm regenerates its list of email addresses and sends itself to all.

(3)If the worm successfully infects a web server, it uses the HTTP service to propagate itself to clients that browse the web server's pages. Upon infecting a victim server, the worm creates a MIME-encoded copy of itself named "README.EML" and traverses the directory tree searching for web-related files such as those with .HTML, .HTM, or .ASP extensions. Each time the worm finds a web content file, it appends a piece of JavaScript to the file. The JavaScript forces a download of README.EML to any client that views the file via a browser. Some versions of Internet Explorer will automatically execute the README.EML file and allow the worm to infect

the. client. The IE vulnerability issue here is the same as in the email propagation mechanism; that is, IE 5.5 SP1 or earlier is vulnerable to the "Automatic Execution of Embedded MIME Types" problem. Allowing JavaScript in the browser enables the worm to take advantage of the IE vulnerability.

(4) The worm is network aware and propagates via open file shares. It will copy itself to all directories, including those found on a network share, for which the user has write permission. The worm will search the shared drives for execuatables, and attach itself to each execuatble it finds. Any other host that accesses the share and loads one of these files can become infected.

5. Attack mechanism: Network attacks include exploitation of the "IIS/PWS Extended Unicode Directory Traversal Vulnerability", the "IIS/PWS Escaped Character Decoding Command Execution Vulnerability", and utilization of backdoors left behind by previous Code Red II and Sadmind infections.

6. Correlations: Several NIMDA probes have been received during this period, but none from the same source as this trace. Below are two traces two days prior, destined for a Sun web server. This payload clearly shows the command script (cmd.exe?) being sent to the web server on port 80

```
#(1 - 227460) [2001-09-20 07:25:33]  WEB-IIS cmd.exe access
IPv4: 164.125.30.79 -> MY.NET.2.59
      hlen=5 TOS=0 dlen=120 ID=17825 flags=0 offset=0 TTL=112 chksum=23297
TCP:  port=2902 -> dport: 80  flags=***AP*** seq=441972099
      ack=1745431376 off=5 res=0 win=17520 urp=0 chksum=15954
Payload:  length = 80

000 : 47 45 54 20 2F 63 2F 77 69 6E 6E 74 2F 73 79 73   GET /c/winnt/sys
010 : 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63   tem32/cmd.exe?/c
020 : 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48   +dir HTTP/1.0..H
030 : 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E 65   ost: www..Connne
040 : 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A   ction: close....

#(1 - 227461) [2001-09-20 07:26:18]  WEB-IIS cmd.exe access
IPv4: 164.125.30.79 -> MY.NET.2.59
      hlen=5 TOS=0 dlen=120 ID=35487 flags=0 offset=0 TTL=112 chksum=5635
TCP:  port=3466 -> dport: 80  flags=***AP*** seq=840122718
      ack=1772958355 off=5 res=0 win=17520 urp=0 chksum=53151
Payload:  length = 80

000 : 47 45 54 20 2F 64 2F 77 69 6E 6E 74 2F 73 79 73   GET /d/winnt/sys
010 : 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63   tem32/cmd.exe?/c
020 : 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48   +dir HTTP/1.0..H
030 : 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E 65   ost: www..Connne
040 : 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A   ction: close....
```

7. Evidence of active targeting: This does not appear to be an active targeting. Due to the distribution of email via news groups, this would more likely be a random spreading of the Worm via email. At best it could be described as a "shotgun" approach to targeting. The sender could not know who would be downloading news from a specific ISP.

8. Severity: To assess the severity, we'll use the formula from SANS: [Target Criticality + Attack Lethality] – [System Countermeasures + Network Countermeasures] = Attack Severity

My assessment would be [2+5] – [5+1] = 1 Attack Severity. (very low).

The organizational news server is not mission critical and it is not available to the general public. Internal NIMDA propagation could be very severe. However, the IDS is effective in detection and the individual desktop systems have been patched to prevent further spread of the Worm.

9. Defensive recommendation: This alert was actually a false positive. However, This detect was a wake up call for the Firewall Team. There was a high level of confidence that everything was being blocked, filtered or detected. The News proxy is open for inbound traffic, though external sources are filtered by IP to only allow the ISP master news server. As we came to discover, the News Proxy is a simple plug with no content scanning. Without an internal network sensor, the company could have faced a quick spread of the worm to unpatched systems.

The news server was temporarily taken out of service while the news feed was expired (flushed). There was no potential damage to the news server as it is a SUN platform and not vulnerable. The news feed was reconnected, but a close eye is kept on the internal sensor to see if any future worms try to come through.

10. Multiple choice test question:

Which one of the following is NOT a potential path by which the NIMDA worm could spread:

(a) SMTP (email)
(b) Open shares on NT systems
(c) NNTP (news feed)
(d) RealAudio

ANSWER: (d) Real Audio. The very prolific NIMDA worm was very inventive in the way it multiplied. Network security professionals should be aware of every possible avenue by which a worm attack might propagate when laying out their sensor network. Seemingly harmless news feeds could provide a path for indirect emails sent to a newsgroup to be read and spread from an internal corporate workstation.

Detect #2 TCP Overlap from Shared Intranet

Four of thirty alerts originating from **BAD.BOY.22.80**

From Port	Priority	Date	To	To Port	Event	Information
80	High	11/20/2001 7:54:21PM GMT	MY.NET.6.59	64,960	TCP_Overlap_Data	ResponseList
DISPLAY=Default:0,LOGDB=LogWithoutRaw:0						
						SourceEthernetAddress BA:DB:OY:07:B6:D0
						DestinationEthernetAddress MY:NE:T0:00:3B:83
						SourcePortName HTTP
						DestinationPortName 64960
						IANAProtocolId 6
80	High	11/20/2001 7:54:21PM GMT	MY.NET.6.59	64,961	TCP_Overlap_Data	ResponseList
DISPLAY=Default:0,LOGDB=LogWithoutRaw:0						
						SourceEthernetAddress BA:DB:OY:07:B6:D0
						DestinationEthernetAddress MY:NE:T0:00:3B:83
						SourcePortName HTTP
						DestinationPortName 64961
						IANAProtocolId 6
80	High	11/20/2001 8:07:32PM GMT	MY.NET.6.59	44,514	TCP_Overlap_Data	ResponseList
DISPLAY=Default:0,LOGDB=LogWithoutRaw:0						
						SourceEthernetAddress BA:DB:OY:07:B6:D0
						DestinationEthernetAddress MY:NE:T0:00:3B:83
						SourcePortName HTTP
						DestinationPortName 44514
						IANAProtocolId 6
80	High	11/20/2001 8:07:32PM GMT	MY.NET.6.59	44,515	TCP_Overlap_Data	ResponseList
DISPLAY=Default:0,LOGDB=LogWithoutRaw:0						
						SourceEthernetAddress BA:DB:OY:07:B6:D0
						DestinationEthernetAddress MY:NE:T0:00:3B:83
						IANAProtocolId 6
						SourcePortName HTTP
						DestinationPortName 44515

1. Source of Trace. This trace was a Real Secure Network Sensor detect from a shared corporate intranet.

2. Detect was generated by: Real Secure Network Sensor (www.iss.net) with the report extracted from Real Secure Console. Real Secure is a network and Server sensor developed by Internet Security System, Inc.

3. Probability the source address was spoofed: Unlikely. The system name resolves and it can be pinged. The fact that this occurred on a shared intranet makes be lean toward to probability of a misconfigured system .

4. Description of attack:.

This signature detects a discrepancy between overlapping TCP segments, which could indicate malfunctioning network equipment, or an attempt by an attacker to deliberately induce false negatives or false positives in a network monitoring tool or intrusion detection system, such as RealSecure.

5. Attack mechanism:

Data in TCP connections is broken into packet-sized segments for transmission. The target host must reassemble these segments into a contiguous stream to deliver it to an application. The TCP/IP specifications are not clear on what should happen if segments representing overlapping data occur and how to interpret such data. By deliberately constructing connections with overlapping but different data in them, attackers can attempt to cause an intrusion detection system or other network monitoring tool to misinterpret the intent of the connection. This can be used to deliberately induce false positives or false negatives in an intrusion detection system or network monitoring tool.

This type of traffic should never happen naturally on a network, but it has been observed in conjunction with malfunctioning network equipment.

This activity is not itself an attack, but in conjunction with other activity is either evidence of malicious intent or malfunctioning network equipment.

6. Correlations: There were only thirty alerts for this signature and BAD.BOY.22.80 was the only source. The alerts occurred over a thirteen minute interval. You can observe reflexive source and destination port numbers. Since the destination is a firewall for the organization, it is likely that this may be some HTTP web traffic that is triggering the event collector.

7. Evidence of active targeting:.

8. Severity: [Target Criticality + Attack Lethality] – [System Countermeasures + Network Countermeasures] = Attack Severity

The destination system is a firewall, though the attack is not considered lethal in this instance. The firewall has been fully patched and the sensor are in place to detect suspicious activity, so the countermeasure scores were high.

(Criticality 3 + Lethality 1) – (Sys Countermeasures 4 + Network Countermeasures 4) = -4 (very low Severity)

9. Defensive recommendation: We could call back to the system owners to check their system for correct configuration, but I suspect that this is simple web traffic.

10. Multiple Choice Test question:

What is the best countermeasure to stealthy scans or fragmented attacks?

A. Network address translation
B. Split DNS (inside/outside)
C. Stateful packet firewall
D. Application proxy firewall
E. All of the above

Answer – E All of the above. There is not much distinction between the countermeasures listed. They should all be able to disrupt, block or collect and analyze stealth scans or fragmented attacks.

Detect #3 HTTP_ActiveX

Event: HTTP_ActiveX

Date	Priority	From	To	Information
11/16/2001 8:43:36PM GMT	High	MY.NET.6.31	MY.NET.6.84	ResponseList

DISPLAY=Default:0,LOGDB=LogWithoutRaw:0

SourceEthernetAddress	08:00:20:AD:47:08
DestinationEthernetAddress	00:50:8B:C8:18:16
SourcePort	80
SourcePortName	HTTP

				DestinationPort	1180
				DestinationPortName	1180
				IANAProtocolId	6
11/19/2001	2:59:01PM GMT	High	MY.NET.6.51	NET.A.226.113	ResponseList
DISPLAY=Default:0,LOGDB=LogWithoutRaw:0					
				SourceEthernetAddress	MY:NE:T0:04:B1:39
				DestinationEthernetAddress	NET:A:07:B6:D0
				SourcePort	80
				SourcePortName	HTTP
				DestinationPort	1724
				DestinationPortName	1724
				IANAProtocolId	6
11/20/2001	4:57:44PM GMT	High	MY.NET.6.52	MY.NET.44.78	ResponseList
DISPLAY=Default:0,LOGDB=LogWithoutRaw:0					
				SourceEthernetAddress	08:00:20:88:73:95
				DestinationEthernetAddress	00:00:EF:07:80:50
				SourcePort	80
				SourcePortName	HTTP
				DestinationPort	2538
				DestinationPortName	2538
				IANAProtocolId	6

1. Source of Trace. The three traces above were taken from a shared corporate intranet.

2. Detect was generated by: Detected by RealSecure Network Sensor v2.5. No false negatives are known for this signature.

3. Probability the source address was spoofed: Unlikely, the traces appear to be basic web accesses through a firewall

4. Description of attack: This signature detects when a web browser attempts to obtain a file containing a Microsoft ActiveX control. RealSecure does not determine if the control being downloaded is malicious, merely that the browser is downloading code.

References

http://www.secadministrator.com/Articles/Index.cfm?ArticleID=15857

5. Attack mechanism:

ActiveX is a Web technology that can be used maliciously to execute local commands on the computer that is running ActiveX. For example, a remote attacker could use ActiveX to execute a local command to shut down the computer.

Specifically, it would let him take any action on the machine that the user himself was capable of taking, such as creating, changing or deleting data, sending data to or receiving data from a web site, reformatting the hard drive, and so forth. User's with Active Scripting or Scripting of Java applets disabled in their IE security zone will not be affected by this vulnerability.

The Microsoft VM contains functionality to create and use ActiveX controls. By design, only a digitally signed applet should be able to use this functionality. However, a flaw in the Microsoft VM could enable an unsigned applet to use it. If a malicious web site operator could persuade a user to visit his web site, he could utilize this vulnerability in the Microsoft VM to execute any ActiveX control present on the visiting user's machine. This would effectively let him take any action the user could take. If the user were running in a highly-restricted security context, he might be able to do very little. But if the user were running as a local administrator, the malicious user would gain complete control over the machine.

6. Correlations:.There have been other systems accessing Active X sites via the firewalls. The detects below were pared down to just show the source/destination IPs and timestamps.

11/19/2001	3:14:30PM GMT	High	MY.NET.6.51	NET.A.226.113
11/19/2001	3:41:19PM GMT	High	MY.NET.6.51	NET.A.50.151
11/19/2001	3:44:09PM GMT	High	MY.NET.6.51	NET.A.50.151
11/19/2001	4:36:17PM GMT	High	MY.NET.6.51	NET.A.226.192
11/19/2001	4:54:29PM GMT	High	MY.NET.6.51	NET.A.50.141
11/19/2001	4:55:51PM GMT	High	MY.NET.6.51	NET.A.50.141
11/19/2001	4:59:11PM GMT	High	MY.NET.6.51	NET.A.50.141
11/19/2001	6:05:10PM GMT	High	MY.NET.6.51	NET.A.226.184
11/19/2001	6:36:17PM GMT	High	MY.NET.6.51	NET.A.226.229
11/20/2001	4:40:23PM GMT	High	MY.NET.6.52	MY.NET.44.78
11/20/2001	4:44:06PM GMT	High	MY.NET.6.52	MY.NET.8.114
11/20/2001	4:51:34PM GMT	High	MY.NET.6.52	MY.NET.8.114
11/20/2001	4:59:32PM GMT	High	MY.NET.6.51	NET.C.67.105
11/20/2001	5:48:40PM GMT	High	MY.NET.6.51	NET.A.226.157
11/20/2001	5:54:17PM GMT	High	MY.NET.6.51	NET.A.226.192
11/20/2001	8:31:43PM GMT	High	MY.NET.6.52	MY.NET.44.81
11/20/2001	8:32:16PM GMT	High	MY.NET.6.52	MY.NET.44.81
11/20/2001	8:32:39PM GMT	High	MY.NET.6.52	MY.NET.44.81
11/20/2001	8:33:11PM GMT	High	MY.NET.6.52	MY.NET.44.81

11/20/2001	8:33:42PM GMT	High	MY.NET.6.52	MY.NET.44.81
11/20/2001	8:34:16PM GMT	High	MY.NET.6.52	MY.NET.44.81
11/20/2001	8:34:20PM GMT	High	MY.NET.6.52	MY.NET.44.81
11/20/2001	8:34:20PM GMT	High	MY.NET.6.52	MY.NET.44.81
11/20/2001	8:34:50PM GMT	High	MY.NET.6.52	MY.NET.44.81
11/20/2001	8:35:01PM GMT	High	MY.NET.6.52	MY.NET.44.81
11/20/2001	8:35:02PM GMT	High	MY.NET.6.52	MY.NET.44.81
11/20/2001	8:35:07PM GMT	High	MY.NET.6.52	MY.NET.44.81
11/20/2001	8:35:23PM GMT	High	MY.NET.6.52	MY.NET.44.81
11/20/2001	8:35:26PM GMT	High	MY.NET.6.52	MY.NET.44.81
11/20/2001	8:41:47PM GMT	High	NET.B.73.71	MY.NET.65.105
11/21/2001	1:02:22PM GMT	High	MY.NET.6.51	NET.C.67.103
11/21/2001	1:10:12PM GMT	High	MY.NET.6.51	NET.C.67.103

7. Evidence of active targeting: None. The traces appear to be normal HTTP traffic. All other parameters are normal, again just the fact that Active X was detected was the trigger.

8. Severity: [Target Criticality + Attack Lethality] – [System Countermeasures + Network Countermeasures] = Attack Severity

The destination systems are all load-balanced firewalls, though the attack is potentially lethal for windows systems. The firewalls are fully patched and the sensor are in place to detect suspicious activity, so the countermeasure scores were high.

(Criticality 3 + Lethality 4) – (Sys Countermeasures 4 + Network Countermeasures 4) = -1 (very low Severity)

9. Defensive recommendation: No recommendations for the current network. The firewalls were configured per corporate policy to strip off any ActiveX content. There is one system that will be looked at further. The trace NET.B.73.71 MY.NET.65.105 indicates that there may be a rogue internal web site supporting ActiveX. While that is allowed within the internal enclave, the server was not previously registered or listed in DNS. This will be corrected.

For those Windows systems that are affected by this vulnerability: Microsoft has released a security advisory, MS00-075 and multiple patches are available depending on the build number.

2000-series Microsoft VM customers will be provided with an update soon.
3100-series Microsoft VM customers upgrade to build 3318 or later from: http://www.microsoft.com/java/vm/dl_vm40.htm
3200-series Microsoft VM customers upgrade to build 3318 or later from: http://www.microsoft.com/java/vm/dl_vm40.htm

3300-series Microsoft VM customers upgrade to build 3318 or later from: http://www.microsoft.com/java/vm/dl_vm40.htm

10. Multiple choice test question:
Which of the following is the primary vulnerability from malicious ActiveX code?

A. No modern firewalls can block Active X code
B. ActiveX code is executed by the virtual machine as a trusted process
C. Intrusion Detection systems cannot detect malicious Active X code
D. An unsigned Java applet cannot execute Active X code

Answer: B. The major misconception is that Active X is constrained to operate within the Java security model. It is not. Modern firewalls can block Active X, Java, Java Script. IDS systems can detect embedded Active X – as indicated in the associated trace above. Signed or unsigned Java can execute Active X depending on the local settings.

Detect #4 NMAP ACK Scan of a DNS Server

```
#(1 - 247069) [2001-10-15 17:02:12] [arachNIDS/28]  SCAN nmap TCP
IPv4: 64.55.99.130 -> MY.NET.2.80
      hlen=5 TOS=0 dlen=40 ID=2030 flags=0 offset=0 TTL=49 chksum=14083
TCP:  port=80 -> dport: 53  flags=***A**** seq=303
      ack=0 off=5 res=0 win=1024 urp=0 chksum=24385
Payload: none
-------------------------------------------------------------------------------
```

1. Source of Trace.
This trace was a SNORT detect, stored in ACID - Analysis Console for Intrusion Databases

2. Detect was generated by: Snort. Snort is an open source (http://www.snort.org/) packet sniffer and/or network intrusion detection system developed by Marty Roesch, with international assistance
.
The rule that was fired was from the SCAN group:

> alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN nmap TCP";flags:A;ack:0; reference:arachnids,28;)

The rule detects older versions of NMAP since the ACK was automatically set to zero.

3. Probability the source address was spoofed:
Unlikely as the scanner needs the information directly back for further action depending on the result of the scan. The registry under ARIN appears to be an Internet Service Provider.

HarvardNet, Inc. (NETBLK-HTW-2CIDR) HTW-2CIDR 64.55.0.0 - 64.55.255.255
THE DELPHI GROUP (NETBLK-HTW-06885) HTW-06885 64.55.99.128 - 64.55.99.255

4. Description of attack: The ACK scan was designed to get through a router that is only allowing established connections through.. Therefore, while an externally generated SYN would not pass, a packet with the ACK flag set would. The NMAP scanner would receive a RESET if the response by the system being scanned were not blocked since no previous connection had been established.

The ACK scan is not effective against stateful packet filters, since they would only allow inbound ACKs when a previous outgoing SYN exists.

In this case, a NMAP TCP ping was sent to determine if a host is reachable. The target system is a DNS server. The packet is going to port 53, presumably looking for DNS services. There is no payload with the ping.

CVE number: CAN-1999-0523 Classified as an information gathering attempt

5. Attack mechanism:
NMAP is a very useful scanning tool. It can be use to run a variety of scans, including: SYN scans, ACK scans, FIN scans, SYN scan with IP fragments, UDP scan, FTP Proxy (bounce attack) scan, RPC scan and TCP prediction tests. It was written by Fyodor and is available at http://www.insecure.org/nmap

The ACK scan relies on the fundamental process of the three-way handshake and uses the victims response in some instances to help fingerprint the system. This method of scanning is useful against non-stateful packet filtering routers/firewalls since the ACK is allowed in where SYN scans originated from the outside might be filtered.

6. Correlations:
This IP appears to only be engaged in scanning. No other alerts have been generated from this source. Long term trending analysis will be needed to see if this source comes back again.

7. Evidence of active targeting:
Looking over a several month history that has some holes in it (see summary alerts below), there seem to be two to three scans per month from this same server. This might be part of a routine reconnaissance where our systems are part of a larger list, perhaps to mask the intended target.

```
#1-126282| [2001-08-06 15:57:15] 64.55.99.130:80 -> MY.NET.2.80:53
[arachNIDS/28]  SCAN nmap TCP
#1-131062| [2001-08-20 19:31:39] 64.55.99.130:80 -> MY.NET.2.80:53
[arachNIDS/28]  SCAN nmap TCP
#1-160902| [2001-08-29 20:53:44] 64.55.99.130:80 -> MY.NET.2.80:53
[arachNIDS/28]  SCAN nmap TCP
#2-1466| [2001-07-25 18:05:01] 64.55.99.130:80 -> MY.NET.2.80:53
[arachNIDS/28]  SCAN nmap TCP
#2-1483| [2001-07-25 20:09:19] 64.55.99.130:80 -> MY.NET.2.80:53
[arachNIDS/28]  SCAN nmap TCP
#1-245750| [2001-10-09 20:32:40] 64.55.99.130:80 -> MY.NET.2.80:53
[arachNIDS/28]  SCAN nmap TCP
#1-246687| [2001-10-13 13:34:32] 64.55.99.130:80 -> MY.NET.2.80:53
[arachNIDS/28]  SCAN nmap TCP
#1-247069| [2001-10-15 17:02:12] 64.55.99.130:80 -> MY.NET.2.80:53
[arachNIDS/28]  SCAN nmap TCP
```

8. Severity: [Target Criticality + Attack Lethality] – [System Countermeasures + Network Countermeasures] = Attack Severity

[3 + 1] – [4 + 2] = -2 (low severity) The DNS server provides a secondary lookup for external queries from the Internet. There is a secondary DNS as well as the services provided by the ISP. System countermeasures are high as the system is patched and the latest BIND version is in place.

9. Defensive recommendation:
There is not a direct threat from the scanning itself, as all unnecessary services/ports are disabled and the latest patches have been applied. Due to the persistent nature of this IP, I would place it

on a watch list with others in the “low and slow” or “regular customer” category. As mentioned before, a stateful packet filter or proxy firewall would help to defend some of the scans.

10. Multiple choice test question:
Which of the following would be considered a stealthy scan technique?
a. TCP SYN/ACK packets
b. Host Scanning
c. ICMP echo requests
d. UDP Echo requests

ANSWER = A TCP SYN/ACK, or TCP half open, scan uses the expected response from a system to send a RESET when it receives a packet that it never originated the communication. The other scanning methods listed are not necessarily stealthy, though the capability of an IDS to detect the scan will depend on the sensitivity of the ruleset used and the frequency of the transmitted packets.

Detect #5 Fast SYN/FIN Scan of Subnet

```
Generated by ACID v0.9.6b15 on Thu October 18, 2001 18:58:53

---------------------------------------------------------------------------
#(1 - 128910) [2001-08-15 03:40:52]  spp_stream4: STEALTH ACTIVITY (SYN FIN
scan) detection
IPv4: 66.30.139.181 -> MY.NET.2.40
      hlen=5 TOS=0 dlen=40 ID=39426 flags=0 offset=0 TTL=27 chksum=37116
TCP:  port=21 -> dport: 21  flags=******SF seq=1365100822
      ack=912682120 off=5 res=0 win=1028 urp=0 chksum=31103
Payload: none
---------------------------------------------------------------------------
#(1 - 128911) [2001-08-15 03:40:52]  spp_stream4: STEALTH ACTIVITY (SYN FIN
scan) detection
IPv4: 66.30.139.181 -> MY.NET.2.41
      hlen=5 TOS=0 dlen=40 ID=39426 flags=0 offset=0 TTL=27 chksum=37115
TCP:  port=21 -> dport: 21  flags=******SF seq=1365100822
      ack=912682120 off=5 res=0 win=1028 urp=0 chksum=31102
Payload: none
---------------------------------------------------------------------------
#(1 - 128912) [2001-08-15 03:40:52]  spp_stream4: STEALTH ACTIVITY (SYN FIN
scan) detection
IPv4: 66.30.139.181 -> MY.NET.2.42
      hlen=5 TOS=0 dlen=40 ID=39426 flags=0 offset=0 TTL=27 chksum=37114
TCP:  port=21 -> dport: 21  flags=******SF seq=1365100822
      ack=912682120 off=5 res=0 win=1028 urp=0 chksum=31101
Payload: none
```

1. Source of Trace.
This trace was a SNORT detect, stored in ACID - Analysis Console for Intrusion Databases

2. Detect was generated by: Snort
Three sequential alerts were shown in full above.

3. Probability the source address was spoofed:
Unlikely. The source of the scan needs the information back if it is to be used for any attacks.

This source belongs to:
ROADRUNNER-NORTHEAST (NETBLK-ROADRUNNER-NORTHEAST)
13241 Woodland Park Road
Herndon, VA 20171
US
Netname: ROADRUNNER-NORTHEAST
Netblock: 66.30.0.0 - 66.30.255.255
Maintainer: RRNE

4. Description of attack:

A very fast SYN/FIN scan was run against the corporate MY.NET.2 subnet. The alert summaries provided in the correlation section below show that IP subnet range from MY.NET.2.40 to MY.NET.2.147 were hit all within a minute. Twenty four alerts occurred over a three second time span. It is likely that my IDS did not catch all the packets. These appear to be crafted packets with identical Sequence Numbers for each packet as it walks through the subnet sequentially. If nmap were used, a timing flat (-T) of "insane" could have produced this fast a scan. The scan was also fixed for source and destination port 21 which would be a possible attempt to get around a firewall using an open FTP control connection port. However, that technique usually has a high source port assigned.

5. Attack mechanism:
The SYN/FIN scan attempts to trigger a response from the victim using the three-way handshake. In normal TCP communication a system originates a connection with a SYN. The destination (if listening on that port) responds with a SYN/ACK. The source responds with an ACK and the connection is established. Prior to the last ACK, most systems do not log the intermediate exchange. That is where the exploits begin with stealthy scans. A SYN/FIN packet should never naturally exist. However, if it is received, most likely the destination system will respond with a RESET. This tips the scanner off to the existence of the server and the listening service.

6. Correlations:

The alerts below were the only ones from the source IP from the log files for several months worth of intercepts.

```
#1-128910| [2001-08-15 03:40:52] 66.30.139.181:21 -> MY.NET.2.40:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128911| [2001-08-15 03:40:52] 66.30.139.181:21 -> MY.NET.2.41:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128912| [2001-08-15 03:40:52] 66.30.139.181:21 -> MY.NET.2.42:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128913| [2001-08-15 03:40:52] 66.30.139.181:21 -> MY.NET.2.44:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128914| [2001-08-15 03:40:52] 66.30.139.181:21 -> MY.NET.2.50:21
```

```
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128915| [2001-08-15 03:40:52] 66.30.139.181:21 -> MY.NET.2.51:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128916| [2001-08-15 03:40:52] 66.30.139.181:21 -> MY.NET.2.52:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128917| [2001-08-15 03:40:52] 66.30.139.181:21 -> MY.NET.2.55:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128919| [2001-08-15 03:40:52] 66.30.139.181:21 -> MY.NET.2.59:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128920| [2001-08-15 03:40:52] 66.30.139.181:21 -> MY.NET.2.62:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128921| [2001-08-15 03:40:52] 66.30.139.181:21 -> MY.NET.2.63:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128922| [2001-08-15 03:40:52] 66.30.139.181:21 -> MY.NET.2.64:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128923| [2001-08-15 03:40:52] 66.30.139.181:21 -> MY.NET.2.65:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128924| [2001-08-15 03:40:52] 66.30.139.181:21 -> MY.NET.2.66:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128925| [2001-08-15 03:40:52] 66.30.139.181:21 -> MY.NET.2.68:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128926| [2001-08-15 03:40:52] 66.30.139.181:21 -> MY.NET.2.71:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128927| [2001-08-15 03:40:53] 66.30.139.181:21 -> MY.NET.2.80:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128928| [2001-08-15 03:40:53] 66.30.139.181:21 -> MY.NET.2.82:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128929| [2001-08-15 03:40:53] 66.30.139.181:21 -> MY.NET.2.100:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128930| [2001-08-15 03:40:53] 66.30.139.181:21 -> MY.NET.2.101:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128931| [2001-08-15 03:40:53] 66.30.139.181:21 -> MY.NET.2.102:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128932| [2001-08-15 03:40:53] 66.30.139.181:21 -> MY.NET.2.110:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128933| [2001-08-15 03:40:53] 66.30.139.181:21 -> MY.NET.2.111:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
#1-128934| [2001-08-15 03:40:54] 66.30.139.181:21 -> MY.NET.2.147:21
spp_stream4: STEALTH ACTIVITY (SYN FIN scan) detection
```

GCIA Analyst #0385, Wes Bateman notes that a window size of 1028 is one of the possible signatures of the Psychoid synscanner tool.

7. Evidence of active targeting:
The coincidence of this fast scanning sequence does appear that this subnet is being targeted.

8. Severity: [Target Criticality + Attack Lethality] – [System Countermeasures + Network Countermeasures] = Attack Severity

[3 + 2] – [4 + 3] = -2 (low severity)

The subnet in question provides internet service to the public. While we feel most of these servers are up-to-date with security patches, there is the opportunity of a public defacement, but no loss of sensitive corporate data. The IDS did detect the scan (or at least every fifth one).

9. Defensive recommendation:
This source IP should be placed on a watch list and possibly blocked if additional attention to MY.NET is found. The external router has unnecessary ports (including ICMP) blocked in the access control list, that would help prevent response to PING scans from the outside. Unused ports and IAVA vulnerable ports were also disabled on the external servers.

10. Multiple choice test question:

Which of the following fragment related attacks are not designed to evade IDS detection?
A. Tiny Fragment Attack
B. Ping O' Death Attack
C. Fragment Overlap Attack
D. All of the above

Answer – B Ping O' Death is a fragmentation attack designed for denial of service. Tiny fragments create packets so small that the port number is contained on the second packet. The Fragment Overlap has two packets, the first coming in on an allowed port, the second with an foreshortened offset value. When reassembled, the second fragment overwrites the port number of the first fragment and is passed to the application in the final form that the hacker wants and that the IDS just missed.

ASSIGNMENT 3 – Analyze This

EXECUTIVE SUMMARY

Part III of the Practical calls for an analysis of five consecutive days of intrusion detection alerts generated by the freeware sensor - SNORT. SNORT output was analyzed for The University network system from 1 to 5 September 2001. The files listed in Table A. were downloaded from the University and include alerts, out of spec (OOS) and scans. Out of these data, almost 780,000 alerts occurred. Each day there were between 87 and 113 unique alerts generated.

What follows is the analysis that tries to identify significant events that might include external reconnaissance of our network, attempts to exploit or gain unauthorized access to university systems and possible misuse of university computers.

I had already performed most of the analysis on all of the alerts for these five days after I reviewed the GCIA Practical Study and Planning Guide. The Guide made it clearer than the original Practical Assignment that full analysis of all alerts was not required. I decided to focus my efforts on the Attacks and Admin related alerts but not to remove any previous analysis on recon, web activity and unknowns.

Table A – Log Files Analyzed

SNORT ALERTS	OUT OF SPEC	SCANS
alert.010901.gz	Oos_Sept.1.2001.gz	Scans.010901.gz
alert.010902.gz	Oos_Sept.2.2001.gz	Scans.010902.gz
alert.010903.gz	Oos_Sept.3.2001.gz	Scans.010903.gz
alert.010904.gz	Oos_Sept.4.2001.gz	Scans.010904.gz
alert.010905.gz	Oos_Sept.5.2001.gz	Scans.010905.gz

Table B. lists summary data collected before detailed analysis was made of the individual detects

Table B Alert Totals

Date	Total Alerts	Unique Alerts
Sept 1	197640	95
Sept 2	166511	90
Sept 3	158281	97
Sept 4	128124	113
Sept 5	129392	87
Total alerts:	779948	

DAILY ALERT OVERVIEW

Detects are listed for each day with a description of the top five alerts for each day. Detects are sorted by number of alerts. These are just the daily summary numbers. Detailed description of the unique alerts is provided in the following section.

Alert Summary from September 1, 2001

Day 1 - 197640 Alerts			
Signature	**# Alerts**	**# Sources**	**# Destinations**
WEB-MISC Attempt to execute cmd	79667	16481	24955
IDS552/web-iis_IIS ISAPI Overflow ida nosize[arachNIDS]	70289	15952	24592
ICMP Destination Unreachable	9989	17	182
MISC traceroute	6360	59	5
CS WEBSERVER – external web traffic	5178	796	1
MISC source port 53 to <1024	4339	1373	8
Possible trojan server activity	3861	393	2543
INFO MSN IM Chat data	3320	129	128
INFO napster login	2846	41	156
WEB-MISC prefix-get //	2716	215	3
ICMP Echo Request Nmap or HPING2	1276	18	93
ICMP Destination Unreachable (Host Unreachable)	1103	16	14
ICMP Destination Unreachable (Network Unreachable)	1029	1	297
MISC Large UDP Packet	802	4	4
Watchlist 000220 IL-ISDNNET-990517	610	60	41
ICMP Echo Request Delphi-Piette Windows	407	4	329
INFO Inbound GNUTella Connect accept	380	39	327
Null scan!	362	43	44
INFO Napster Client Data	279	46	211
ICMP traceroute	261	126	159
Incomplete Packet Fragments Discarded	253	4	3
TCP SRC and DST outside network	207	47	114
FTP DoS ftpd globbing	199	9	8
External RPC call	189	2	172
ICMP Echo Request Windows	179	30	22
SCAN Proxy attempt	164	25	27
Watchlist 000222 NET-NCFC	152	13	27
SMB Name Wildcard	125	29	26
ICMP Echo Request Sun Solaris	117	6	31
ICMP Fragment Reassembly Time Exceeded	86	13	13
WEB-MISC http directory traversal	78	12	5
INFO Outbound GNUTella Connect accept	75	73	33
spp_http_decode: IIS Unicode attack detected	54	10	9
ICMP Echo Request CyberKit 2.2 Windows	53	10	4
WEB-MISC 403 Forbidden	46	4	24
Queso fingerprint	44	19	20

WEB-CGI scriptalias access	40	4	3
Port 55850 tcp – Possible myserver activity - ref. 010313-1	39	9	10
INFO Possible IRC Access	35	25	18
CS WEBSERVER – external ftp traffic	24	12	1
INFO FTP anonymous FTP	24	14	5
EXPLOIT x86 NOOP	24	8	8
TELNET login incorrect	21	6	19
MISC Large ICMP Packet	20	15	8
High port 65535 udp -possible Red Worm - traffic	18	9	8
SUNRPC highport access!	17	1	1
ICMP Echo Request L3retriever Ping	17	3	2
High port 65535 tcp - possible Red Worm - traffic	17	9	9
ICMP Destination Unreachable (Protocol Unreachable)	17	1	1
EXPLOIT x86 setuid 0	16	14	14
WEB-FRONTPAGE shtml.dll	16	2	2
WEB-CGI csh access	14	11	3
INFO napster upload request	13	6	4
NMAP TCP ping!	12	8	9
connect to 515 from inside	12	1	1
Tiny Fragments – Possible Hostile Activity	12	7	9
WEB-IIS encoding access	10	2	2
spp_http_decode: CGI Null Byte attack detected	10	2	2
WEB-CGI redirect access	10	9	6
beetle.ucs	9	3	4
INFO napster new user login	7	1	5
WEB-MISC count.cgi access	6	5	2
INFO - Possible Squid Scan	5	4	4
WEB-FRONTPAGE _vti_rpc access	5	4	3
X11 outgoing	5	4	4
ICMP Echo Request BSDtype	4	2	2
SCAN Synscan Portscan ID 19104	4	4	4
WEB-IIS _vti_inf access	4	4	3
WEB-MISC L3retriever HTTP Probe	4	2	2
WEB-CGI rsh access	4	2	1
x86 NOOP - unicode BUFFER OVERFLOW ATTACK	4	3	1
INFO Inbound GNUTella Connect request	3	2	2
WEB-IIS Unauthorized IP Access Attempt	3	3	3
WEB-CGI files.pl access	3	1	1
ICMP SRC and DST outside network	3	2	1
SYN-FIN scan!	3	1	1

SCAN FIN	3	2	2
Virus - Possible pif Worm	3	1	1
RFB - Possible WinVNC - 010708-1	3	3	3
EXPLOIT x86 stealth noop	2	2	1
WEB-CGI upload.pl access	2	1	1
Probable NMAP fingerprint attempt	2	1	1
EXPLOIT x86 setgid 0	2	2	2
WEB-FRONTPAGE fpcount.exe access	2	2	1
ICMP Destination Unreachable (Fragmentation Needed and DF bit was set)	2	2	1
WEB-CGI w3-msql access	1	1	1
WEB-MISC Lotus Domino directory traversal	1	1	1
WEB-IIS view source via translate header	1	1	1
WEB-CGI ksh access	1	1	1
ICMP Address Mask Request (Undefined Code!)	1	1	1
RPC portmap request rstatd	1	1	1
WEB-MISC whisker head	1	1	1
ICMP Source Quench	1	1	1
INFO - Web Cmd completed	1	1	1
SCAN XMAS	1	1	1

Day 1 Top Five Analysis:

Out of the top five alerts by frequency, approximately 40% of the intercepts were from WEB-MISC Attempt to execute cmd. There were 16481 source IPs and 24955 destination Ips.

Thirty five percent of the alerts were from IDS552/web-iis_IIS ISAPI Overflow ida nosize[arachNIDS]. There were 15952 sources and 24592 distinct destination IPs.

There were 9989 ICMP Destination Unreachable alerts that accounted for 5% of the days events. Seventeen distinct sources and 182 destinations were involved.

The MISC traceroute accounted for 3% of the traffic with 59 unique sources and 5 destination addresses.

CS WEBSERVER – external web traffic alert generated a little over 2% of the daily traffic. There were 796 unique sources but only one destination address. Can I guess that 99.99.100.165 is one of my public web servers?

Additional Day 1 Analysis:

Many ICMP unreachable alerts were sent to 99.99.30.2 from a variety of external systems. This may be an indication of some reconnaissance being performed while spoofing one of my IPs

Watchlist 000220 IL-ISDNNET-990517 was a custom rule to monitor traffic from an IP block

registered to European Regional Internet Registry/RIPE NCC. While I am new to the IDS at the University, I assume some of their system have been misbehaving and we are watching them closely.

Several (233 of 362) NULL SCAN! alerts were generated from 63.203.103.68. The same IP was responsible for seven other related scans or access attempts as seen below. The source seems particularly interested in my server 99.99.225.30 that was scanned 234 times.

5 different signatures are present for 63.203.103.68 as a source
1 instances of SCAN FIN
1 instances of SCAN XMAS
2 instances of IDS552/web-iis_IIS ISAPI Overflow ida nosize
3 instances of SYN-FIN scan!
226 instances of Null scan!

Another watch has been placed on the The Computer Network Center Chinese Academy of Sciences (NET-NCFC) IP block which generated 152 scan from 13 different hosts within their managed IP range.

DAY 2

Alert Summary from Sept 2, 2001

Day 2 - 166511 total alerts			
Signature	**# Alerts**	**# Sources**	**# Destinations**
WEB-MISC Attempt to execute cmd	66521	14864	23563
IDS552/web-iis_IIS ISAPI Overflow ida nosize [arachNIDS]	58251	14310	23111
ICMP Destination Unreachable (Communication Administratively Prohibited)	7909	9	186
MISC traceroute	5326	61	8
MISC source port 53 to <1024	3834	1317	11
Tiny Fragments - Possible Hostile Activity	3343	4	7
CS WEBSERVER - external web traffic	3151	791	1
INFO MSN IM Chat data	3123	142	130
WEB-MISC prefix-get //	2348	201	4
ICMP Echo Request Nmap or HPING2	2001	14	130
spp_http_decode: IIS Unicode attack detected	1841	2	208
INFO napster login	1670	36	140
ICMP Destination Unreachable (Network Unreachable)	1525	2	284
ICMP Destination Unreachable (Host Unreachable)	1169	14	15
INFO Napster Client Data	974	56	180
Null scan!	446	36	31

Watchlist 000220 IL-ISDNNET-990517	321	58	48
INFO Inbound GNUTella Connect accept	318	45	282
Watchlist 000222 NET-NCFC	267	19	32
ICMP traceroute	220	124	121
INFO FTP anonymous FTP	198	22	105
FTP DoS ftpd globbing	177	6	6
TCP SRC and DST outside network	173	35	120
Incomplete Packet Fragments Discarded	122	3	3
SCAN Proxy attempt	99	26	24
INFO Outbound GNUTella Connect accept	98	94	32
connect to 515 from outside	90	1	86
SMB Name Wildcard	89	23	24
EXPLOIT x86 NOOP	77	4	4
ICMP Echo Request Sun Solaris	66	5	24
ICMP Echo Request CyberKit 2.2 Windows	64	13	3
ICMP Destination Unreachable (Protocol	64	3	4
MISC Large UDP Packet	54	5	5
ICMP Source Quench	54	3	1
ICMP Echo Request Windows	51	28	17
WEB-MISC 403 Forbidden	43	5	20
INFO Possible IRC Access	40	17	20
MISC Large ICMP Packet	39	12	5
Queso fingerprint	39	16	15
Port 55850 tcp - Possible myserver activity - ref. 010313-1	30	5	5
ICMP Fragment Reassembly Time Exceeded	28	6	6
CS WEBSERVER - external ftp traffic	27	17	1
TELNET login incorrect	22	6	20
WEB-MISC count.cgi access	13	10	1
WEB-FRONTPAGE _vti_rpc access	13	6	4
WEB-MISC http directory traversal	11	8	2
WEB-IIS _vti_inf access	10	8	5
Possible trojan server activity	10	4	4
High port 65535 tcp - possible Red Worm - traffic	9	7	7
connect to 515 from inside	9	1	1
WEB-FRONTPAGE fpcount.exe access	9	6	2
INFO napster upload request	9	2	2
EXPLOIT x86 setuid 0	9	9	9
WEB-FRONTPAGE shtml.dll	8	2	1
NMAP TCP ping!	8	3	3
beetle.ucs	6	3	2
High port 65535 udp - possible Red Worm -	6	4	4
SCAN Synscan Portscan ID 19104	6	6	6
EXPLOIT x86 setgid 0	5	5	5

ICMP Echo Request L3retriever Ping	5	2	2
INFO - Web Cmd completed	5	2	3
WEB-CGI csh access	5	5	2
WEB-MISC whisker head	5	1	1
WEB-MISC L3retriever HTTP Probe	4	1	1
SCAN XMAS	3	2	2
X11 outgoing	3	2	2
INFO Inbound GNUTella Connect request	3	3	2
ICMP Echo Request Delphi-Piette Windows	3	3	2
BACKDOOR NetMetro Incoming Traffic	3	1	1
ICMP Echo Request BSDtype	3	1	1
x86 NOOP - unicode BUFFER OVERFLOW ATTACK	2	1	1
SCAN FIN	2	1	1
SUNRPC highport access!	2	2	1
External FTP to HelpDesk 99.99.53.29	2	2	1
WEB-CGI ksh access	2	2	1
SNMP public access	2	1	2
INFO - Possible Squid Scan	2	2	2
Virus - Possible scr Worm	1	1	1
WEB-MISC Lotus Domino directory traversal	1	1	1
INFO Outbound GNUTella Connect request	1	1	1
WEB-CGI redirect access	1	1	1
WEB-CGI scriptalias access	1	1	1
Russia Dynamo - SANS Flash 28-jul-00	1	1	1
RFB - Possible WinVNC - 010708-1	1	1	1
FTP passwd attempt	1	1	1
WEB-IIS Unauthorized IP Access Attempt	1	1	1
Probable NMAP fingerprint attempt	1	1	1
External FTP to HelpDesk 99.99.70.50	1	1	1
SMTP relaying denied	1	1	1

Day 2 Analysis

Of more than 166 thousand alerts for the day, 40% are from the WEB-MISC Attempt to execute cmd. There were 14864 source addresses and 23563 destination hosts.

Thirty five percent of the days alerts were IDS552/web-iis_IIS ISAPI Overflow ida nosize [arachNIDS], with 14310 source hosts and 23111 destination hosts involved.

The ICMP Destination Unreachable (Communication Administratively Prohibited) rule generated 4.7% of the alerts from 9 sources and 186 destinations.

The MISC traceroute was responsible for a little over three percent of the alerts from 61 sources

and 8 destinations.

Finally, 2% of the alerts were from MISC source port 53 to <1024 with 1317 sources and 11 destination systems.

DAY 3

Summary of Alerts from September 3, 2001

Day 3 – 158281 total alerts			
Signature	**Alerts**	**Sources**	**Destinations**
WEB-MISC Attempt to execute cmd	65911	15191	24063
IDS552/web-iis_IIS ISAPI Overflowida nosize [arachNIDS]	57955	14485	23705
ICMP Destination Unreachable(Communication Administratively Prohibited)	6198	8	203
MISC traceroute	4079	61	8
MISC Large UDP Packet	3571	15	7
MISC source port 53 to <1024	3501	1385	8
CS WEBSERVER - external webtraffic	2930	975	1
WEB-MISC prefix-get //	2643	231	1
INFO MSN IM Chat data	2584	147	144
INFO napster login	2054	36	145
ICMP Echo Request Nmap or HPING2	1378	41	131
ICMP Destination Unreachable(Network Unreachable)	876	1	290
ICMP Destination Unreachable (HostUnreachable)	597	32	7
Watchlist 000220 IL-ISDNNET-990517	399	30	37
INFO Inbound GNUTella Connectaccept	393	51	366
TCP SRC and DST outside network	370	64	129
SCAN Proxy attempt	338	29	28
ICMP traceroute	329	189	193
ICMP Echo Request Sun Solaris	237	8	53
Null scan!	235	37	40
INFO Napster Client Data	234	61	200
External RPC call	138	2	130
ICMP Fragment Reassembly TimeExceeded	123	14	20
INFO Outbound GNUTella Connectaccept	110	106	41
Watchlist 000222 NET-NCFC	97	25	46
FTP DoS ftpd globbing	78	3	3
SMTP relaying denied	71	3	3
INFO Possible IRC Access	63	35	26
SMB Name Wildcard	54	24	23
ICMP Echo Request CyberKit 2.2Windows	51	9	6
Queso fingerprint	48	13	16
INFO FTP anonymous FTP	46	25	12

ICMP Echo Request Windows	46	25	15
ICMP Echo Request L3retriever Ping	44	4	5
WEB-MISC 403 Forbidden	37	6	30
ICMP Source Quench	37	1	1
MISC Large ICMP Packet	34	18	7
EXPLOIT x86 NOOP	28	15	15
TELNET login incorrect	27	6	23
spp_http_decode: IIS Unicodeattack detected	26	7	8
CS WEBSERVER - external ftptraffic	25	12	1
WEB-MISC http directory traversal	21	10	2
Possible trojan server activity	19	1	1
beetle.ucs	17	3	5
Tiny Fragments - Possible HostileActivity	14	9	13
EXPLOIT x86 setuid 0	14	13	12
WEB-MISC count.cgi access	14	13	3
High port 65535 tcp - possible RedWorm - traffic	14	8	8
ICMP Echo Request BSDtype	11	3	3
ICMP Echo Request Broadscan SmurfScanner	11	1	11
INFO Outbound GNUTella Connectrequest	10	4	2
EXPLOIT x86 NOPS	9	1	1
Port 55850 tcp - Possible myserveractivity - ref. 010313-1	8	3	3
ICMP Destination Unreachable(Protocol Unreachable)	8	5	5
ICMP Echo Request Delphi-PietteWindows	6	3	6
NMAP TCP ping!	6	4	5
WEB-IIS _vti_inf access	6	6	4
connect to 515 from inside	6	1	1
INFO napster upload request	6	4	2
MISC Source Port 20 to <1024	5	1	1
WEB-FRONTPAGE fpcount.exe access	5	4	2
WEB-CGI csh access	5	5	1
WEB-FRONTPAGE _vti_rpc access	5	5	2
EXPLOIT x86 setgid 0	5	5	5
SCAN FIN	5	3	2
Probable NMAP fingerprint attempt	4	2	2
x86 NOOP - unicode BUFFER OVERFLOWATTACK	4	2	2
X11 outgoing	4	3	3
INFO Inbound GNUTella Connectrequest	3	2	3
MISC PCAnywhere Startup	3	1	1
INFO - Possible Squid Scan	3	2	3
WEB-CGI redirect access	2	2	2
WEB-MISC L3retriever HTTP Probe	2	1	1
INFO - Web Cmd completed	2	1	2
WEB-CGI scriptalias access	2	2	2

WEB-CGI finger access	2	2	1
WEB-CGI rsh access	2	2	1
SUNRPC highport access!	2	2	2
TELNET SGI telnetd format bug	2	1	1
WEB-CGI calendar access	1	1	1
WEB-MISC whisker head	1	1	1
ICMP Reserved for Security (Type19) (Undefined Code!)	1	1	1
WEB-MISC Invalid URL	1	1	1
High port 65535 udp - possible RedWorm - traffic	1	1	1
SCAN XMAS	1	1	1
WEB-IIS Unauthorized IP AccessAttempt	1	1	1
BACKDOOR NetMetro File List	1	1	1
SCAN Synscan Portscan ID 19104	1	1	1
IDS475/web-iis_web-webdav-propfind[arachNIDS]	1	1	1
EXPLOIT x86 stealth noop	1	1	1
WEB-MISC Lotus Domino directorytraversal	1	1	1
DNS zone transfer	1	1	1
WEB-FRONTPAGE shtml.dll	1	1	1
WEB-CGI archie access	1	1	1
WEB-CGI tsch access	1	1	1
ICMP Destination Unreachable(Fragmentation Needed and DF bit was set)	1	3	3

DAY 3 Analysis

On day three, 42% of the alerts were fromWEB-MISC Attempt to execute cmd with 15191 different sources and 24063 different destinations.

The IDS552/web-iis_IIS ISAPI Overflowida nosize [arachNIDS] alert came in second with 37% of the alerts from 14485 sources going and 23705 destinations.

Only 4% of the alert traffic was triggered by the ICMP Destination Unreachable(Communication Administratively Prohibited). This set of alerts originated from 8 source hosts and 203 destination hosts.

Less than 3% of the traffic on Day 3 came from MISC traceroutes from 61 sources and 8 destination IPs.

And rounding out the top five for the day, approximately 2% of the alerts were from MISC Large UDP Packet from 15 sources and 7 destination hosts.

DAY 4

Summary of Alerts from September 4, 2001

Day 4 – 128124 total alerts			
Signature	**Alerts**	**Sources**	**Destinations**
WEB-MISC Attempt to execute cmd	49350	13827	22283
IDS552/web-iis_IIS ISAPI Overflow ida nosize[arachNIDS]	42941	12912	21340
ICMP Destination Unreachable (Communication Administratively Prohibited)	4313	14	214
High port 65535 tcp - possible Red Worm traffic -	4256	650	3610
MISC source port 53 to <1024	3339	1447	12
ICMP Echo Request Nmap or HPING2	3107	44	143
INFO MSN IM Chat data	2922	244	231
MISC traceroute	2499	62	10
WEB-MISC prefix-get //	2490	317	2
CS WEBSERVER – external web traffic	2410	956	1
MISC Large UDP Packet	1991	13	9
Watchlist 000220 IL-ISDNNET-990517	1110	42	38
INFO napster login	1079	43	133
ICMP Echo Request Windows	970	25	15
ICMP Destination Unreachable (Network Unreachable)	720	2	239
INFO Possible IRC Access	530	28	26
Port 55850 tcp – Possible myserver activity - ref. 010313-1	433	14	15
ICMP Destination Unreachable (Host Unreachable)	408	50	9
TCP SRC and DST outside network	337	87	207
INFO Inbound GNUTella Connect accept	335	60	309
SUNRPC highport access!	324	2	2
ICMP traceroute	239	169	137
Watchlist 000222 NET-NCFC	183	18	33
RPC tcp traffic contains bin_sh	163	2	2
INFO Napster Client Data	134	54	102
ICMP Echo Request L3retriever Ping	117	3	5
INFO Outbound GNUTella Connect accept	116	114	39
SMTP relaying denied	106	3	4
ICMP Echo Request Sun Solaris	101	3	33
Queso fingerprint	93	13	15
INFO FTP anonymous FTP	86	14	46
SCAN Proxy attempt	75	34	22
External RPC call	71	1	71
Null scan!	60	29	32
FTP DoS ftpd globbing	59	7	8
EXPLOIT x86 NOOP	57	12	11
connect to 515 from outside	54	1	54

ICMP Echo Request CyberKit 2.2 Windows	47	14	7
WEB-MISC 403 Forbidden	39	5	29
ICMP Fragment Reassembly Time Exceeded	39	15	16
Incomplete Packet Fragments Discarded	38	2	2
MISC Large ICMP Packet	28	8	7
CS WEBSERVER – external ftp traffic	27	6	1
SMB Name Wildcard	25	21	22
TELNET login incorrect	23	7	22
WEB-MISC http directory traversal	23	14	2
Possible trojan server activity	19	6	6
EXPLOIT x86 stealth noop	16	2	2
WEB-MISC count.cgi access	16	7	3
x86 NOOP - unicode BUFFER OVERFLOW ATTACK	14	5	5
WEB-FRONTPAGE fpcount.exe access	11	6	1
WEB-FRONTPAGE fourdots request	11	1	1
beetle.ucs	9	4	7
Tiny Fragments – Possible Hostile Activity	9	6	8
ICMP Destination Unreachable (Fragmentation Needed and DF bit was set)	8	7	1
spp_http_decode: IIS Unicode attack detected	8	3	2
ICMP Source Quench	8	5	3
EXPLOIT x86 NOPS	7	1	1
FTP CWD / - possible warez site	7	1	7
ICMP Echo Request BSDtype	7	6	6
SCAN Synscan Portscan ID 19104	7	7	6
WEB-MISC Lotus Domino directory traversal	6	2	3
ICMP SRC and DST outside network	6	4	4
EXPLOIT x86 setuid 0	6	6	6
X11 outgoing	5	4	4
EXPLOIT x86 setgid 0	5	5	5
High port 65535 udp - possible Red Worm traffic -	5	4	4
WEB-MISC L3retriever HTTP Probe	4	1	1
INFO - Web Cmd completed	4	1	3
SCAN FIN	4	2	2
Port 55850 udp – Possible myserver activity - ref. 010313-1	3	1	1
INFO Outbound GNUTella Connect request	3	3	3
WEB-CGI redirect access	3	3	2
WEB-IIS _vti_inf access	3	3	3
EXPLOIT NTPDX buffer overflow	3	2	2
connect to 515 from inside	3	1	1
WEB-CGI rsh access	2	2	1
WEB-IIS view source via translate header	2	1	1

WEB-CGI upload.pl access	2	1	1
Russia Dynamo – SANS Flash 28-jul-00	2	2	2
BACKDOOR NetMetro Incoming Traffic	2	1	1
WEB-IIS Unauthorized IP Access Attempt	2	1	2
WEB-FRONTPAGE _vti_rpc access	2	2	2
Virus - Possible scr Worm	2	2	2
INFO napster upload request	2	2	2
WEB-MISC whisker head	2	2	2
WEB-CGI archie access	2	2	2
WEB-CGI w3-msql access	1	1	1
INFO Inbound GNUTella Connect request	1	1	1
INFO - Possible Squid Scan	1	1	1
Virus - Possible pif Worm	1	1	1
DDOS mstream handler to client	1	1	1
Attempted Sun RPC high port access	1	1	1
Virus - Possible MyRomeo Worm	1	1	1
WEB-CGI webgais access	1	1	1
DNS SPOOF query response with ttl	1	1	1
NMAP TCP ping!	1	1	1
WEB-CGI glimpse access	1	1	1
ICMP Destination Unreachable (Protocol Unreachable)	1	1	1
SMTP chameleon overflow	1	1	1
TELNET access	1	1	1
RFB – Possible WinVNC -010708-1	1	1	1

Day 4 Analysis

On Day 4, the top three alerts were again WEB-MISC Attempt to execute cmd (39%), IDS552/web-iis_IIS ISAPI Overflow ida nosize[arachNIDS] (33%) and ICMP Destination Unreachable (Communication Administratively Prohibited) (3%).

The very troubling trend for the day is the over four thousand High port 65535 tcp - possible Red Worm traffic alerts. These alerts record 650 sources and 3610 destinations. The source/destination IP for almost all of this traffic is 130.11.37.101 (see SOURCE ANALYSIS/REGISTRATION section for detailed listing). Potentially there are 646 university computers that should be examined for potential infection (MY.NET source IPs). Below is an extract from the alert file showing outbound communications.

09/04-06:00:44.854091 [**] High port 65535 tcp - possible Red Worm - traffic [**] 99.99.1.1:3128 -> 130.161.37.101:65535
09/04-06:00:44.974220 [**] High port 65535 tcp - possible Red Worm - traffic [**] 99.99.1.13:3128 -> 130.161.37.101:65535

There are also four alerts for UDP related Red Worm traffic. Four systems should be looked at as

they were the focus of this traffic: 99.99.153.149; 99.99.228.150; 99.99.181.76; 99.99.225.26.

MISC source port 53 to <1024 accounted for just slightly less than 3% of the daily alerts. There were 1447 source hosts and 12 destination hosts.

DAY 5

Summary of Alerts from September 5, 2001

Day 5 – 129392 total alerts			
Signature	**Alerts**	**Sources**	**Destinations**
WEB-MISC Attempt to execute cmd	44019	13003	20925
IDS552/web-iis_IIS ISAPI Overflow ida nosize [arachNIDS]	38676	12117	20146
MISC Large UDP Packet	14260	29	21
MISC source port 53 to <1024	4577	1364	11
ICMP Destination Unreachable (Communication Administratively Prohibited)	3902	16	213
ICMP Echo Request Nmap or HPING2	3043	44	69
INFO MSN IM Chat data	2904	248	225
Watchlist 000220 IL-ISDNNET-990517	2875	45	34
MISC traceroute	2189	66	11
Possible trojan server activity	2188	5	5
WEB-MISC prefix-get //	2061	295	3
CS WEBSERVER - external web traffic	1789	857	1
INFO napster login	954	43	134
Null scan!	867	19	20
Watchlist 000222 NET-NCFC	847	26	39
ICMP Destination Unreachable (Network Unreachable	556	3	246
INFO Possible IRC Access	546	30	30
INFO Inbound GNUTella Connect accept	356	63	329
ICMP Destination Unreachable (Host Unreachable)	321	5	7
ICMP Fragment Reassembly Time Exceeded	285	17	20
Incomplete Packet Fragments Discarded	284	5	5
ICMP traceroute	247	158	141
TCP SRC and DST outside network	234	74	154
INFO Napster Client Data	191	51	117
ICMP Echo Request CyberKit 2.2 Windows	155	22	10
FTP DoS ftpd globbing	149	20	14
ICMP Echo Request Windows	146	29	22
INFO Outbound GNUTella Connect accept	121	118	44

ICMP Echo Request L3retriever Ping	78	7	9
ICMP Echo Request Sun Solaris	77	5	37
SCAN Proxy attempt	65	21	19
WEB-MISC 403 Forbidden	50	5	32
Queso fingerprint	27	13	15
High port 65535 tcp - possible Red Worm - traffic	23	7	7
TELNET login incorrect	23	7	21
INFO FTP anonymous FTP	22	8	17
WEB-MISC http directory traversal	22	14	2
spp_http_decode: IIS Unicode attack detected	18	2	9
SMB Name Wildcard	17	16	16
ICMP Echo Request BSDtype	16	6	6
EXPLOIT x86 setuid 0	16	16	16
Port 55850 tcp - Possible myserver activity - ref. 010313-1	16	8	8
EXPLOIT x86 NOOP	14	7	7
beetle.ucs	12	5	4
WEB-FRONTPAGE _vti_rpc access	12	9	6
External RPC call	12	1	12
WEB-FRONTPAGE fpcount.exe access	11	6	1
WEB-MISC count.cgi access	10	7	2
CS WEBSERVER - external ftp traffic	10	5	1
SUNRPC highport access!	8	1	1
MISC Large ICMP Packet	8	6	2
WEB-IIS _vti_inf access	7	5	3
INFO Outbound GNUTella Connect request	5	4	2
EXPLOIT x86 setgid 0	5	5	5
WEB-FRONTPAGE fourdots request	5	1	1
INFO - Web Cmd completed	5	1	2
SCAN FIN	4	1	1
ICMP Destination Unreachable (Protocol Unreachable)	4	2	2
NMAP TCP ping!	3	3	3
SCAN Synscan Portscan ID 19104	3	3	3
SMTP relaying denied	3	2	2
INFO napster upload request	3	2	2
SYN-FIN scan!	3	1	1
WEB-FRONTPAGE author.exe access	2	1	1
WEB-CGI csh access	2	2	1
x86 NOOP - unicode BUFFER OVERFLOW ATTACK	2	2	2
X11 outgoing	2	2	2
ICMP SRC and DST outside network	2	1	1

WEB-MISC L3retriever HTTP Probe	2	1	1
High port 65535 udp - possible Red Worm traffic -	2	1	1
Probable NMAP fingerprint attempt	2	2	2
Tiny Fragments - Possible Hostile Activity	2	2	2
spp_http_decode: CGI Null Byte attack detected	2	1	1
FTP MKD . - possible warez site	1	1	1
WEB-CGI calendar access	1	1	1
INFO Inbound GNUTella Connect request	1	1	1
ICMP Source Quench	1	1	1
INFO - Possible Squid Scan	1	1	1
WEB-CGI redirect access	1	1	1
WEB-CGI files.pl access	1	1	1
ICMP Echo Request Delphi-Piette Windows	1	1	1
connect to 515 from inside	1	1	1
WEB-IIS Unauthorized IP Access Attempt	1	1	1
External FTP to HelpDesk 99.99.83.197	1	1	1
WEB-IIS view source via translate header	1	1	1
Virus - Possible MyRomeo Worm	1	1	1

Day 5 Analysis

The last day of analysis yields the usual top five suspects. WEB-MISC Attempt toexecute cmd accounts for 34% of the traffic. These alerts involved 13003 source and 20925 detinations.

IDS552/web-iis_IIS ISAPIOverflow ida nosize[arachNIDS] accounted for 30% of the alerts with over 12,000 source hosts and 20,000 destination host..

MISC Large UDP Packet provided 11% of the alerts for the day. These alerts arrived from 29 sources and involved 21 unique destinations.

MISC source port 53 to<1024 created 3.5% of the alerts from 1364 sources but only 11 destination hosts.

ICMP DestinationUnreachable (CommunicationAdministratively Prohibited) was back in the number five spot with 3% of the traffic. These alerts list 16 different sources and 213 unique destinations.

DETAILED ALERT REVIEW SORTED BY SEVERITY

The following table is a comprehensive list of the unique alerts for all five days. Files were analyzed on a daily basis since my limited disk space and CPU could not support full concatenation of all five days of data.

Threat Types were assigned using class types from Snort rules. Descriptions are provided and recommendations are focused on the potentially damaging Attacks and Admin related alerts. Some alerts cannot be described very fully since we do not have the SNORT rules that were used for the detects. As stated earlier, an initial attempt was made to review all alerts until reading the GIAC Practical Guide. As a result, there are a number of reconnaissance and 'bad unknown' alert descriptions that I kept.

ALERT	THREAT TYPE	DESCRIPTION/RECOMMENDATION

Attempted Sun RPC high port access	Admin	SUN RPC has many vulnerabilities as seen in the CVE list. Often the Sun RPC dispatch server will open a high port 32771 to listen for requests for RPC information. This can be used as a back door to access RPC despite the front door (port 111) being blocked. CVE Entries for RPC attacks. rpc.statd and others are in SANS top 10 vulnerabilities. A couple sources have been involved here and running scans and fingerprints as well. I would be interested in seeing traces involving MY.NET.179.79, MY.NET.163.17, MY.NET.218.218, MY.NET.60.11 and MY.NET.179.78. These systems don't seem to be responding as source with any alerts. Although MY.NET 104.106 and 233.202 were sources for ICMP Echo request back to 209.22.74.47 show was one of the sources for the SUNRPC alert. ACTION: Disable RPC on all systems unless absolutely necessary. Block this port at the external router. CVE-1999-0008 Buffer overflow in NIS+, in Sun's rpc.nisd program CVE-1999-0212 Solaris rpc.mountd generates error messages that allow a remote attacker to determine what files are on the server. CVE-1999-0320 SunOS rpc.cmsd allows attackers to obtain root access by overwriting arbitrary files. CVE-1999-0493 rpc.statd allows remote attackers to forward RPC calls to the local operating system via the SM_MON and SM_NOTIFY commands, which in turn could be used to remotely exploit other bugs such as in automountd. CVE-1999-0687 The ToolTalk ttsession daemon uses weak RPC authentication, which allows a remote attacker to execute commands. CVE-1999-0696 Buffer overflow in CDE Calendar Manager Service Daemon (rpc.cmsd)

BACKDOOR NetMetro File List *File List"; flags: A+; content:"|2D 2D|"; reference:arachnids,79; sid:159* BACKDOOR NetMetro Incoming Traffic *flags: A+; reference:arachnids,79; sid:160*	Admin	Possible trojan backdoor. MY.NET.218.210 was a source for this. Check logs for tampering on destination systems.
EXPLOIT NTPDX buffer overflow	Admin	Network Time Protocol daemon on some systems has a potential exploit http://net-services.ufl.edu/~www/net/mhonarc/net-managers/archive.d20010501/msg00002.html and is of a concern since NTP may be running with root permissions. 64.124.69.60 is the source of both an attempted buffer attack and possible Red Worm activity focused on 99.99.181.76 151.200.176.24 ran a similar attack on 99.99.178.115. No responses were detected from either of my systems.

EXPLOIT x86 NOOP EXPLOIT x86 setuid 0 EXPLOIT x86 stealth noop x86 NOOP - unicode BUFFER OVERFLOWATTACK	Admin	NOOP codes (0x90 for Intel CPUs) are frequently used as padding to overflow a buffer and subsequently insert malicious code for execution. 99.99.234.50 has had the attention of several system with a Queso fingerprint and Null scan and a NOOP and stealth attacks. The sources are not the same, though they could have been spoofed. 99.99.130.86 has been the focus of 64.224.109.6 with Squid scans, a setuid 0 and ten NOOP exploits. This system should be checked for any abnormalities or changes to the baseline configuration. These exploits go for a several days. 64.224.109.6 is also working the buffer overflow on MY.NET.130.86. Several university systems seem to also be of interest to a variety of sources trying a range of scans and exploits. I would have system logs checked on: 99.99.111.130 99.99.201.202 99.99.202.62 99.99.203.134 99.99.208.90 99.99.217.66 99.99.221.210 99.99.210.134 99.99.221.154 99.99.222.190 99.99.237.74 99.99.224.78 99.99.243.50 Watching the various patterns of alerts coming from a wide number of sources, it may also be a possibility that

External RPC call	Admin	The RPC vulnerability was described earlier. There are a large number of calls from outside sources to systems inside the network on port 111. Also, the fact that many of the calls only occur once, only to jump a few IP's to another host, suggest a possible scan for systems with RPC running. 64.77.62.20 is an example of seventy one alerts over six minutes that appear to span six of my subnets. No other responses from university systems are seen. 213.131.174.51 alerts here 43 times on Day 3 and on Day 4 triggers the "connect to 515 from outside" alert while going from MY.NET.132.210 to MY.NET.137.221 IP range in under two minutes. Scanning for printer services? Systems that do not need RPC running should have it disabled immediately, or at the very least block it with a security router or firewall at the network gateway..
SMTP chameleon overflow	Admin	CAN-1999-0261;Netmanager Chameleon SMTPd has several buffer overflows that cause a crash. One system attempted an overflow 151.193.165.225:2504 -> 99.99.253.41:25. There were only two alerts for this event, though the source IP was also involved in several other alerts that are local "Watch" lists.

SNMP public access	Admin	Simple Network Management Protocol (SNMP) is widely used by network administrators to monitor and administer all types of network-connected devices ranging from routers to printers to computers. SNMP uses an unencrypted "community string" as its only authentication mechanism. The default community string used by the vast majority of SNMP devices is "public". Attackers can use this vulnerability in SNMP to reconfigure or shut down devices remotely. Alternatively, they can sniff SNMP traffic to obtain insights to help with their attack plan If SNMP is allowing access from external network locations, external sources may have control of certain systems on affected servers. Servers listening on port 161 that are shown by the IDS logs as having been accessed or at least touched by outside sources should be examined. If not needed, SNMP should be disabled on our external networks. If not, I recommend a filter of SNMP (Port 161/UDP) at the border-router or firewall unless it is absolutely necessary to poll or manage devices from outside of the local network Only one source triggered two alerts here. ACTION: With the recent vulnerability announcement, I would run SNMPing tool on our 99.99 subnets to check for responding systems and disable. References: CAN-1999-0517

TELNET SGI telnetd format bug *content: "_RLD"; content: "/bin/sh";reference:arachnids,304; classtype:attempted-admin; sid:711*	Admin	The alert intercepts a potential shell command that would exploit a vulnerability in the TELNET daemon on specific versions of SGI-IRIX systems and be able to execute with root permissions. Patches are available. MY.NET.60.11 was the only recipient of this alert. However, this system has a lot of alert activity. It was scanned by multiple systems with different scan types and was fingerprinted as well. It is also the source of may portmap scans and it responded to ICMP echo requests. There is possible IRC activity and a handful of incorrect TELNET logins to non-university IPs. Need to see if this system really is a SGI system or not and look at what legitimate activity is going on here.
INFO - Web Cmd completed	Admin attempt	Not sure of the specific rule, but it may be associated with Web exploits and/or Code Red worm activity or normal web activity. MY.NET..100.165 (CS Department web server?) was the primary source. One might consider invoking a policy of no web browsing from servers to minimize the possibility of malicious code being executed at the same permission level as the (expected) privileged user running the browser (e.g, root)..

RFB – Possible WinVNC -010708-1	Attack	WinVNC is a freeware package developed by AT&T Labs for remote viewing of desktops. The software is susceptable to buffer overflow. The alerts might be failed logins or brute force attacks. I am not sure whether this alert is based on the WinVNC vulnerability or one of the two candidates listed below: CVE-2000-1164 WinVNC installs the WinVNC3 registry key with permissions that give Special Access (read and modify) to the Everybody group, which allows users to read and modify sensitive information such as passwords and gain access to the system. CAN-2001-0167 ** CANDIDATE (under review) ** Buffer overflow in AT&T WinVNC (Virtual Network Computing) client 3.3.3r7 and earlier allows remote attackers to execute arbitrary commands via a long rfbConnFailed packet with a long reason string. CAN-2001-0168 ** CANDIDATE (under review) ** Buffer overflow in AT&T WinVNC (Virtual Network Computing) server 3.3.3r7 and earlier allows remote attackers to execute arbitrary commands via a long HTTP GET request when the DebugLevel registry key is greater than 0. There were only five alerts over the five days to external IPs. I would check MY.NET.234.142, MY.NET.218.142, MY.NET.150.143, MY.NET.97.225 and MY.NET.140.117 if this is not authorized activity.

RPC portmap request rstatd	Attack	This vulnerability may allow an RPC program to register with the Portmapper, replacing known services with trojans. 24.48.114.169 runs through five of my subnets in one minute and is associated with other RPC call alerts. This is a candidate for blocking at the border router ACTION: Besides disabling RPC at least on any external system, we should also block the RPC port (port 111) at the border router or firewall and block the RPC "loopback" ports, 32770-32789 (TCP and UDP) per SANS guidance.
spp_http_decode: CGI Null Byte attack detected	Attack	A candidate vulnerability exists from the Way-board CGI program allows remote attackers to read arbitrary files by specifying the filename in the db parameter and terminating the filename with a null byte. 212.162.178.140 is running this and associated with many other alerts affiliated with Code Red (http directory traversal and CGI-script alias). 209.122.45.243 triggers quite a few alerts very quickly and the source port is incrementing in concert with the destination IPs.
spp_http_decode: IIS Unicodeattack detected	Attack	The unicode attack method exploits the capability of embedding hex characters and escaped control characters in URLs. This is one of the primary attack methods of Code Red. MY.NET.100.165 is source for this as well as 40 ACTION: Check alerted systems for modified files

SUNRPC highport access!	Attack	This is similar to the first alert described, the Attempted Sun RPC high port access, except that this alert supposedly describes the activity as being successful, rather than attempted. Any systems on the destination end of this alert should be checked. Several systems that were shown in this activity though had a source port of 22, being the default port for secure shell, which may suggest that at least some of these alerts may be false positives, since they may just be random high ports initiating a connection with an outside server, and it is the return packets which are triggering the alert, though this would not be the case in all situations, such as the one illustrated above. Reference: CVE-1999-0189 216.218.255.227 has a string of several hundred alerts hitting MY.NET.218.118 every two to seven minutes, but no other associated alerts. 209.61.191.39 is also hitting this port and is associated with a Queso fingerprint. Scan + admin attempt – watch this guy and check the school systems on the this end. 207.46.230.218 is both attempting this connect along with a TELNET alert. ACTION: Check MY.NET.60.11 and MY.NET.218.118 as to why all the interest/alerts with them as destination. Consider blocking this port at external router.

WEB-IIS Unauthorized IP Access Attempt	Attack	CAN-1999-1233 ** CANDIDATE (under review) ** IIS 4.0 does not properly restrict access for the initial session request from a user's IP address if the address does not resolve to a DNS domain, aka the "Domain Resolution" vulnerability. Only two university sources are involved here. Could be routine traffic to older IIS version.
WEB-MISC Lotus Domino directory traversal	Attack	CVE-2001-0009 Directory traversal vulnerability in Lotus Domino 5.0.5 web server allows remote attackers to read arbitrary files via a .. (dot dot) attack. This could be normal traffic to the university CS web server.
FTP passwd attempt	Attempted Admin	This may be normal or it may be an attempt to gain access at guessing passwords. The source 128.8.96.149 is involved with a lot of scans on the afternoon of Day 2. Need to see what FTP services are authorized on MY.NET.70.148. No other responses from my system.
RPC tcp traffic contains bin_sh	Bad unknown	This rule seems to have added some key text embedded in remote procedures calls that would indicate an attempted admin or opening of a shell. ACTION: Check syslogs for anomalous entries.

Tiny Fragments - Possible Hostile Activity	Bad Unknown	Tiny Fragment attacks create an initial fragment that is so small so the TCP header is split and the TCP port number is in the second packet. Tools like Nmap or Fragrouter help create fragmented packets that help bypass non-stateful IDS detection. Summary: This could be a variety of attacks, including an ICMP scan, a covert channel (data being transmitted through ICMP packets), a denial of service through malformed ICMP packets, or another as of yet unknown purpose. The fact that many packets came from a single IP to a single IP lends credence to the possibility of a covert channel, since there needs to be enough packets transferred to move the data. Reference: CVE-1999-0683, CVE-1999-0804 208.25.55.145 is one source that is also involved with null scans. Consider blocking this source.
INFO Inbound GNUTella Connectrequest INFO Outbound GNUTella Connect accept INFO Outbound GNUTella Connect request	Bad- unknown	Gnutella is a file searching/sharing program. There are a wide range of external and internal sources involved with this and there may be copyright infringement and/or liabilities associated with this activity. There is also an inherent bandwidth difficulty raised by the clients sending Pings to discover other clients. Blocking is difficult as users could ride over other common ports. University systems may have to be watched for GNUtella activity and users individually reprimanded or suspended from computer usage. http://rr.sans.org/firewall/gnutella.php

INFO Napster Client Data INFO napster login INFO napster new user login INFO napster upload request	Bad-unknown	Default port for Napster applications is 6699 and 6700. Client machines looking for MP3 files to share find each other through central servers and transfer files directly. Concerns are over copyright infringement or worse, malicious code transfers. Similar recommendations with the GNUTella intercepts.
MISC Large UDP Packet *dsize: >4000; reference:arachnids,247; classtype:bad-unknown; sid:521*	Bad-unknown	These alerts are growing over the five days. APNIC.NET source IPs start with the alerts on Day 1, going to over three thousand hits on Day 3, and more than twelve and thirteen thousand hits respectively on Days 4 and 5. Could it be that the University has some streaming media servers for off-site training that are causing this?
MISC PCAnywhere Startup	Bad-unknown	These alerts could be legitimate Symmantec pcAnywhere clients or a probe/scan with the same tool.
MISC Source Port 20 to <1024	Bad-unknown	Possible old versions of BIND – upgrade.
MISC source port 53 to <1024	Bad-unknown	The high talker here – 134.93.19.12 – might be working DNS queries or zone transfers with 99.99.130.122 (source and dest port 53). 207.171.178.5 (Amazon.com) is also working port 53 to 53 between two of my university systems: 99.99.140.16 and 99.99.140.17. 159.230.4.2 is talking to what is probably one of my primary DNS servers. From the volume of interaction on other days, I think that 99.99.1.3,4 and 5 are university DNS systems.

FTP DoS ftpd globbing	DDOS	NAI COVERT Labs reported a file globbing vulnerability in ftpd daemon which can lead to a root compromise. CAN-2001-0247 http://archives.neohapsis.com/archives/vulnwatch/2001-q3/att-0038/00-part If this is a SGI system it should be patched. These alerts were from University sources going to external destinations (U. of Dayton and Monmouth U.).
ICMP Source Quench	DDOS	Possible indication of spoofing
INFO FTP anonymous FTP	Possible Access Attempt	This may be a routine login attempt.
DNS SPOOF query response with ttl	Recon	Time to live parameters can be manipulated in crafted packets to help map networks. With each packet reaching out one step more, routers and firewalls can sometimes be identified along the path.

ICMP Address Mask Request (Undefined Code!) ICMP Echo Request Broadscan SmurfScanner ICMP Echo Request BSDtype ICMP Echo Request CyberKit 2.2 Windows ICMP Echo Request Delphi-PietteWindows ICMP Echo Request L3retriever Ping ICMP Echo Request Nmap or HPING2 ICMP Echo Request Sun Solaris ICMP Echo Request Windows ICMP Fragment Reassembly TimeExceeded	Recon	The use of ICMP packets can provide a wealth of information for the attacker. Responses, and no responses both can be used to help map out a network and do some fingerprinting. All of the Nmap or HPING2 alerts are originating from my university systems. A high talker 99.99.226.18 is focused on two systems 204.71.200.75 (Cable Wireless) and 206.79.171.51 (Exodus Comms) and might be performing system checks for load balancing between). These checks seem to be running regularly throughout the entire day 99.99.208.82 is also performing regular pings to Boston U. systems

ICMP Destination Unreachable ICMP Destination Unreachable (Communication Administratively Prohibited) ICMP Destination Unreachable (Fragmentation Needed and DF bit was set) ICMP Destination Unreachable (HostUnreachable) ICMP Destination Unreachable (Network Unreachable ICMP Destination Unreachable (Protocol Unreachable) ICMP Destination Unreachable(Fragmentation Needed and DF bit was set) ICMP SRC and DST outside network	Recon	99.99.14.1 and 99.99.16.5 are the sources for most of these alerts on Day 4 For the ICMP alert, this is ICMP traffic being sent to a multicast address, which explains why it is probably being also broadcast to our local network. It may be part of a DOS or smurf attack against a different network, though the broadcast address it is sent to may cause collateral damage, especially if the provider's routers are allowing multicast traffic. For the UDP traffic, since it also is connectionless, it could be a similar situation to the ICMP traffic, especially since it also is being sent to broadcast addresses of .254 and .255, though there are several instances of non-broadcast addresses being used as the destination. The volume of traffic is so large though (at over 290,000 alerts) that the theory of it being part of a denial of service sent to broadcast addresses, as supported by the majority of the data, is the most probable. Reference: CVE-1999-0513 On all five days, 99.99.140.9 and 99.99.219.154 are the source of most of the traceroutes and Dest. Unreachable alerts. These should be checked for correct configurations. At the same time, 99.99.14.1 and 16.5 are the destinations that trigger most of the unreachable alerts. It is unclear whether there may be a problem with router configurations, or incorrect advertising of IPs that are not publically routable.

ICMP traceroute	Recon	As mentioned in the ICMP section, there are a couple University systems that seem to be involved in the majority of the traceroutes and routing/DNS configurations should be checked.
IDS475/web-iis_web-webdav-propfind[arachNIDS]	Recon	reference:cve,CVE-2000-0869 The default configuration of Apache 1.3.12 in SuSE Linux 6.4 enables WebDAV, which allows remote attackers to list arbitrary directories via the PROPFIND HTTP request method.
IDS552/web-iis_IIS ISAPI Overflow ida nosize [arachNIDS]	Recon	reference:cve,CAN-2000-0071 IIS 4.0 allows a remote attacker to obtain the real pathname of the document root by requesting non-existent files with .ida or .idq extensions.
NMAP TCP ping!	Recon	This seems to be an example of the TCP ping from NMAP, which is usually used when the normal ICMP echo request is not expected to be responded to. Reference: http://www.insecure.org,
Null scan!	Recon	The Null scan is used to penetrate certain firewalls which block TCP packets based on flags. Null packets have no flags set, and a sequence number of zero. They elicit RST packets from closed ports, and no reply from open ports, since they discard the null packet. Based on the ports being scanned, I believe certain services and Trojans are being scanned for (such as Napster on port 6699). Reference: http://www.nwconnection.com/2001_03/pdf31/cybercrm31.pdf 141.157.85.167 is involved as the source for multiple scan types. Consider blocking the IP.

Probable NMAP fingerprint attempt	Recon	Summary: Nmap can be used to fingerprint operating systems through the information in their return packets (sequence numbers, ports open or closed, etc.). However, it requires at least one open and one closed port to be accurate, by its own "admission" during use. The fact that the source port in this example is 6699 suggests this may actually be a Napster data transfer though. References: N/a. More information about Nmap can be acquired at http://www.insecure.org/nmap
Queso fingerprint	Recon	Queso is another an older type of fingerprint scan designed to determine the target's operating system. This information can be used later for more directed cracking purposes. Here the Auth port 113 is being hit primarily by 198.186.202.147 References: CAN-1999-0454
SCAN FIN	Recon	24.112.76.76 is running this scan and should be watched.
SCAN XMAS	Recon	This scan has all the TCP flags set (i.e., lit up like a Christmas tree). It is definitely not a legal packet.

SMB Name Wildcard	Recon	The Server Message Block (SMB) protocol, also known as the Common Internet File System (CIFS), enables file sharing over networks. Improper configuration can expose critical system files or give full file system access to any hostile party connected to the Internet. This shows data sent to the NetBIOS ports on several systems within the network. This type of traffic can be used to identify the operating system (most systems with port 137 open are windows machines), or also can lead to denial of service attacks or file system access using a directory traversal exploit. Any internal systems touched on ports 137-139 by outside sources should be examined and inbound Port 139 should be blocked. There are a number of University systems as destinations on these alerts. References: CVE-1999-0225, CAN-1999-0495, CAN-2000-0544 Windows NT and Windows 2000 hosts allow a remote attacker to cause a denial of service via malformed DCE/RPC SMBwriteX requests that contain an invalid data length.

SYN-FIN scan!	Recon	These are two more types of port scans, similar to the Null scan, but with different flagsets and different responses elicited. The portscans coming from internal addresses may very well be false positives. However, the syn-fin scans from outside to many internal addresses are a form of mapping the network. 63.203.103.68 is running this and Null Scans on our network. References: http://www.nwconnection.com/2001_03/pdf31/cybercrm31.pdf

WEB-CGI archie access *attempted recon* WEB-CGI calendar access *attempted recon* WEB-CGI csh access *reference:cve,CAN-1999-0509;classtype:attempted-recon* WEB-CGI files.pl access *attempted-recon* WEB-CGI finger access *arachnids,221; reference:cve,CVE-1999-0612;classtype:attempted-recon* WEB-CGI glimpse access *reference:cve,CVE-1999-0147; reference:bugtraq,2026; classtype:attempted-recon* WEB-CGI ksh access *reference:cve,CAN-1999-0509;classtype:attempted-recon* WEB-CGI redirect access *reference:cve,CAN-1999-0509;classtype:attempted-recon* WEB-CGI rsh access *reference:cve,CAN-1999-0509;classtype:attempted-recon* WEB-CGI scriptalias access *cve,CVE-1999-0236; reference:bugtraq,2300; reference:arachnids,227; classtype:attempted-recon* WEB-CGI tsch access WEB-CGI upload.pl access *classtype:attempted-recon* WEB-CGI w3-msql access *bugtraq,591; reference:cve,CVE-1999-0276; reference:arachnids,210;classtype:attempted-recon* WEB-CGI webgais access *arachnids,472; reference:bugtraq,2058; reference:cve,CVE-1999-0176;classtype:attempted-recon*	Recon	Exploiting a Common Gateway Interface (CGI) vulnerability would allow a hacker to run commands at the same permission level as the web server. Automated programs like Whisker or cgiscan walk through the web server in search of an exploitable program. 99.99.6.7 is a frequent destination for these access attempts as well as Queso fingerprinting. I suspect this is a web server, but we need to ensure it is patched and unneeded cgi programs are either removed or updated.
WEB-MISC count.cgi access	Recon	An expoit in the popular web statistics program allows viewing of any GIF on the server – even if it is not in the web root directory. Patch with v2.4 of wwwcount
WEB-MISC http directory traversal	Recon	Exploits idg.dll allowing viewing of web files. Patch IIS.

TOP TALKERS LIST

The practical asks for a "top talkers" list – who are the top ten talkers in terms of Scans, Alerts, and/or OOS files, using what I consider to be meaningful criteria in the log files. I ran a series of awk, sed and shell scripts to merge the five days worth of alert files and extract both the destination and source IP addresses. From this list, a unique count was made of the occurrences for each IP. The two tables below identify the top ten external talkers and the top ten talkers from MY.NET.

Top 10 External Talkers

Rank	Frequency	IP
1.	22599	211.90.176.59
2.	10925	211.90.88.43
3.	9211	211.90.164.34
4.	8620	130.161.37.101
5.	7342	211.96.99.59
6.	7024	200.250.65.1
7.	6922	217.57.15.133
8.	6706	130.206.73.191
9.	6489	130.219.176.111
10.	6397	200.26.105.130

Not completely unexpected, Top Talkers #1, 2, 3 and 5 all come from Asia Pacific Network Information Center. #4 comes from Technische Universiteit Delft (NET-DUT-LAN). This is also the source of the Day 4 Red Worm traffic.

Top Ten Local Talkers (from MY.NET)		
Rank	**Frequency**	**IP**
1.	24460	99.99.140.9
2.	17010	99.99.14.1
3.	16550	99.99.100.165
4.	14730	99.99.16.5
5.	12677	99.99.253.114
6.	6841	99.99.226.18
7.	6624	99.99.219.154
8.	6270	99.99.1.3
9.	5244	99.99.208.82
10.	4889	99.99.30.2

From my own university servers, there is a significant volume difference just between the top ten talkers. 99.99.140.9 is involved in over six times the volume as 99.99.30.2.

Though the current Top Ten Hackers list was not available from a historical perspective, I did take

a look at the IPs listed recently to see if any correlation existed. The list from http://www.dshield.org/top10.html is always a good stop to see if you should be blocking anyone who is misbehaving. No correlation to the top talkers in data analyzed for this report.

Top Ten Watch/Block list from Dshield database as listed on incidents.org	
IP Address	**Host Name**
211.110.1.47	211.110.1.47
132.192.43.245	mrpark1.utmem.edu
211.251.241.98	211.251.241.98
128.242.217.103	128.242.217.103
64.175.21.	adsl-64-175-21-195.dsl.snfc21.pacbell.net
212.41.199.5	212-41-199-5.adsl.galactica.it
211.21.67.110	211.21.67.110
143.236.23.113	cis324.uwsp.edu
128.59.205.170	bus205-170.gsb.columbia.edu
134.34.19.101	wl-869.wlan.uni-konstanz.de

SOURCE ANALYSIS/REGISTRATION

Five external source addresses were selected to gather additional information and registration information. The reasons I selected these hosts for further investigation is describe with each extract from ARIN.

Out of 802 Large UDP Packet alerts on September 1, 2001, 651 of the alerts were generated from 64.157.10.118 and 114 alerts were generated from 61.152.19.95. I am concerned about the first IP since it corresponds to a potential Red Worm High Port alert.

LOOKUP #1 for 64.157.10.118

Level 3 Communications, Inc. (NETBLK-LC-ORG-ARIN)
1025 Eldorado Boulevard
Broomfield, CO 80021
US
Netname: LC-ORG-ARIN
Netblock: 64.152.0.0 - 64.159.255.255
Maintainer: LVLT
Coordinator:
level Communications (LC-ORG-ARIN) ipaddressing@level3.com
+1 (877) 453-8353

The second site was examined since it also had some related alerts of ICMP Fragment Reassembly Time Exceeded. Both IPs were interfacing with MY.NET.153.113

LOOKUP #2 for 61.152.19.95

Asia Pacific Network Information Center (NETBLK-APNIC2)

These addresses have been further assigned to Asia-Pacific users.
Contact info can be found in the APNIC database,
at WHOIS.APNIC.NET or http://www.apnic.net/
Please do not send spam complaints to APNIC.
AU
Netname: APNIC3
Netblock: 61.0.0.0 - 61.255.255.255
Maintainer: AP

The next IP examination was triggered after looking at the ICMP Unreachable alerts. It seems as though 200.250.65.1 was a source of a lot of traffic to MY.NET.30.2. It was also very active with alerts for WEB-MISC Attempt to execute CMD as well as IIS ISAPI Overflows. The IP address appears to be from an IP block assigned to Brazilian users

Excerpt from SnortSnarf:
2 different signatures are present for 200.250.65.1 as a source
1231 instances of IDS552/web-iis_IIS ISAPI Overflow ida nosize
1310 instances of WEB-MISC Attempt to execute cmd

There are 286 distinct destination IPs in the alerts of the type on this page.

LOOKUP #3 for 200.250.65.1
Comite Gestor da Internet no Brasil (NETBLK-BRAZIL-BLK2)
R. Pio XI, 1500
Sao Paulo, SP 05468-901
BR
Netname: BRAZIL-BLK2
Netblock: 200.128.0.0 - 200.255.255.255
Maintainer: BR
Coordinator:
Registro.br (NF-ORG-ARIN) blkadm@nic.br
+55 19 9119-0304
Domain System inverse mapping provided by:
NS.DNS.BR 143.108.23.2
NS1.DNS.BR 200.255.253.234
NS2.DNS.BR 200.19.119.99
These addresses have been further assigned to Brazilian users.
Contact information can be found at the WHOIS server located
at whois.registro.br and at http://whois.nic.br
Record last updated on 30-Aug-2001.
Database last updated on 29-Sep-2001 23:14:31 EDT.

LOOKUP #4
On 4 September, possible Red Worm High Port alerts climbed into the Top 5 list (by volume). It seems as though 103.161.37.101 was responsible for 4242 out of 4256 of the alerts. The source is in the block belonging to a university in The Netherlands.

Technische Universiteit Delft (NET-DUT-LAN)
Dienst Technische Ondersteuning
2600 AJ Delft,
NL
Netname: DUNET
Netblock: 130.161.0.0 - 130.161.255.255
Coordinator:
Kruijf, Freek de (FD18-ARIN) SSC@TUDelft.nl
+31 15 2783226 (FAX) +31 15 2783787

LOOKUP #5
On 5 September I noticed that there were many possible IIS Unicode attacks with only two sources. After drilling down, I found that one of the two IPs was responsible for 17 of the 18 alerts as well as 13 WEB-MISC Attempt to execute cmd alerts. The source was 194.175.74.65

European Regional Internet Registry/RIPE NCC (NETBLK-RIPE-C2)
These addresses have been further assigned to European users.
Contact info can be found in the RIPE database, via the
WHOIS and TELNET servers at whois.ripe.net, and at
http://www.ripe.net/db/whois.html
NL
Netname: RIPE-CBLK2
Netblock: 194.0.0.0 - 194.255.255.255
Maintainer: RIPE
Coordinator:
Reseaux IP European Network Co-ordination Centre Singel 258 (RIPE-NCC-ARIN) nicdb@RIPE.NET
+31 20 535 4444

CORRELATION FROM PRIOR ANALYSIS
There were several other GCIA analysts with correlating information on the Watchlist 000220 IL-ISDNNET-990517 alert.

Benjamin Robinson, Analyst number 0370
http://www.sans.org/y2k/practical/Benjamin_Robson_GCIA.zip] tracked similar activity in his Practical in June of this year. I concur with his recommendations to treat sources from this IP Block as hostile and to consider blocking them at the external router.

Chris Baker Analyst number 0371
http://www.sans.org/y2k/practical/Chris_Baker_GCIA.zip] also detected and analyzed a lot of traffic associated with this Watchlist. He repeated concern from Chris Kuenthe [Analyst number 0303, 22 February 2005 http://www.sans.org/y2k/practical/chris_kuethe_gcia.html] that this traffic could be used to troll for trojans and backdoors.

NAI Labs provided good analysis of FTP Globbing vulnerabilities:
http://archives.neohapsis.com/archives/vulnwatch/2001-q3/att-0038/00-part

Laurel Chappell has an excellent paper on Scans posted on Novell Connection web site.
http://www.nwconnection.com/2001_03/pdf31/cybercrm31.pdf

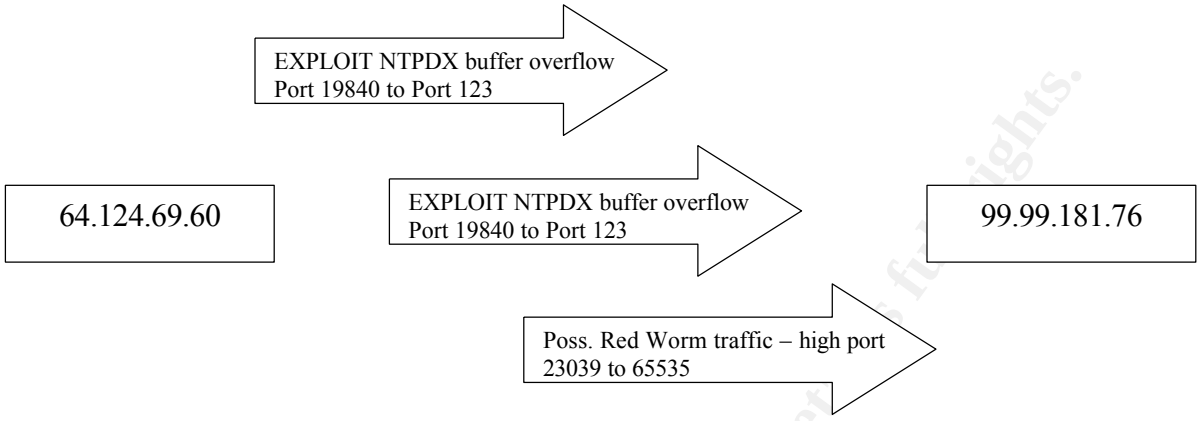
LINK GRAPHS

Link graphs can sometimes help visualize the traffic flow between source and destination hosts. A couple line graphs were developed here to portray communications that appeared irregular.

The first link was between a very active scanner (63.23.103.68) and his primary interest (99.99.225.30) on my university network. Four types of scans were detected and one ISAPI overflow, all sourced from the external host. When broken out for detailed analysis, the high level of interest in 99.99.225.30 is very obvious. Fortunately, there was no other traffic coming from the scanned system to indicated that the system had been compromised.

63.23.103.68	**Src Port**	**Direction** Type (# of occurrances)	**Dest Port**	99.99.225.30
	0	➔ Null Scan (213)	0	
	60377 6112 15563 1 0 6294 0 98 10 0 96	➔ Null Scan (13)	25703 6112 32939 23222 257 8285 48222 22658 48481 44602 49146	
	49066	➔ ISAPI overflow (2)	80	
	59329	➔ SCAN XMAS (1)	29290	
	45973	➔ SCAN FIN (1)	19513	
	14842	➔ SYN-FIN Scan (3)	3975	

The second link graph is somewhat simpler. I zeroed in on possible Red Worm traffic and found some associated traffic between 64.124.69.60 and my system 99.99.181.76 as illustrated below.



SCAN ANALYSIS

Based on the scanning reports, any instance of university computers acting as the source of a scan will be investigated further. The following was an excerpt of 99.99.*.* IPs as scan sources from the SCAN files from Sept 1st, with 1000 or more scan instances for the day.

Top Local Scanners Sept 1, 2001	
Frequency	**IP Address**
37376	99.99.160.114
7942	99.99.218.50
4234	99.99.202.38
3946	99.99.217.54
3832	99.99.201.66
3416	99.99.201.42
3236	99.99.219.198
3118	99.99.221.22
2964	99.99.202.62
2666	99.99.233.202
2445	99.99.235.186
2403	99.99.218.46
2116	99.99.235.150
1776	99.99.217.150
1561	99.99.202.26
1524	99.99.221.98
1282	99.99.206.226
1271	99.99.201.10
1268	99.99.217.254
1129	99.99.219.58
1085	99.99.212.50

1079	99.99.150.220

COMPROMISED SYSTEMS/DANGEROUS ACTIVITY SUMMARY

In addition to the systems that were listed in the Detailed Alert Review section, the following is a summary of systems that I am concerned about and need to investigate further or clarify the usage of the system at the school.

There were over six hundred Red Worm alerts with university systems as sources. They should be scanned locally if they are not up-to-date with patches. IPs of special interest (other alerts as well):

99.99.150.133
99.99.20.10
99.99.205.110
99.99.205.130
99.99.217.150
99.99.217.150
99.99.219.198
99.99.221.242
99.99.222.74
99.99.234.138
99.99.234.138
99.99.242.218
99.99.253.24
99.99.253.43
99.99.253.51
99.99.6.35
99.99.6.39
99.99.6.47
99.99.69.64
99.99.98.238

Check 99.99.6.39 possible MyRomeo Worm infection alert.

A lot of activity (2000 – 4000 alerts) with 99.99.235.14 and 99.99.98.190 involved (both source and destination) possible with Sub7 or Ramen trojan activity. These alerts are either fixed source ports while running through wide IP ranges, or are static27374 ports (known TCP port for Subseven v2.1). Need to investigate potential misuse of servers. 99.99.60.14, 99.99.253.106, 99.99.217.194 and 99.99.253.114 also alerting as sources of Sub7/Ramen activity.

209.73.162.12 is repeatedly active on FrontPage shtml.dll alerts. If this is not routine web traffic, consider blocking the source IP. I would also disable Frontpage if it is not needed as a web service.

DEFENSIVE RECOMMENDATIONS

Many defensive procedures are recommended, based on an incomplete understanding of what external interfaces are critical to this campus and without a complete map of the external and internal networks at the University. Based on the traffic analysis I make the following recommendations:

We should strongly consider blocking a couple of IP ranges until the ISPs cleaned up their act. Specifically the APNIC.NET and Comite Gestor da Internet no Brasil.

Generically, I would first make a comprehensive review of needed ports and services on the local systems that were considered compromised or were given frequent attention from the public.

Based on observed alerts and SANS FAQ on port blocking, the following recommendations are provided for consideration (my comments underlined after SANS notes):

1. Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp) Most all of these events were observed from the outside and from the campus.

2. RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp) Portmapping, RPC exploits and NFS activity (large UDP packets) were observed in the alerts. I could expect some intra-university file exchanges between different IT projects. This should be blocked with those exceptions.

3. NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). With several alerts on SMB wildcard, port 137 activity was observed. If possible, this should be blocked and activity constrained to the campus network.

4. X Windows -- 6000/tcp through 6255/tcp. We had a couple alerts on X11 and don't know why the school would need this as an external interface. Block it if unnecessary.

5. Naming services-- DNS (53/udp) Block DNS traffic to all machines which are not DNS servers and DNS zone transfers (53/tcp) except from external secondaries.

6. Mail-- SMTP (25/tcp) My ideal mail flow would flow through a viral content scanner. Additionally, I would consider stripping off attachments with probably harmful executables (for instance: .exe, .scr, .bat). If I have a firewall, it would only exchange mail with authorized campus mail servers.

9. Miscellaneous—

NTP – Ensure school NTP servers are patched. Recommend blocking inbound port 123 (NTP). Best architecture would be to have one NTP server configured, possibly with a backup, for all university systems to reference. No need for everyone to go outside to synch themselves.

SNMP (161/tcp and 161/udp, 162/tcp and 162/udp) – Another candidate to block at the external

router – unless some ISP needs some router maintenance interface that isn't already out-of-band.

10. ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and destination unreachable messages except "packet too big" messages (type 3, code 4). There was a lot of this activity, both inbound and outbound. Unless there is some strong need, this should be blocked or at least severely constrained.

Additional recommendations:

- Scan, rebuild the infected Code Red boxes, re-scan and put back on-line
- Check systems that were flagged with suspected trojan traffic.
- Search out and investigate all servers that showed up as active scanners.
- Run SNMPing and disable all systems that respond.
- Disable RPC services on any external Unix systems.

OVERVIEW OF ANALYSIS PROCESS

My analysis method starts from the top, zooms in and then backs out again. After collecting some top-level numbers, a detailed examination is made of individual alerts for each day with significant events noted. When all traffic has been analyzed, comparisons are made of the significant events and trends common in all of the logs.

A valid homenet IP had to be established to run the SNORT logs through SNORTSNARF. After a search to ensure uniqueness throughout the alert files, instances of MY.NET were replaced with 99.99.*.* through the use of the sed script below.

sed 's/MY\.NET/99\.99/g' alertfile > outputalertfile

The Alert files were run through SnortSnarf (v010821.1) to help manage the immense volume of data. A manual process of reviewing the top alerts (by occurrence) then took place. Items of interest were documented for further detailed analysis. These items included: high severity alerts (from already compromised systems), high volume alerts associated with very few sources or destinations (e.g., less than 10).

Shell scripts were developed to combine all five days of data and determine who the top talkers were. The following awk and shell commands extracted the Destination and Source IP out of the concatenated alert files. Similar scripts were used for the SCAN files.

awk 'BEGIN {FS = "]"}; {print $3} alertfile.txt | awk '{print $1} >longlist.txt
awk 'BEGIN {FS = "]"}; {print $3} alertfile.txt | awk '{print $3} >> longlist.txt

This script will provide the sorted IPs based on the number of occurrances (alerts) of that IP. It is important to sort the list first to help the uniq command elimiate duplicate IPs.

Sort|uniq –c|sort –r –n –k 1