Global Information Assurance Certification Paper

Providing Network Traffic Analysis Services to a Government Contractor

A Scenario for GIAC Enterprises

GCSC Practical Assignment
Version 1.0

Submitted for Certification By:

Chris Compton, GSEC, GCIA
Monday, April 19, 2004

Part I: Methodology and Process

Business Structure

GCSC Consulting is a small business, organized as a Limited Liability Company, consisting of two consultants, and two technicians. It has been in operation since 1998. The primary service of the company is network traffic analysis for intrusion detection. One consultant has experience concentrated in the private sector with almost 40 years of experience in various private sector industries, 75% of which has been working in federal government contracting. The managing consultant has a combination of private sector experience and public sector experience with the federal government, with ten years of experience in the information technology field, half of which was full time in security. The security technicians both have approximately three years of experience, with one year of specialized experience in security. Their duties are maintaining the business network and three computer labs. The technicians perform a majority of the travel for setting up and configuring the monitoring equipment at customer sites, and coordinating the technical resources required to perform monitoring. The technicians also monitor the equipment for proper operation, and assist in correcting network security problems.

Business Methodology

The target audience of the company is federal contractors, and a secondary target audience is federal government agencies. There are two teams, which consist of a consultant and a technician. This allows for two simultaneous projects to occur at once. All staff holds the GIAC Security Essentials Certification (GSEC). The consultants are both GIAC Certified Intrusion Analysts (GCIA). The technicians are Microsoft Certified System Engineers (MCSE).

The company depends heavily on word of mouth, repeat customers and referrals for sales and marketing. Approximately 6-10 hours per week of regular time is spent marketing through traditional sales approaching new customers, and around 8-10% of net project earnings are invested into marketing materials and advertising. The company utilizes materials such as letters, brochures, trade magazine ads, portfolios, and a very detail and extensive website.

The goal of each team is to perform at least 26 audits per year. In cases where additional security projects are taken on, this amount may be adjusted, or the project work may be sub-contracted. The teams are paid on a commission style basis. This encourages all the staff to sell and perform, and allows high achieving team members to earn higher salaries. The consultants (18%) are typically the “sales” people. If a technician (8%) closes a sale, we pay bonuses up to 5% above the base percentage.

Customer Requirements

GCSC Consulting has learned of an opportunity with GIAC Enterprises, a government contractor with the U.S. Department of Defense. This contractor develops and maintains a database of maintenance records, a portion of which contains information classified at a secret level. The contractor has one corporate office, and two project offices. The first project office is located 20 miles from the corporate office, and the second project office is approximately 250 miles away.

The client's business currently has a staff of 25, but expects to double or triple that amount over the next year. They also utilize sub-contractors as needed. The client has just been awarded a new contract, which is quadrupling the income of the company.

Some of the information the customer handles is classified as secret. Due to the possibility of contact with this type of information, a minimum clearance at the level of secret is required. One team maintains clearances at a top secret level for another project, so this team would be the best suited to serve this customer. For this project, due to the security clearances required, only one team can participate. Because of the location of the project offices, the consulting team will have to arrange two sessions. The corporate office contains 75 computer systems, with various versions of Linux and Windows operating systems. The project offices house three computers each connected to a WAN which connects back to the corporate office. The computers used at the secret clearance level are located at the two project sites; however, they are disconnected from any outside network connections, and connected only to the secret network. Since the secret network belongs to a third party (U.S. Government), monitoring these segments is unauthorized.

The Approach

When identifying potential clients, we look for businesses that are growing at a pace that far exceeds their capability to keep up with many aspects of their growth. Many federal contractors find themselves growing at rates exceeding 100%.[1] We watch the government contract solicitations, newspapers, contractor websites, and we utilize a small network of defense contractor insiders to get the best leads on who would be most in need of our services. Many of the smaller contractors are very apprehensive about the security of their systems and have little idea what is happening on their networks. This becomes a larger, nagging problem as the contractor grows in size.

[1] Washington Technology

This can be paralyzing for the contractor at times, thus many seem to ignore the problem – until approached. Surprising enough, some of them even provide IT services to the federal government, which is often another area of growth for the business. Through displaying our expertise, we are often tapped for projects as subcontractors for federal government projects.

Part II: Proposal and Pitch

Mery C. Eoh
GIAC Enterprises
123 Anytown, USA 12345-678
(111) 222-3333

Dear Mery:

Ima Referrer spoke with me last week about your company's recent growth, and your growing concern for the security of your information. We recently performed a network traffic audit for Ima's business, which was a great success in helping them protect their future. Ima conveyed your apprehension regarding the security of your computer systems, and finding the right people to help you. GCSC Consulting's team is a perfect fit for your needs.

As you are probably aware, the federal government is increasingly concerned over the security of their contractors. The U.S. Department of Defense recently began enforcing a new requirement for secure communications with all DoD vendors, strictly limiting those who are not in compliance. This trend is not likely to change soon. If your business is unprepared, and your security is not under control, you could find your current and future business with the government hampered, or at a standstill.

GCSC Consulting has the expertise to evaluate the security of your organization. Please review the attached proposal for an audit of your network, and I will contact you next week to discuss any questions you may have regarding this proposal. At your convenience, we will meet with you and your staff to answer your questions, and make adjustments to the proposal if necessary. We encourage you to bring your technical staff to ask us detailed technical questions about the review process. Thank you for your time and consideration, and we look forward to working with you!

Sincerely,
<*Signed*> Joe Consultant
Project Manager
GCSC Consulting
1-800-123-GCSC

<*Hand Written Note*> P.S. **If you purchase within the next 10 days, we will provide a free 90-day subscription to our vulnerability alert service.** Our analysts personally evaluate the latest high risk threats and alert you with step-by-step instructions when you need to take action. (An $1800 value)

Executive Summary

Every day, GCSC Consulting takes the worry out of security for businesses just like you. Through our comprehensive network analysis techniques, you will know if your business systems are being used by intruders for private gain, or for a launching pad to attacking other systems. Know if your security measures are actually protecting your business, or if adjustments need to be made. When it comes to security, knowing is everything.

Our consultants provide professional, business class security services. We cover all phases of security, from planning and implementation, to auditing and remediation. Start your path to security with our network analysis to find out what areas of your security measures are working for you, and which aren't. We will provide you with a comprehensive report covering the security issues affecting you, and our expert recommendations for enhancing your network defenses. A one on one seminar at the conclusion of the analysis allows you to plan and respond to the issues facing your business. It will mark the beginning of your commitment to protecting the hard work of your organization, and the end of risking your future.

Your assigned GCSC Consulting Security Team will be with you from start to finish from your first project to the next. The consistent teamwork will be like having your own in-house security team, without the added expense. We are there when you need us most. We will know your systems, your staff, AND your company.

At GCSC Consulting, we know how demanding the growth of your company can be. You need the experience of professionals with certified security capability, and with over 50 years of combined experience in government contracting and information technology. Experience the top-notch customer service and expertise you expect from your own security team.

Case in point…

Interprofix, Inc.
October 1999
An outbreak of a destructive variant of the infamous Melissa virus wreaked havoc by deleting valuable proprietary software source code through networked drives. Systems were rapidly infected before virus scanners could catch it.

Information gathered in an assessment previously conducted by GCSC Consulting, found the company's source code storage solution was exposed to attack. During the team's facilitation at the review seminar, it was determined that backups were only performed monthly. As a result, a novel backup solution was developed that day, and implemented over the next three weeks to protect the company's critical asset: source code.

Four and a half months later, with a combination of full and incremental backups, information lost in the aftermath resulted in a few lost hours, rather than weeks or months.

Used with customer permission.

Company Profile

GCSC Consulting is a small business dedicated to providing professional, one on one security consulting to firms experiencing growth at exponential rates, and requiring the service of experts to protect them while becoming leaders in the government contracting industry.

We do not offer cookie cutter security at GCSC Consulting. All of the staff at GCSC Consulting holds industry certifications in information technology and security. Our consultants possess 50 years of combined experience in serving government contractors, and providing quality information technology services. We know the challenges that you face in the federal contracting industry, and we know IT. Our expert technicians work closely with you and your IT staff to provide the most secure and productive environment, based on your needs.

- GCSC Consulting has exposed covert communications channels, and hidden Trojan software undetected by vulnerability scanning software and eliminated them within minutes of discovery.
- Our analysts have saved companies like yours thousands of dollars through pin pointing system configurations, and software causing excessive bandwidth usage.
- Our highly skilled technicians prevented valuable company accounting and sales data from being leaked outside the internal network for 5 different government contractors.

Our Services

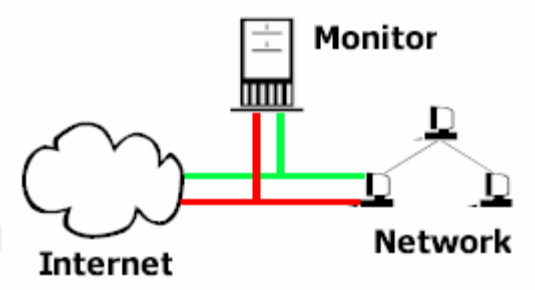
Security can be achieved effectively through a four step cycle. Adopting this process will provide you with a comprehensive strategy to implement, manage and maintain your IT security. Our service will jump start the process, by:

- Providing you with the information to implement critical policy that directly applies to your organization.
- Analyzing the current threats, and high risk vulnerabilities essential to protecting your assets.
- Delivering the information you need to fix the problems at hand, and build your defenses against the latest security threats.

- Verifying the security countermeasures you have implemented are actually functioning as intended.

Our network analysis process is customized specifically to your organization, and in less than 30 days you will have results. The analysis process is non-intrusive, and consists of four phases: Interviewing, Monitoring, Analysis, and Reporting.

Our monitoring devices use the latest technology in processing power, memory and storage capability. We run one of the most stable and secure operating systems existing, adapted from a version of UNIX developed at the University of California, Berkeley (BSD). Our systems are invisible to the network, and they capture traffic that flows across the network using a high speed access ports (TAPS). This ensures that your network performance is unaffected, and hooking up to your network requires minimal changes.



After the monitoring period, we retrieve the monitoring systems and the information is analyzed by a GIAC Certified Intrusion Analyst, with the experience to detect dangerous conditions on your network. The personal attention to detail is a level of service that is unmatched by automated vulnerability audits. With analysis of the network traffic we see first hand how your system configurations work – or do not work.

Here's how the process works:

	Consultant conducts interviews of staff. Technician installs equipment.
	Equipment monitors network traffic.
	Technician recovers equipment.
	Consultant analyzes and correlates data off-site.
	Results review seminar.

Day 1	Day 2 through 9	Day 10	Day 11 through 19	Day 20

Your team arrives on the first day and the consultant interviews key staff, while the technician prepares the monitoring equipment. The team visits with the management to find out what concerns exist, and to discuss the overall security of your organization.

On day two, the technician verifies the proper functionality of the monitoring equipment, and makes final adjustments to the location and configuration of the monitoring systems. On the tenth day, our technician returns to gather the monitoring equipment and returns your network to its original configuration.

Approximately three weeks from the start of the process, a detailed report will be ready for you, and a full review, including multimedia presentation will be made on site with the attendees of your choice. We will provide an overview of the findings, suggested plans of action, and how you can maintain your security in the future. The team will be there with you for valuable collaboration to answer your questions, and to formulate solutions to your problems.

The Team

Joe Consultant, GSEC, GCIA

Joe is the founder of GCSC Consulting. He is a former technical expert serving in federal law enforcement. Joe holds a Top Secret clearance, and handles our classified projects. He has managed the IT department of one of the nation's most innovative corporations, and managed security and auditing for a federal agency. Joe holds a B.S. Degree in Justice, with a concentration in Computer Programming. With over 10 years of experience in information technology, and certification as an intrusion analyst, Joe is a consultant you can depend on.

Needa Tech, GSEC, MCSE

Needa comes to us from a well known computer system manufacturer. She has handled security configuration for thousands of computers and devices. She also holds a Top Secret Clearance, making this the team capable of handling many projects where a clearance is a necessity. Needa has an Associate in Science with concentration in Computer Information Systems, four years of experience in information technology, and she maintains an industry security certification, along with the Microsoft Certified System Engineer credential.

Service Pricing

We are expensive. We charge what we do because we perform like no other business you will find. You will not find a company more dedicated, and more thorough than GCSC Consulting for your security. Knowing that, we strive to provide our unmatched service at an affordable price. The cost of a standard network traffic audit is $12,000 for clients with one site within a 150 mile radius. With three total sites to audit, we will audit each project site for an additional $3,000. The total project cost would be $18,000.

For this price, you get:

- One on one interaction with top experts in the field of IT security.
- Your own, consistent, assigned team for this and any future projects.
- Expert review on the health and status of your network.
- Detailed analysis of the effectiveness of your current security.
- Detailed report and plan of action.
- Comprehensive review seminar with your team.
- **Security for your organization**.

For this price, you **DON'T** get:

- Simple automated scans which can miss the critical vulnerabilities.
- Template based reports, which aren't tailored to your company.
- A report high in technicality, but low in functionality, leaving you to guess what you need to do next.
- A different, less experienced consultant than the one who convinced you to sign up for an audit.
- The typical exit interview, where you are merely there for show.
- A feeling like you wasted your money once we are done.

We require 50% of the total payment when the project starts. We will bill the remaining %50 a few days prior to the delivery of the final report. Payment is Net 10 Days.

Additional work performed by the team beyond the scope of this project will be billed at the standard billable rate of $112.00 per hour. This work is billed at half hour increments.

NOTE: The following discounts are only available for the next 30 days. Our typical discounts range from 3-5%.

Discount Option 1
Earn a 10% discount if the total amount is paid in full by the 20th day from the start of the project.

Discount Option 2
If the total amount is paid in full within the first three days of the project, we offer a 10% discount on the entire amount due.

Here is a breakdown of your options:

	Base	Option 1	Option 2
Payment #1:	$9,000	$9,000	$18,000
Payment #2:	$9,000	$9,000	
Discount:		10% off Payment #2	10% off Entire Amount
Total Cost:	$18,000	$17,100	$16,200

The Delivery

Your team hand delivers your detailed report on the vulnerabilities and other findings on your network, along with corrective actions. This is presented on site with your staff in a review seminar. Ask questions. Learn about your security. Plan your response.

During your review seminar, you will actively participate in shaping the security of your organization. You not only have the opportunity to ask questions, but you have the opportunity to learn from the findings of the team. Your team will work with you to come up with the most effective solutions for securing your organization, based on your ideas and input. You will be learning from some of the best security consultants in the industry.

The greatest feature is that your team will be assigned to you for future reviews and on other security projects. This means if you decide to expand your security infrastructure to support your new employees, your team will be assigned to lead this effort. In effect, this is like having your own security staff, who knows your networks and systems like you do. This will decrease the cost of performing services. It will speed up the planning and implementation of the task at hand, and you will rest better knowing you have a trusted and knowledgeable security team on the job.

<< END OF CUSTOMER PORTION OF PROPOSAL >>

Sales Methodology

For the type of services we offer, I have learned that the most effective push within companies of this type and size often comes from the top level, so it is essential to reach the President/CEO of the company and establish a line of communication. The overall success of security in an organization is often attributed to the "top-down" methodology, as well.[2] Another useful person to contact is a financial officer of the company. This person is often highly trusted and respected by the president, and the financial officer understands how important it is to secure information and protect the assets of the company. Reaching this person adds weight to the credibility of the services and enhances the line of communication with the President/CEO.[3]

In this situation, we have received information from a customer on a potential client, along with permission to mention that this person referred us to the company. This information is used to immediately distinguish this proposal as one which comes with a recommendation from a credible colleague, rather than a fishing expedition from some unknown consulting firm.[4] This can also put us at the top of the list if another security firm is soliciting or negotiating a contract for services.

The letter uses the "wisdom" of *Guerrilla Marketing*[5], and an attached proposal is specifically tailored to the company. No action is required of the customer, as it is stated that the project manager will contact the potential client the following week.

A few of the key suggestions by Levinson, which are used in the letter:

- Keep the letter to one page.
- Use short paragraphs, under six lines each.
- Indention of paragraphs.
- A "P.S" which contains an attractive benefit, inspiring a sense of urgency.

Once a client has signed up for an audit, we promptly write a thank you letter to the referring business (In this case "Ima Referrer"), If there are no rules or regulations prohibiting it, we also send a promotional item, such as a logo pen, coffee mug, shirt, or embroidered attaché case. This is another tactic cleaned from Levinson's *Guerilla* series of books.[6]

[2] Network Magazine
[3] Harrison
[4] Economy
[5] Levinson, Jay Conrad
[6] Levinson, Jay Conrad, et al.

Part III: Project Performance

Customer Project Information

Project Overview

This project provides a detail view of the use of your network. This will highlight security deficiencies, system vulnerabilities and compromised systems. You will receive an entrance interview, a written report, and a review seminar. We ask that management be available to our consultant on the first day of the process for ensuring the best results of the analysis. The technician will install and configure the monitoring equipment. We require that a system administrator be available to work with our technician for the first two days for at least 8 hours each day for setting up equipment, and the tenth day for approximately 4 hours for recovering the monitoring equipment. This will ensure the proper placement of the equipment, and allow for determining your current security architecture. The results seminar will take place with the project team on or after the 20th day of the start of the project, and no later than the 30th day of the project. The actual meeting time will be arranged at a time convenient to you, within standard business hours (Monday - Friday, 7AM – 5PM). We require a date to be set by the 10th day of the project.

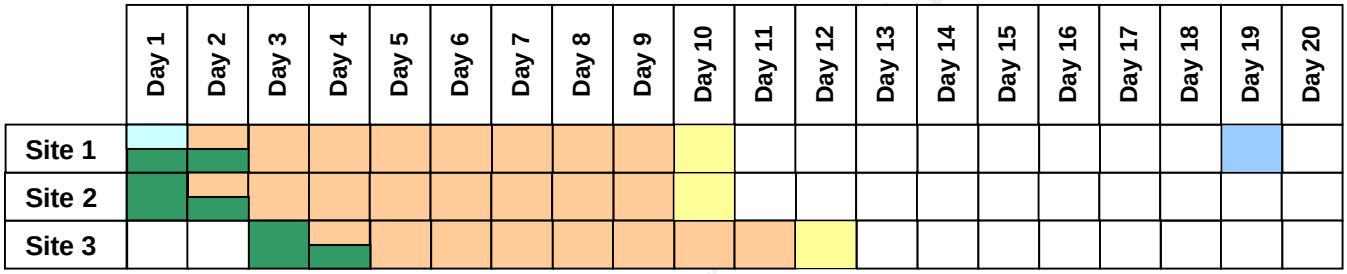
Any services recommended by GCSC Consulting staff before, during, or after the review, including services recommended during the review seminar, are additional services beyond the scope of the review, and are not covered under this project.

Project Goals

- Detect inadequate or improper configuration of perimeter devices, and network assets.
- Eliminate highly lethal vulnerabilities without delay.
- Notify management of high risk vulnerabilities as soon as possible.
- Highlight vulnerabilities which pose a danger to the business, and provide the information necessary to act through detailed deliverables.
- Recommend actions to enhance security through the deliverables.
- Build trust, show our expertise, and continue providing quality services.

Project Schedule

	Consultant arrives to begin the monitoring process and interview staff.
	Technician installs monitoring equipment and monitors proper functioning.
	Traffic monitoring period. Consultant analyzes and correlates data from the labs.
	Technician returns to recover equipment.
	Results review seminar. ** Or appropriate day before Day 30.*



Total On-Site Hours: 54

Day One
Time: 10 Hours
Staff: 2 Employees
Site: 1 & 2

Requirements for completion:

- **Personnel:** At a minimum, the Office Manager, and the IT Manager must be available for interview by the consultant. The most productive interviews have at least two to three other department managers or company executives available. Each interviewee should be available for a one hour block of time. The System Administrator must be available to the technician for the entire day.
- **Facilities:** Access to any areas which contain networking equipment is required to place monitoring equipment.
- **Equipment:** None. All equipment is provided.

What happens: The consultant and technician arrive with the network monitoring equipment. With the assistance of the site's system administrator, the technician installs the monitoring equipment on the network. The technician also gathers information from the site administrator on the placement of equipment at the remote site (Site 3), and installs equipment at the local project office (Site 2). The consultant conducts interviews with the executives and staff. Before turning the equipment on, a

quick scan of the network with nmap and Nessus in "safe" mode occurs. After this is complete, the other equipment is turned on, and monitoring begins. The consultant departs the site.

Day Two

Time: 8 Hours
Staff: 1 Employee
Site: 1 & 2

Requirements for completion:

- **Personnel:** The System Administrator should be available to the technician the entire day.
- **Facilities:** Access is required to any areas where monitoring equipment was installed to verify proper operation.
- **Equipment:** None.

What happens: The data up until the current time is transmitted to the "home" consultant for analysis. This traffic is immediately assessed to determine proper capturing of data, and to look for immediate anomalies that may require altering the location or configuration of the sensors, and at times, more sensors are added. We attempt to quickly hone in on any obviously high risk vulnerabilities, and the administrator is alerted. Sensors are double checked. The technician departs the client site at the end of this phase.

Day Three

Time: 8 Hours
Staff: 1 Employee
Site: 3

Requirements for completion:

- **Personnel:** The site Project Manager should be available to the technician the entire day.
- **Facilities:** Access to any areas which contain networking equipment is required to place monitoring equipment.
- **Equipment:** None.

What happens: The technician travels to the remote site. The technician meets with the site project manager, and installed the sensors in the appropriate places. Before turning the equipment on, a quick scan of the network with nmap and Nessus in "safe" mode occurs. After this is complete, the other equipment is turned on, and monitoring begins. The technician departs the site.

Day Four

Time: 8 Hours
Staff: 1 Employee
Site: 3

Requirements for completion:

- **Personnel:** The site Project Manager should be available to the technician the entire day. If the System Administrator can be on site this day, it would facilitate problem solving, otherwise the technician will depart as soon as data capture is verified.
- **Facilities:** Access is required to any areas where monitoring equipment was installed to verify proper operation.
- **Equipment:** None.

What happens: The data up until the current time is transmitted to the "home" consultant for analysis. This traffic is immediately assessed to determine proper capturing of data, and to look for immediate anomalies that may require altering the location or configuration of the sensors, and at times, more sensors are added. We attempt to quickly hone in on any obviously high risk vulnerabilities, and the administrator is alerted. Sensors are double checked. The technician departs the client site at the end of this phase.

Day Ten

Time: 6 Hours
Staff: 1 Employee
Site: 1 & 2

Requirements for completion:

- **Personnel:** The System Administrator should be available to the technician for a 6 hour period.
- **Facilities:** Access is required to any areas where monitoring equipment was installed to recover equipment.
- **Equipment:** None.

What happens: The technician returns and gathers all the sensors and Site 1 & 2, and returns the network to original configuration. Data is taken back to the lab for a "full picture" analysis.

Day Twelve

Time: 4 Hours
Staff: 1 Employee
Site: 3

Requirements for completion:

- **Personnel:** The site Project Manager should be available to the technician for a 4 hour period.
- **Facilities:** Access is required to any areas where monitoring equipment was installed to recover equipment.
- **Equipment:** None.

What Happens: The technician returns and gathers all the sensors, and returns the network to original configuration. Data is taken back to the lab for a "full picture" analysis.

Day Nineteen

Time: 10 Hours
Staff: 2 Employees
Site: 1

Requirements for completion:

- **Personnel:** At a minimum, we request that all interviewed parties, and the System Administrator be present ("The Panel"). Questioning of the team should only be presented through the panel, although you are welcome to invite any staff you feel should attend.
- **Facilities and Equipment:** A meeting room with proper air conditioning, room and seating for attendees, a clear wall, or projection screen for viewing, and a large table suitable for the panel.

What Happens: The consultant and technician return on day nineteen (or a day convenient to the customer after this day, but before the 30th day.), to present the findings, answer questions related to the findings, suggest a plan of action, and discuss the implementation of those plans.

<< END OF CUSTOMER PORTION OF PROJECT DOCUMENTATION >>

Internal Project Information

Project Budget

Project Price	$ 18000.00	
Travel		
Consultant		
Mileage to/from Site 1 (25 Miles @ 0.375)		$ 09.38
Technician		
Mileage to/from Site 1 (25 Miles @ 0.375)		$ 09.38
Mileage to/from Site 2 (33 Miles @ 0.375)		$ 12.38
Mileage to/from Site 3 (300 Miles @ 0.375)		$ 112.50
Lodging		
Technician		
1 Night at Site 3 (Corporate Rate)		$ 87.00
Meals and Incidentals		
Technician		
$60.00 / 2 Days		$ 60.00
Compensation		
Consultant		
18% of Gross		$ 3240.00
Technician		
08% of Gross		$ 1440.00
Project Gross Income:	$ 18000.00*	
Project Expenses:		$ 4970.64
Project Net Income:		$ 13029.36*

*** Minus up to $1,800 depending on the discount options exercised.**

The consultant earns %18 of the total contract amount from each audit, while the technician earns 8% of the total amount. (In projects requiring extensive travel, we offer a generous bonus for the technicians.)

Project Responsibilities

Client responsibility was clearly defined in the project details under each "Requirements for completion" section.

Vendor responsibility is to provide all equipment, set up and remove the equipment, prepare a deliverable report, and conduct a review seminar.

Equipment Provided:
Network traffic monitoring computer (8 Units)
Test access ports (TAP) (8 Units)
Required wires, cables and software
Presentation laptop, screen and projector

Materials Provided:
Written report of findings
CD-ROM of the report and presentation

Labor Provided:
Equipment setup (Configuring software, attaching wires, cables and power, etc.)
Equipment removal (Shutting down software, removing wires, cables and power, etc.)
Staff interviews by consultant
Traffic analysis by consultant
Multimedia presentation by the team (including setting up of equipment)

Project Facilitation (Interviews)

Interview Script

This interview was outlined using the textbook titled, "Contemporary Business Communications."[7]

Greeting and (Re)Introduction

> Good Morning, <NAME>, I am Joe Consultant, with GCSC Consulting. Thank you for taking time to speak with me.

[7] Ober

Explain Purpose, Use of Information, and Time Required

I would like to discuss a few items regarding the security of your organization. Our discussion will contribute to a more successful conclusion to this review, and allow me to address specific concerns that you, your colleagues, or the company as a whole may have. I have asked for an hour of your time, but it is possible we will not use all of it. I understand you have other issues to tend to, but please know that I am here for the day. I am not in a hurry, and there is no need to rush answers on my part.

Include Appropriate Section of Relevant Questions Here

See Below.

Summarize Points

Summarize the points discussed during the interview.

All interviews are concluded with the question:
Is there anything that we did not discuss that you feel I should know, or is a concern to you with regard to your security?

Conclude Interview

Thank you so much for your time, <NAME>. Here is my business card in the event you wish to follow up on any topic we discussed today. I look forward to seeing you at the review seminar soon.

Interview Questions

Company Officer

The Company Officer questions are designed to develop an understanding of what factors are influencing the company's decision to become secure, the concern of the officer for security within the company, the perceived "crown jewels" of the company, and the level of control and authority that is placed with the System Administrator.

The follow up questions on #5 can tread on thin ice, and would be reserved for a very limited audience, such as chief officers. If it perceived that the interviewee is becoming defensive or uncomfortable, this question will be "defused" with a comment, such as:

"It is widely known that a primary goal of an intruder during an attack is to obtain the highest level privilege possible. This level of privilege often exists with the system administrator accounts…."

These questions are intended to leave the officer thinking about the importance of separation of duties, and the possibility that one person could have the power to being a multi-million dollar company to the ground. Again, this is a company that is small, yet planning to double or triple in size. It will add millions of dollars of revenue to its budget in the near future.

1. Before you learned of GCSC Consulting, when was the last time security was discussed in a meeting?
   Follow-up:
   - Who brought the topic up?
   - Why?

2. Why do you feel you need to be secure?
3. If I could only do one thing for the company, what would you want that to be?
4. Visualize someone attacking your network, and having the capability to view anything here. What is the single most important thing you would you not want to be seen?
   Follow-up:
   - Are there any other items which are important?

5. If your System Administrator quit tomorrow, would you know where [most important thing] is stored?
   Follow-up:
   - Would someone with system administrator access be solely capable of destroying all of [most important thing]?
   - Is the System Administrator the only person with this capability?

IT Manager (Ask Company Officer questions as well)

This group of questions is intended to determine the progress of the company's IT security program. We want to know where policy and procedure exists for controlling the technology of the company. We want to know if users are trained in basic skills, such as social engineering, changing passwords, and handling viruses. We also establish if someone is watching for vulnerabilities, and if virus software has been deployed. The last item is to find out what has been done to try to secure the company.

These questions provide an overall view of where the security program is, and where it is going. This helps us tailor the deliverable, based on policy that is in place and measures that have been taken to date. For instance, if there is no system security plan, we could bring a basic template to the seminar, and address a few important policies that should be implemented based on the review. We could even offer to develop a plan for the company.

6. Do you have a security plan?
    Follow-up:
    - If so, how often is it updated?
    - Can I have a copy?
7. Do you have a user awareness training program?
8. Who keeps up with the current vulnerabilities?
9. How many computers run virus software?
    Follow-up:
    - How often does it update?
10. What steps has your organization taken to become secure to date?

System Administrator

When interviewing the System Administrator, the concentration is on determining the workload, the amount of resources that are provided to the administrator, and the emphasis that is placed on security by the administrator.

If an administrator is overworked, and has a low priority with regard to security, a deliverable which contains multiple tasks for implementing security will most likely gather dust, and we will most likely never return. In this situation, if the administrator generally receives the resources he needs, we would be better off providing this information, along with proposals for what it would cost to allow us to fix the problems within a short time frame.

11. Do you ever feel pressured to sacrifice security in favor of additional functionality of the network or systems?
    Follow-up:
    - How?
12. How much does you opinion weigh in influencing those decisions?
13. Do you have the tools you need to do your job?
    Follow-up:
    - If not, why?
    - What do you need?
14. What is your most critical computer system in the organization?
    Follow-up:
    - Why?
15. On a scale of 1 to 10, with 10 being the most important, what rating do you give security in a typical day?
    Follow-up:
    - Why?

Potential Pitfalls

No problems are found.
While this should be a good thing, it can be bad. The lack of activity could signify to the management that they were fooled or mislead, and/or we are incapable of finding such activity. If we are in a situation where a client's network is well protected, we will demonstrate the effectiveness of the security by showing failed attempts to exploit areas which are protected. We will also take a look at areas where security can be improved, independent of attempted intrusions.

If we have little or no information which is productive to verify or enhance the security of the company, we will offer to conduct another monitoring session, possibly on a three or four week interval. This would only require the technician to place and gather the equipment, and very little labor will have been invested in analyzing the data at this point, so the loss on the project would be acceptable.

Monitoring equipment failure.
This would most likely require extending the monitoring phase, and delay the project by a few days, unless the sensor failed early on in the process. The risk is relatively low, since our technicians completely refurbish equipment after each project, and high quality components are used.

Network equipment failure.
This situation would be out of our control; however, for the customer, we would either restart or extend the monitoring phase. In situations requiring travel, we would allow one free restart due to failure on the customer's part, additional trips would be charged under the standard hourly rate.

Proper personnel are not available.
Warning Signs:

- Key personnel are on leave, or take leave.
- Lack of concern and information regarding whereabouts of personnel.

If the required personnel are not available for the setup of the equipment, this could be disastrous. Since we require the presence of certain personnel, it would be a breach of contract if we had consistent personnel problems. If there are reasonable factors which have caused the situation (such as mission impacting system failures), we will work with the client to re-arrange scheduling. If the reasons are more obstructive in nature, or are due to lack of priority:

We will request a meeting with the Company Officer, IT manager, the administrator and the team to deal with the issues that may be delaying the completion of the project.

The last resort would be termination of the contract due to breach of the service agreement contract requiring the presence of certain personnel.

Difficulty with system administrator participation.
Warning Signs:

- Often unavailable, or is "too covered up."
- Appears agitated at the presence of the team.
- Questions access to network equipment.

This is another potentially disastrous situation. One of the goals of placing the technician with the system administrator consistently for a two day period is to build a rapport and relationship with this key employee. We expect the nature of a system administrator to be one of skepticism and suspicion when anyone is working with "their" equipment. This is a good thing in our eyes. We allow a few hours on the first day for the technician to spend discussing the equipment and process in great detail, and to build the initial rapport.

If necessary, we will request a meeting with the IT manager, the administrator and the team to deal with the issues that may be delaying the completion of the project.

The last resort would be termination of the contract due to breach of the service agreement contract requiring the presence of certain personnel.

Illegal activity of an employee discovered.
While as security "auditors" we actively look for unscrupulous activity, due to the very small size of the typical clientele, uncovering an employee engaged in illegal activity poses many difficult issues. One must consider the position of the offender, the validity of the data gathered, and the possibility of becoming a witness to trial. Any information of this nature is marked confidential, and is reported to the IT Manager, and if involving IT personnel, it is reported to the Company Officer.

Adding Value

As noted at the beginning of this paper, many of the contractors of this class fear the state of security of their systems, but take no action. The service to analyze network traffic for intrusions is really a "foot in the door" approach to educating customers on the importance of security, showing them we truly care, and that we KNOW what we are doing. Once a relationship is built, we have the opportunity to conduct training, perform security auditing, risk assessments, security plan development, and installation and configuration of security related devices, such as firewalls, intrusion detection systems, etc. A bonus is the contractor who also provides IT services directly to the government. We have the potential to be pulled in as sub-contractors to provide security consulting to the contracting agency.

We NEVER leave a customer with a configuration such that they are at a high risk of attack. If a dangerous condition is found, such as rules allowing all traffic in and out of a firewall because they don't want to "break" anything, we work with the customer to make corrections immediately. If we see virus/worm infected systems on the network, typically we will provide them with the patches and directions necessary to repair the system. If the level of infection is only one or two computers, and handling the infection does not mean rebuilding the computer, we will handle the cleanup on the spot.

On day two and four of the project, the technician is verifying the monitoring equipment, data and transmitting the previous day's information to the consultant. For this work, there is an entire day scheduled. While this process should take only an hour or two, if there are problems with equipment or the data, this could eat into a day very quickly. For the most part, this process goes smoothly (within an hour), leaving the technician and administrator dedicated to each other for the entire day. This allows the technician to work side by side with the administrator to fix problems that are detected – on the spot, without delay. The technician can help adjust perimeter device configurations, clean infected computers, verify fixes and updates. The technician can also share security related tips and tricks with the administrator. We are well aware that fixing these problems up front costs business, but we have scheduled an entire day, so it is within a time frame which was compensated to begin with, and the relationship building by working as a team is priceless for client longevity.

The review seminar is also a primary means to over-deliver. Many organizations refer to this as the "exit interview," or a similar cold phrase. We use the term "seminar" to specifically convey the connotation that this will be a learning experience and a situation where discussion is encouraged. The goal is to create brainstorming sessions where the customer actively participates in developing ideas for solving their problems. From

these ideas, we can shape them into the security solutions that are needed by the customer, and propose these solutions for future projects. In this situation, the customer invests their own intellectual capital in their security and is more likely to follow through on implementing and maintaining the solutions.

References

Economy, Peter, "Fishing for Referrals," *1099 The Magazine For Independent Professionals Web Page*, <http://www.1099.com/c/co/dw/pe/economy003.html> (17 April 2004)

Harrison, Walter T., and Horngren, Charles T., *Financial Accounting*, Fifth Edition, Prentice Hall, New Jersey, 2004 (Page 11)

Levinson, Jay Conrad, *Guerilla Marketing*, Houghton Mifflin Company, New York, 1998 (Page 108)

Levinson, Jay Conrad, et al., *Guerilla Publicity*, Adams Media Corporation, Avon, Massachusetts, 2002 (Pages 142-143)

Network Magazine, "A top-down approach for Security," *Network Magazine Website,* June 2003, <http://www.networkmagazineindia.com/200306/is15.shtml> (16 April 2004)

Ober, Scot, *Contemporary Business Communications*, Fourth Edition, Houghton Mifflin Company, New York, 2001 (Pages 379-381)

Washington Technology, "Washington Technology's 2003 Fast 50 Government Contractors," *Washington Technology Website*, <http://www.washingtontechnology.com/smallbusiness/fast50/2003/> (17 April 2004)

Part IV: Final Deliverable

Executive Summary

Managing security for any company is a challenge on many levels. From talking with you and your staff, it is clear that security is not the only challenge facing you. The growth your company is experiencing is rapid. Your staff is desperately working to support the current growth, and the expansion you will experience in the near future. It is important that security of your systems does not get forgotten in the process.

Security is a balance of three key areas: Confidentiality, Integrity and Availability. For you, all three are of paramount importance. Since you handle information which is considered non-public, confidentiality is imperative. The integrity of your information is essential to serving your customer, and providing accurate development. The dependence upon computers for daily administration and operations is unquestionable, so availability also rates high as well. You customer also depends on the availability of your databases on a 24/7 schedule. You may not realized that you depend on your networks and systems on mission critical level, that is, the loss of computing resources would cause major financial loss, and would cut off your primary service to your company. It is for this reason that security must be on the forefront of your growth.

Worm infection appears widespread, and is the highest priority for a response. With the vast amount of security flaws being found in the Windows operating system, it is essential to stay on top of updates. Virus management software does not seem to be commonly installed, or if it is, it is not updated regularly enough. The problem is that bulletins are disseminated so rapidly, that a response is often warranted within a 24-48 hour period in order to offer protection. Gaining control of patching and virus monitoring is essential in preventing disruption of your network, and ultimately your business. The worm traffic will affect you in some of the following ways:

- Decreased productivity, due to consumed resources
- Increased cost, due to bandwidth consumption
- Increased cost, due to labor to repair infections
- Negative public relations, due to the non-availability of, or security incidents on your network.

The time to have an enterprise wide anti-virus management program, and patch management program is now! An internal push from you, the management, to make your employees more aware of security would also be an excellent tool. We would recommend providing our IT security awareness training solution to current employees,

and implement a policy of training all new employees as a part of orientation. Employees are a crucial link to keeping the business secure. No matter how much technical security you have, social engineering is working against you. Make an effort to educate everyone, and have virus protection. Many virus solutions have centralized management panels which allow the control of scanning, reporting and updating from a central location. We would be happy to work with you on this project.

You will find more analysis and defensive recommendations as you proceed through the audit. Keep in mind that this audit is based on logs which show "bad" things, so often times, as managers, you and your IT staff will feel beat up for everything that is wrong, while receiving no credit for what is right. To the contrary, we found your IT staff to be very helpful, knowledgeable, and concerned for your systems. We often encounter apprehensive staff, resistant to change. Your IT staff, particularly, your System Administrator, regularly asked questions of our team, and we look forward to working with all of them in the future. We hope that the time we spent helping to correct some of the high risk vulnerabilities helped your staff be more productive through this audit process, and gave you a head start on fortifying your defenses against the possibility of intrusion.

The traffic from the network was run through an intrusion detection system in our lab, and compared against a standard set of rules to build an alert list. We also analyzed traffic which is considered "Out of Spec.," that is, it does not fall within generally accepted rules for TCP/IP traffic. This provides an overall means for assessing the traffic on the network, and targeting problem areas.

With that – we begin with our methodology, followed by the findings.

Audit Methodology

GCSC Consulting uses analysis methods taught by the SANS Institute, an industry pioneer in computer security. Analysts worldwide use these methods for detecting, assessing, reporting and responding to threats and vulnerabilities. Information gathered at your site is run through an intrusion detection system in our computer lab. In essence we "replay" your network traffic on a special network. This often generates thousands of alerts and logs, which are deciphered by the analyst.

We create three categories of information:

- Port and Network Scan Information
- Out of Specification Traffic
- Intrusion Detection System Alerts

Port and network scan information is analyzed to find the top ten internal and the top ten external scanners. This information is used to get a picture of who is looking at your network, and any internal problems that may be present on your network.

Out of specification traffic does not comply with established standards for network traffic. This type of traffic can highlight software, such as file sharing software, and it can highlight malicious traffic attempting to bypass your security. This provides a picture of services on your network that may be a target for exploitation.

Intrusion detection system alerts provide information on events occurring on your network. The analyst develops an overall picture of the alerts, then similar groups of alerts are created. At this point the groups are analyzed in detail.

The analyst applies a standard analytical process to the alerts, consisting of three steps:

- Step 1: Analysis
- Step 2: Correlation
- Step 3: Defense

The analyst first analyzes the alerts. During this process, the analyst determines whether the alert, or group of alerts, is a false positive. In other words, the analyst looks to see whether the alert displayed is actually what happened. The analysts also assesses: The probability that the source of the alert could have been forged, the mechanism of attack, evidence on whether you are the true target, and the severity of the alert as it applies to your systems.

During correlation, the analyst compares the alerts to multiple databases of common vulnerabilities and exposures. This gives us insight to further correlate the findings and confirm suspicions, and to prove that the attack is correctly identified. It also provides a basis for formulating a response. We also use software to visualize network traffic.

The response is handled in the defense step. The analyst develops a prescription for handling the problem at hand. We track vulnerability information from various security alert notification services, and major vendors of hardware and software. This information is used to provide the answers on where to go, what to get, and what to do.

Our method provides a stable, organized approach to assessing the security of a wide range of networks, and allows us to consistently communicate the results of our audits.

1. Scanning Traffic

Top Ten External Talkers in Terms of Scanning		
163.22.61.130	[TANET Taiwan Academic Network]	45745
138.89.191.87	pool-138-89-191-87.nwrk.east.verizon.net	37488
130.191.162.114	[San Diego State University]	31025
213.37.78.189	[MADRITEL (ISP) - Madrid, Spain]	30900
68.77.156.170	adsl-68-77-156-170.dsl.emhril.ameritech.net	29996
211.250.169.55	[Baeseok Elementary School - Seoul, Korea]	29450
66.139.49.49	adsl-66-139-49-49.grind-gear.com	28418
156.26.121.70	[Wichita State University]	28355
200.95.109.108	dsl-200-95-109-108.prod-infinitum.com.mx	28150
67.121.104.220	adsl-67-121-104-220.dsl.irvnca.pacbell.net	27317

Taken from the "scans" files. Scanned the MY.NET network.

Top Ten Internal Talkers in Terms of Scanning		
MY.NET.1.3	mynet3.GIACEnterprises.com	3457541
MY.NET.84.164	engr-84-164.pooled.GIACEnterprises.com	3032437
MY.NET.84.194	engr-84-194.pooled.GIACEnterprises.com	2198571
MY.NET.162.92	oneill-1.GIACEnterprises.com	2179667
MY.NET.111.72	cuereims.GIACEnterprises.com	2168993
MY.NET.1.4	MYNET4.GIACEnterprises.com	1016937
MY.NET.163.107	physics105pc-01.GIACEnterprises.com	813077
MY.NET.153.222	libstkpc93.lib.GIACEnterprises.com	544726
MY.NET.80.149	pplant-80-149.pooled.GIACEnterprises.com	461304
MY.NET.110.72	eds-lin1.engr.GIACEnterprises.com	414881

Taken from the "scans" files. Sources of scans within the MY.NET network.

Looking first to the internal scanners, this is probably the highest threat to the enterprise network as a whole. External scanners will be evaluated through the alert analysis section of the audit. Internal scanners can indicate compromised resources which need to be brought under control inside the business. Inappropriate traffic originating from inside the business could lead to bad publicity, additional cost due to bandwidth use, and degradation of service to the most important part of the network: the service to your customer. The internal section is also urgent due to the overwhelming traffic noted in the tables as compared to external scanners.

The number one “blowtorch” in terms of emissions, the mynet3.GIACEnterprises.com host was constantly scanning from port 41446 to a wide array of external IP addresses on port 53. This system was compromised, and was scanning for systems with vulnerable BIND DNS servers through port 53 UDP. The continual scanning, which did not pause through the whole evaluation period was suspicious and caused me to lean toward less benign explanations. Scanning looks like the log excerpt below:

01/05-12:27:43.000000 MY.NET.1.3:41446 -> 216.109.116.17:53 UDP
01/05-12:27:43.000000 MY.NET.1.3:41446 -> 62.242.234.100:53 UDP
01/05-12:27:43.000000 MY.NET.1.3:41446 -> 64.158.176.221:53 UDP
01/05-12:27:43.000000 MY.NET.1.3:41446 -> 64.233.207.2:53 UDP
01/05-12:27:44.000000 MY.NET.1.3:41446 -> 139.223.200.199:53 UDP
01/05-12:27:44.000000 MY.NET.1.3:41446 -> 208.201.249.238:53 UDP
01/05-12:27:44.000000 MY.NET.1.3:41446 -> 211.144.32.7:53 UDP
01/05-12:27:44.000000 MY.NET.1.3:41446 -> 61.172.201.254:53 UDP

Could this be someone checking up on the server?
01/06-08:57:57.498636 [**] NMAP TCP ping! [**] 65.207.54.194:80 -> MY.NET.1.3:41446
01/09-15:33:55.394539 [**] NMAP TCP ping! [**] 65.207.54.194:80 -> MY.NET.1.3:41446

The next system in line was also compromised and under the control of someone.
01/05-21:44:02.000000 MY.NET.84.164:1304 -> 68.43.213.7:1331 UDP
01/05-21:44:03.000000 MY.NET.84.164:1304 -> 134.139.107.90:3219 UDP
01/05-21:44:03.000000 MY.NET.84.164:1304 -> 158.121.124.30:2814 UDP
01/05-21:44:03.000000 MY.NET.84.164:1304 -> 211.107.25.120:2510 UDP
01/05-21:44:03.000000 MY.NET.84.164:1304 -> 24.131.169.229:2518 UDP

Action Taken!

We considered the MY.NET.1.3 and MY.NET.84.164 systems compromised. MY.NET.1.3 was actively searching for DNS servers to exploit. These systems were removed from the network, and rebuilt by the administrator.

See the “domain” service section at the CERT Scanning Activity page for a list of vulnerabilities which are driving the active scanning.
http://www.cert.org/current/scanning.html

The next three systems in line, which are not far behind, and exhibit similar levels of scanning, appear to be compromised as well. Outbound port 135 scans could be a sign of a new phenomena using the RPC facility of Microsoft Windows to distribute spam, which causes the message to pop up in a window on the user’s computer.

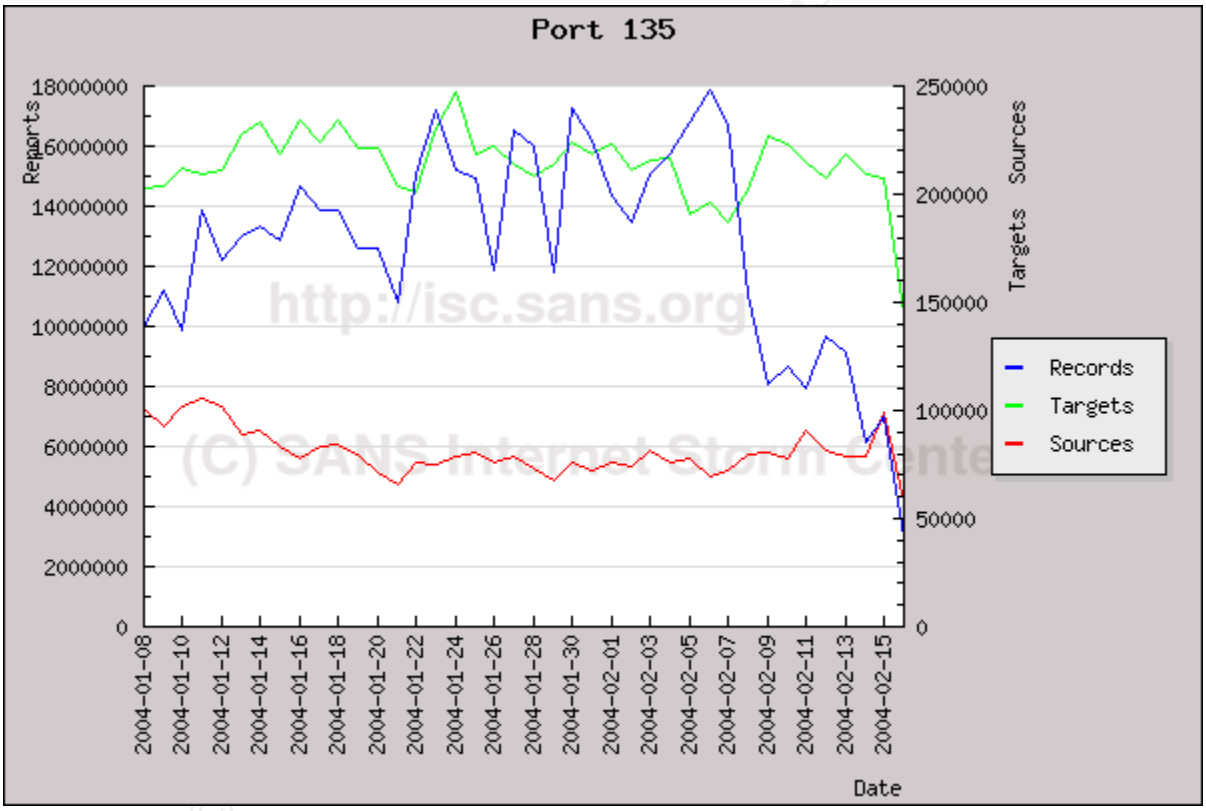
Since the IP subnet seems to be random between the two hosts, the IP addresses increment by one value, and scanning is constant through the logs, we suspected this was the Blaster worm (or a variant).

01/05-15:11:07.000000 MY.NET.84.194:2259 -> 132.186.170.141:135 SYN ******S*
01/05-15:11:07.000000 MY.NET.84.194:2260 -> 132.186.170.142:135 SYN ******S*
01/05-15:11:12.000000 MY.NET.84.194:2301 -> 132.186.170.183:135 SYN ******S*

01/05-15:11:12.000000 MY.NET.84.194:2302 -> 132.186.170.184:135 SYN ******S*
01/05-15:11:12.000000 MY.NET.84.194:2303 -> 132.186.170.185:135 SYN ******S*

01/05-11:40:31.000000 MY.NET.162.92:3177 -> 176.75.60.31:135 SYN ******S*
01/05-11:40:31.000000 MY.NET.162.92:3178 -> 176.75.60.32:135 SYN ******S*
01/05-11:40:31.000000 MY.NET.162.92:3179 -> 176.75.60.33:135 SYN ******S*
01/05-11:40:31.000000 MY.NET.162.92:3180 -> 176.75.60.34:135 SYN ******S*
01/05-11:40:31.000000 MY.NET.162.92:3181 -> 176.75.60.35:135 SYN ******S*

01/05-21:55:31.000000 MY.NET.111.72:1129 -> 77.55.30.182:135 SYN ******S*
01/05-21:55:31.000000 MY.NET.111.72:1130 -> 77.55.30.183:135 SYN ******S*
01/05-21:55:31.000000 MY.NET.111.72:1131 -> 77.55.30.184:135 SYN ******S*
01/05-21:55:31.000000 MY.NET.111.72:1132 -> 77.55.30.185:135 SYN ******S*
01/05-21:55:31.000000 MY.NET.111.72:1133 -> 77.55.30.186:135 SYN ******S*



As shown in the graph above from the SANS Internet Storm Center, scanning on the internet for port 135 is at an extreme level, both around the evaluation period of the logs, and continues to be steady. On the day this graph was taken (2/16), this port ranked #5 overall. If you combine just the three infections noted above, you have by far the biggest threat to the network out of any threat that we logged.

Action Taken!

We immediately disconnected these machines from the network, and ran a virus removal tool called "Stinger" from McAffee: http://us.mcafee.com/virusInfo/?id=stinger

We applied the RPC patch from Microsoft: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp

Systems were returned to normal network use within minutes, and verified as clean. We also ran the Windows Update to download the critical updates.

We suggested an excellent document for your IT staff to use to build new computers to be used on the network, the ISC Analysis "how-to": "Windows XP: Surviving the first day." at: http://www.sans.org/rr/papers/index.php?id=1298

For information on the Blaster type worms, see the Sophos information at: http://www.sophos.com/virusinfo/analyses/w32blastera.html

Also see: CERT Advisory CA-2003-20 W32/Blaster worm http://www.cert.org/advisories/CA-2003-20.html

For more information on the RPC facility use for spamming, see: "*Spam Masquerades as Admin Alerts"* by Brian McWilliams http://www.wired.com/news/technology/0,1282,55795,00.html

The RPC vulnerability is a popular exploit, a SANS Top Twenty Threat, and correcting this problem on a network level should be top priority. If this is not the Blaster worm, it would be a variant of this type of worm. In addition to the hosts above, the systems noted in this table should also be highly suspect for infection, and warrant immediate investigation. The number to the right represents the "hits" that were seen in the scan logs.

Additional Suspected RPC Worm Infections	
System	**Hits**
MY.NET.163.107	813073
MY.NET.80.149	457493
MY.NET.112.153	215007
MY.NET.80.243	194966
MY.NET.69.190	13856
MY.NET.84.203	565
MY.NET.81.109	381

The rest of the top ten in this category should be investigated for other types of worms or compromise as well, because with such a high number of scans, it's likely either someone is using the system for scanning, or it is infected with a self-propagating worm.

5. Out of Specification (OOS) Traffic

Top Ten Destination Ports for OOS Traffic		
Port	**Name**	**Hits**
110	**POP-3**	**2381**
80	**HTTP**	**946**
25	**SMTP**	**756**
4662	**P2P File Sharing**	**293**
3647	**???**	**167**
1426	**Satellite-data Acquisition System 1**	**94**
6881	**P2P (BitTorrent)**	**80**
113	**Kazimas (or auth/identd)**	**62**
1304	**Boomerang**	**48**
1214	**Kazaa/Morpheous/Grokster**	**14**

The problem with providing a table like the one above is that it paints a grave picture. High hits for a port doesn't necessarily mean that these ports are being attacked. It does suggest that they are begin targeted, which includes scanning, so attention needs to be paid to the servers which run these ports, because there is heightened interest in them. The top risk would be to mail servers. Make sure that your mail servers are patched and all software on these machines are up to date. You need to take a look at your web servers to since they provide service to your customer. From the logs we can see examples where traffic captured in these logs appear to be directly related to scanning:
(You see the scanner conducting scans against port 110, the top port noted in the logs.)

Scan Logs:

```
01/06-02:16:15.000000 68.122.128.111:17161 -> MY.NET.12.4:110 NULL ********
01/06-02:16:15.000000 68.122.128.111:17161 -> MY.NET.12.4:110 SYN ******S*
01/06-02:38:08.000000 68.122.128.111:17417 -> MY.NET.12.4:110 NULL ********
01/06-02:38:08.000000 68.122.128.111:17417 -> MY.NET.12.4:110 SYN ******S*
01/06-03:21:55.000000 68.122.128.111:17929 -> MY.NET.12.4:110 NULL ********
01/06-03:21:55.000000 68.122.128.111:17929 -> MY.NET.12.4:110 SYN ******S*
```

Correlating Alert Logs:

```
01/06-02:16:15.485895  [**] Null scan! [**] 68.122.128.111:17161 -> MY.NET.12.4:110
```

01/06-02:38:08.784198 [**] Null scan! [**] 68.122.128.111:17417 -> MY.NET.12.4:110
01/06-03:21:55.196158 [**] Null scan! [**] 68.122.128.111:17929 -> MY.NET.12.4:110

Correlating OOS Logs:

01/06-02:16:15.485898 68.122.128.111:17161 -> MY.NET.12.4:110
TCP TTL:80 TOS:0x0 ID:4660 IpLen:20 DgmLen:40
******** Seq: 0x6300001 Ack: 0x6DA6D68E Win: 0x800 TcpLen: 20
01/06-02:38:08.784203 68.122.128.111:17417 -> MY.NET.12.4:110
TCP TTL:80 TOS:0x0 ID:4660 IpLen:20 DgmLen:40
******** Seq: 0x6401001 Ack: 0xBF091330 Win: 0x800 TcpLen: 20
01/06-03:21:55.196160 68.122.128.111:17929 -> MY.NET.12.4:110
TCP TTL:80 TOS:0x0 ID:4660 IpLen:20 DgmLen:40
******** Seq: 0x65F1001 Ack: 0x66509A16 Win: 0x800 TcpLen: 20

The other nugget of information to take away from this table is that P2P file sharing is apparently present on the network. This poses a serious risk to your company. Illegally downloaded software, music and other non-business related files open your company to legal action, and they also pose a high risk of introducing trojans, with malicious software embeded that can leak information, or allow remote control of your computer systems by outsiders.

I would say that the major concentration for file sharing should be to address the computer noted in the IRC alert section (pplant-80-149.pooled.GIACEnterprises.com, MY.NET.80.149). If you haven't developed an Acceptable Use Policy for your users to sign, you should do so. Then you should start enforcing it by disciplining your employees. We have provided a sample policy on your CD-ROM.

Most interesting is the traffic to port 3647. This traffic was between two hosts: MY.NET.66.42 and 194.67.70.10, which apparently belongs to Moscow State University. Interrogation of the 194 host yields the following information:

```
inetnum:        194.67.70.0 - 194.67.70.15
netname:        SOI-NET
descr:          States Oceanographic Institut Network
country:        RU
admin-c:        IVZ5-RIPE
tech-c:         IVZ6-RIPE
status:         ASSIGNED PA
notify:         ivz@motor.ru
notify:         tihon@koptevo.net
mnt-by:         RADIO-MSU-MNT
changed:        evgen@radio-msu.net 20010705
source:         RIPE
route:          194.67.64.0/18
```

```
descr:          DELEGATED CIDR BLOCK
descr:          Provider Local Registry
descr:          Radio-MSU
origin:         AS2683
notify:         noc@radio-msu.net
mnt-by:         RADIO-MSU-MNT
changed:        evgen@radio-msu.net 19980730
source:         RIPE
```

Scan Logs:

01/06-02:41:18.000000 194.67.70.10:44190 -> MY.NET.66.42:3647 SYN 12****S* RESERVEDBITS
01/06-02:50:56.000000 194.67.70.10:52179 -> MY.NET.66.42:3647 SYN 12****S* RESERVEDBITS

OOS Logs:

01/06-02:41:18.446292 194.67.70.10:44190 -> MY.NET.66.42:3647
TCP TTL:51 TOS:0x0 ID:61676 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x89DAB501 Ack: 0x0 Win: 0x16D0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 879775260 0 NOP WS: 0
--
01/06-02:50:56.182813 194.67.70.10:52179 -> MY.NET.66.42:3647
TCP TTL:51 TOS:0x0 ID:36301 IpLen:20 DgmLen:60 DF
12****S* Seq: 0xAEBBA25A Ack: 0x0 Win: 0x16D0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 879832983 0 NOP WS: 0

It looks like this traffic was flagged due to the ECN reserved bits being on for the SYN packets. The only reference I could find related to port 3647 was a post on the Neohapsis Archives at: http://archives.neohapsis.com/archives/incidents/2000-11/0209.html In this article it describes an IRC bot called egghead. Looking at the documentation though, I see that the listening port (for telneting) is configurable, so it could be coincidence. Regardless, there is something happening between these two hosts for a long period of time, so this system should be investigated. This information was reported directly to the IT manager as soon as it was discovered, since this is regular communication with a foreign entity. (http://www.eggheads.org/support/egghtml/1.6.15/egg-core.html)

I used the following reference in evaluating oos logs:
RFC 791 - Internet Protocol
http://www.faqs.org/rfcs/rfc791.html

6. Alert Traffic

2.3.2 Detect Section Overview

Categorization and Ranking of Alerts		
#1	Internet Relay Chat	74938
#2	Anomalous Traffic	7259
#3	Network Shares	5059
#4	Service Exploits	1910
#5	Port Access	1477

Internet Relay Chat (74938 Alerts) Rank: #1

Top 5 Alert Sources

```
MY.NET.80.149
64.180.102.29
213.230.192.163
216.194.70.11
80.247.212.222
```

Overview

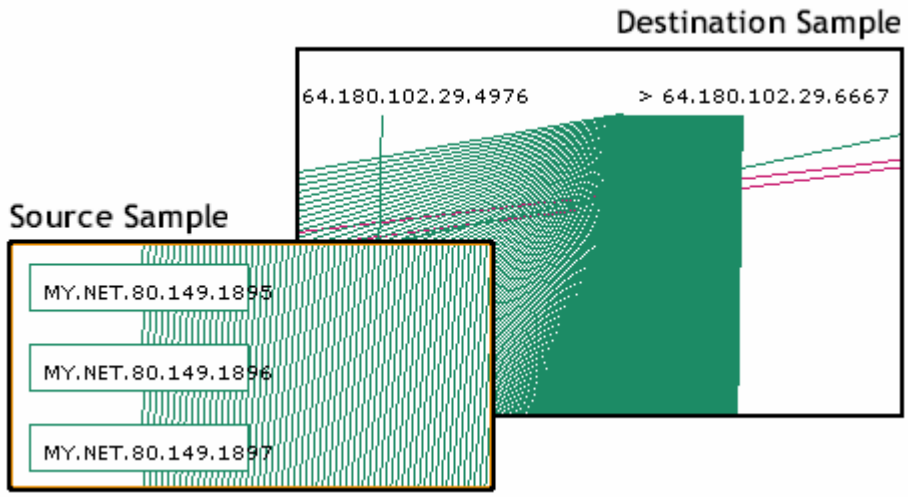
Internet Relay Chat related detects accounted for over 80% of the alerts audited. More troubling is the majority of these IRC alerts are related to XDCC, a file sharing component of IRC. While not specifically mentioned, Peer to Peer (P2P) file sharing ranks in the SANS Top 20 Internet Security Vulnerabilities. Many of the issues surrounding P2P file sharing apply to XDCC as well, since it is used to share many of the same types of files, such as music, movies, and illegal software (Warez).

Core Findings

The "XDCC client detected attempting to IRC" rule is the top alert out of the entire review. It appears as if one host is the primary culprit for the massive level of alerts.

Asset Analysis

The disproportionate amount of traffic is flowing from the MY.NET.80.149 host to the 64.180.102.29 host.



The entire viewable file of the this traffic is available on your CD-ROM.

Looking at the logs to correlate with the graph we see constant traffic which appears to last at least a day and a half – it ends near the end of the evaluation period, so it is possible this activity resumes and continued. There are also numerous /kill alerts within this run of traffic, which accounts for a number of this type of alert.

01/08-18:19:16.437083 [**] [GIACENT NIDS IRC Alert] IRC user /kill detected, possible trojan. [**] 64.180.102.29:6667 -> MY.NET.80.149:2238
01/08-18:19:17.629704 [**] [GIACENT NIDS IRC Alert] XDCC client detected attempting to IRC [**] MY.NET.80.149:2254 -> 64.180.102.29:6667
Note: For the remainder of the logs in this example, the repetitive alert text has been removed for illustrative purposes.
01/08-18:19:20.386609[**] MY.NET.80.149:2266 -> 64.180.102.29:6667
01/08-18:19:22.391109[**] MY.NET.80.149:2277 -> 64.180.102.29:6667
...SNIP...
01/09-23:31:36.152812[**] MY.NET.80.149:4222 -> 64.180.102.29:6667
01/09-23:31:42.904187 [**] [GIACENT NIDS IRC Alert] IRC user /kill detected, possible trojan. [**] 64.180.102.29:6667 -> MY.NET.80.149:4227
01/09-23:31:44.642444[**] MY.NET.80.149:4282 -> 64.180.102.29:6667
01/09-23:31:45.093081[**] MY.NET.80.149:4287 -> 64.180.102.29:6667
01/09-23:31:56.002705[**] MY.NET.80.149:4354 -> 64.180.102.29:6667
01/09-23:31:58.635090 [**] [GIACENT NIDS IRC Alert] IRC user /kill detected, possible trojan. [**] 64.180.102.29:6667 -> MY.NET.80.149:4375
01/09-23:32:00.098194[**] MY.NET.80.149:4390 -> 64.180.102.29:6667
01/09-23:32:00.580854[**] MY.NET.80.149:4395 -> 64.180.102.29:6667
01/09-23:32:03.892125[**] MY.NET.80.149:4425 -> 64.180.102.29:6667
..SNIP...
01/09-23:49:17.379628[**] MY.NET.80.149:4099 -> 64.180.102.29:6667
01/09-23:49:18.720766[**] MY.NET.80.149:4109 -> 64.180.102.29:6667

At first appearance, this may look like a scan, but keep in mind these entries are from the alert logs, and also note the apparent attempts to "kill" the user. These alerts emanate to the external host on the same external port. It is highly possible this host is compromised – if not, it exhibits behavior dangerous to the network.

Action Taken!

! This host was exhibiting very suspicious behavior, and producing an excessive amount of traffic to an IRC port. This system was removed from the network, and held by the system administrator until management discusses this with the user.

Host Interrogation

64.180.102.29

```
TELUS Communications Inc. NET-TELAC-BLK10 (NET-64-180-0-0-1)
64.180.0.0 - 64.180.255.255
New West Office-Server  ADSL HSIA163-CA (NET-64-180-100-0-1)
 64.180.100.0 - 64.180.103.255
OrgName:    TELUS Communications Inc.
OrgID:      TACE
Address:    #2600 4720 Kingsway Avenue
City:       Burnaby
StateProv:  BC
PostalCode: V5N-4N2
Country:    CA
ReferralServer: rwhois://rwhois.telus.net:4321
NetRange:   64.180.0.0 - 64.180.255.255
CIDR:       64.180.0.0/16
NetName:    NET-TELAC-BLK10
NetHandle:  NET-64-180-0-0-1
Parent:     NET-64-0-0-0-0
NetType:    Direct Allocation
NameServer: HELIUM.BC.TAC.NET
NameServer: NEON.BC.TAC.NET
Comment:    ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
RegDate:    2000-08-04
Updated:    2002-11-20
TechHandle: MO229-ARIN
TechName:   Owen, Margot
TechPhone:  +1-604-454-5107
TechEmail:  IP-admin@bc.tac.net
OrgAbuseHandle: AAT-ARIN
OrgAbuseName:   Abuse at TELUS
OrgAbusePhone:  +1-604-444-5791
```

```
OrgAbuseEmail:  abuse@telus.com
OrgTechHandle: IA86-ARIN
OrgTechName:   IP Admin
OrgTechPhone:  +1-403-503-3800
OrgTechEmail:  add-req.tac@telus.com
OrgTechHandle: PSINET-CA-ARIN
OrgTechName:   TELUS Communications Inc.
OrgTechPhone:  +1-613-780-2200
OrgTechEmail:  swip@swip.ca.telus.com
OrgTechHandle: TBOTP-ARIN
OrgTechName:   TELUS BC ORG TECH POC
OrgTechPhone:  +1-604-444-5791
OrgTechEmail:  IPadmin@telus.com
```

Further Reading

Instructions on Cleaning IRC bot & backdoor: XDCC
http://security.duke.edu/cleaning/xdcc.html

Anomalous Traffic (7259 Alerts) Rank: #2

Summary of Anomalous Traffic Related Alerts	
Incomplete Packet Fragments Discarded	5195
Tiny Fragments - Possible Hostile Activity	1029
Possible trojan server activity	728
TCP SRC and DST outside network	160
ICMP SRC and DST outside network	144
Fragmentation Overflow Attack	3
Total:	7259

Overview

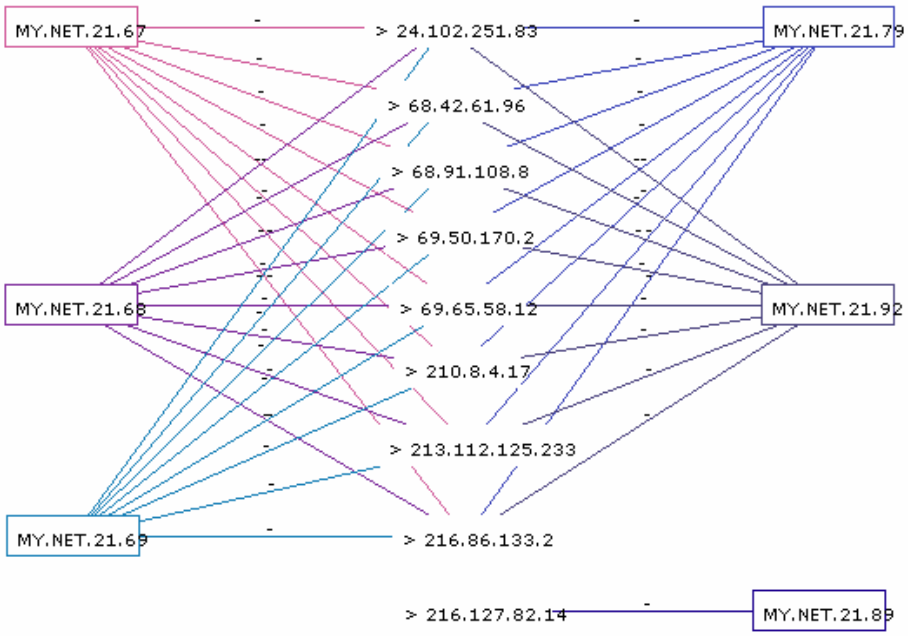
Anomalous traffic can be a bad sign. Fragmented traffic is often used to evade security measures in place on the network, so particular attention is needed to verify the intent of this type of traffic. This type of traffic can flow right through the firewall.

Top 5 Alert Sources
MY.NET.21.67
MY.NET.21.79
MY.NET.21.92
MY.NET.21.68
24.2.127.135

Core Findings & Asset Analysis

Looking to the top offenders, the trend shows that the MY.NET.21 subnet is the source of most of the traffic from the top alert of this category. This appears to emanate from

the top four IP addresses. The destinations appear to all go to random external addresses, and the interesting pattern to note is that all of the sources appear to contact the same IP at the same time.



Sample Logs

```
01/07-11:58:48.356147  [**] Incomplete Packet Fragments Discarded [**] MY.NET.21.67 -> 68.91.108.8
01/07-11:58:48.831733  [**] Incomplete Packet Fragments Discarded [**] MY.NET.21.68 -> 68.91.108.8
01/07-11:58:49.326773  [**] Incomplete Packet Fragments Discarded [**] MY.NET.21.67 -> 68.91.108.8
01/07-11:58:49.342685  [**] Incomplete Packet Fragments Discarded [**] MY.NET.21.69 -> 68.91.108.8
01/07-11:58:49.539693  [**] Incomplete Packet Fragments Discarded [**] MY.NET.21.79 -> 68.91.108.8
01/07-11:58:50.127391  [**] Incomplete Packet Fragments Discarded [**] MY.NET.21.68 -> 68.91.108.8
01/07-11:58:50.270315  [**] Incomplete Packet Fragments Discarded [**] MY.NET.21.92 -> 68.91.108.8

01/08-01:24:50.577322  [**] Incomplete Packet Fragments Discarded [**] MY.NET.21.69 -> 68.42.61.96
01/08-01:24:50.580149  [**] Incomplete Packet Fragments Discarded [**] MY.NET.21.67 -> 68.42.61.96
01/08-01:24:53.831542  [**] Incomplete Packet Fragments Discarded [**] MY.NET.21.79 -> 68.42.61.96
01/08-01:24:57.474985  [**] Incomplete Packet Fragments Discarded [**] MY.NET.21.69 -> 68.42.61.96
01/08-01:24:57.516718  [**] Incomplete Packet Fragments Discarded [**] MY.NET.21.79 -> 68.42.61.96
01/08-01:25:09.323071  [**] Incomplete Packet Fragments Discarded [**] MY.NET.21.92 -> 68.42.61.96
01/08-01:25:14.573272  [**] Incomplete Packet Fragments Discarded [**] MY.NET.21.69 -> 68.42.61.96
```

The fact that this traffic is emanating from the network, rather than coming from the outside, means that there may be a group of compromised systems which are being used for some type of coordinated attack. We could be looking at a DDOS attack using fragmented packets.

For the alerts which trigger for the source and destination outside the network, I consulted a GCIA practical from Tom King where similar traffic was evaluated as primarily due to misconfiguration in DHCP. (http://www.giac.org/practical/GCIA/Tom_King_GCIA.pdf) I would also check to make sure that these devices are authorized. It seems that some of the addresses are private, non-routable IP address, which may indicate that someone either has unauthorized connections to the network, or is running some type of LAN.

Looking at the logs I see that a majority of the IP's fall within the range of 172.128.0.0 – 172.211.0.0. Most of this range belongs to America Online. See the "Host Interrogation" section. Could this be due to dual use of dialup and network? You might keep an eye on this, because, it is plausible that someone could come through a users unprotected AOL connection into a less defended area of the network. Modems (and we will include Cable and DSL) are a notorious manner in which security is bypassed.

With the Trojan server alerts, many of these are triggered by scanning for port 27374. We see a few of the excerpts below (correlating scans to alerts. Note the times and ports:

```
01/06-09:46:37.000000 212.49.171.233:1444 -> MY.NET.190.177:27374 SYN ******S*
01/06-09:46:37.000000 212.49.171.233:1449 -> MY.NET.190.178:27374 SYN ******S*
01/06-09:46:37.000000 212.49.171.233:1453 -> MY.NET.190.179:27374 SYN ******S*
01/06-09:46:37.423087  [**] Possible trojan server activity [**] 212.49.171.233:1444 ->
MY.NET.190.177:27374
01/06-09:46:37.429501  [**] Possible trojan server activity [**] 212.49.171.233:1449 ->
MY.NET.190.178:27374
01/06-09:46:37.436607  [**] Possible trojan server activity [**] 212.49.171.233:1453 ->
MY.NET.190.179:27374
01/06-09:46:40.000000 212.49.171.233:1544 -> MY.NET.190.238:27374 SYN ******S*
01/06-09:46:40.000000 212.49.171.233:1545 -> MY.NET.190.239:27374 SYN ******S*
01/06-09:46:40.000000 212.49.171.233:1546 -> MY.NET.190.240:27374 SYN ******S*
01/06-09:46:40.488170  [**] Possible trojan server activity [**] 212.49.171.233:1544 ->
MY.NET.190.238:27374
01/06-09:46:40.493795  [**] Possible trojan server activity [**] 212.49.171.233:1545 ->
MY.NET.190.239:27374
01/06-09:46:40.500401  [**] Possible trojan server activity [**] 212.49.171.233:1546 ->
MY.NET.190.240:27374
```

The remainder of traffic for this alert appears to be between port 25, 80 and 443. It is perfectly normal to see SMTP, Web and SSL (Secure Sockets Layer) communicating with an ephemeral port such as 27374. The only problem is that this appears frequently in the logs, and raises suspicion that it is communication due to compromised systems.

It is interesting to note, according to a comment on the Internet Storm Center website, that the maker of SubSeven also added a backdoor to the attackers interface. This means that the attacker is open to attack. (http://isc.incidents.org/show_comment.html?id=464). So the danger to the network can be from compromised systems, or devious users attempting to exploit other vulnerable computers.

Action Taken!

With the System Administrator, we checked these systems for use of SubSeven:
MY.NET.34.11 MY.NET.24.34
MY.NET.24.74 MY.NET.12.6 MY.NET.12.7
All had apparently received a trojan by email. The systems were removed from the network and reimaged by the System Administrator.

Host Interrogation

Sample of "Incomplete Fragment" Targets
Name: pcp08333943pcs.tallah01.fl.comcast.net
Address: 68.42.61.96
Name: adsl-68-91-108-8.dsl.hstntx.swbell.net
Address: 68.91.108.8
Name: astro.sh3lls.net
Address: 69.50.170.2
Name: static017.mel.off.connect.com.au
Address: 210.8.4.17
Name: dns1.mswin.net
Address: 216.86.133.2

172.165.0.0

```
OrgName:    America Online
OrgID:      AOL
Address:    22000 AOL Way
City:       Dulles
StateProv:  VA
PostalCode: 20166
Country:    US

NetRange:   172.128.0.0 - 172.191.255.255
CIDR:       172.128.0.0/10
NetName:    AOL-172BLK
```

```
NetHandle:  NET-172-128-0-0-1
Parent:     NET-172-0-0-0-0
NetType:    Direct Allocation
NameServer: DAHA-01.NS.AOL.COM
NameServer: DAHA-02.NS.AOL.COM
NameServer: DAHA-07.NS.AOL.COM
Comment:    ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
RegDate:    2000-03-24
Updated:    2003-08-08

TechHandle: AOL-NOC-ARIN
TechName:   America Online, Inc.
TechPhone:  +1-703-265-4670
TechEmail:  domains@aol.net

OrgAbuseHandle: AOL382-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-703-265-4670
OrgAbuseEmail:  abuse@aol.net

OrgNOCHandle: AOL236-ARIN
OrgNOCName:   NOC
OrgNOCPhone:  +1-703-265-4670
OrgNOCEmail:  noc@aol.net

OrgTechHandle: AOL-NOC-ARIN
OrgTechName:   America Online, Inc.
OrgTechPhone:  +1-703-265-4670
OrgTechEmail:  domains@aol.net
```

Network Shares (5059 Alerts) — Rank: #3

Summary of Network Share Related Alerts	
SMB Name Wildcard	4862
SMB C access	196
NETBIOS NT NULL session	1
Total:	5059

SMB Name Wildcard

Overview

CVE ID: CAN-1999-0621

Top 5 Alert Sources
MY.NET.11.6
MY.NET.111.228
MY.NET.150.198
MY.NET.75.13
MY.NET.150.44

An offending datagram could appear similar to this capture from the SANS Institute Intrusion Detection FAQ.

```
[**] SMB Name Wildcard [**]
05/10-18:08:05.359797 badguy.com:137 -> goodguy.com:137
UDP TTL:119 TOS:0x0 ID:45361
Len: 58
00 D4 00 00 00 01 00 00 00 00 00 00 20 43 4B 41 ............ CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 00 00 21 AAAAAAAAAAAAA..!
00 01 ..
```

The “SMB Name Wildcard” alert showed up the most often for the top ten scanners on the network. This particular class of vulnerability shows up in the SANS Top List for Windows Remote Access Services. According to ArachNIDS, these types of packets are a part of the Windows operating system’s method for determining NetBIOS names when only the IP address is known. Information about the computer can be gathered through this method. This means the workstation name, domain, and users logged in, is exposed. (http://whitehats.com/info/IDS177) This information could be useful to an attacker for other exploits. A more common reason for this traffic is due to worm propagation. Unprotected network shares allow malicious software to install onto the system, and begin searching for other hosts to infect.

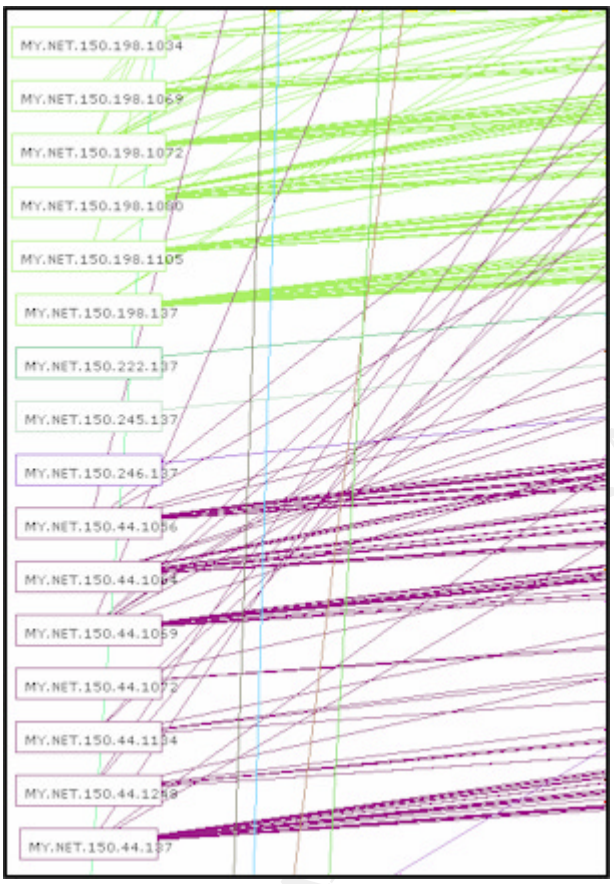
Core Findings

On a general network view, it appears that there are problems with NetBIOS traffic on the network. Activity patterns suggest infection and proliferation of one or more worms which exploit vulnerabilities in the Windows Remote Access Services.
Affected hosts will most likely be experiencing slowness, and possibly failure to respond, due to scanning, and being scanned. Once a worm is installed, the host is potentially open to further intrusion, and will actively seek other hosts to infect.

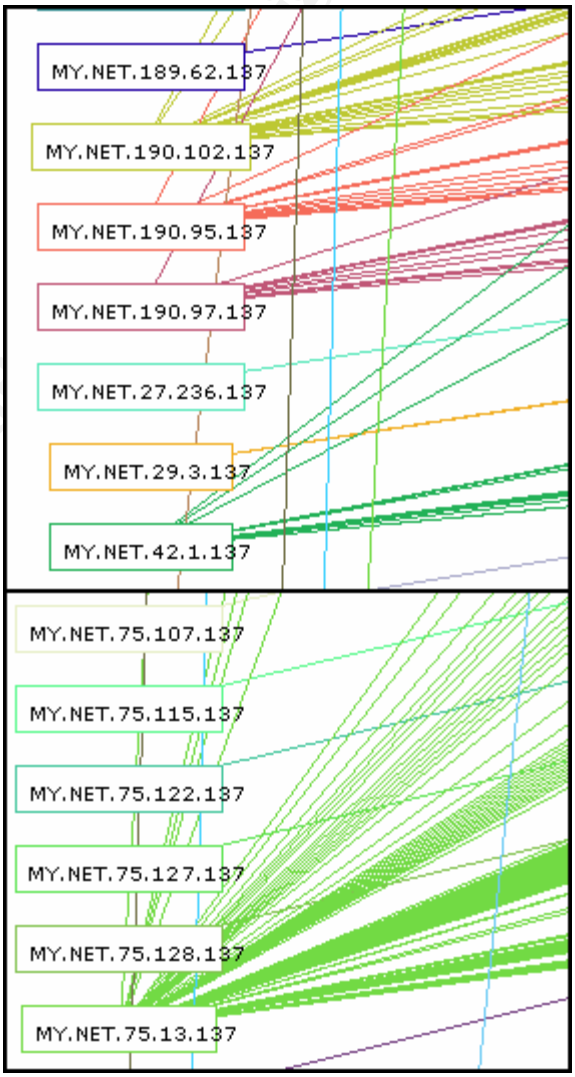
The shear level of traffic across the network due to scanning will most likely increase as new hosts are found to infect, and those hosts begin scanning (exponential growth). Increased bandwidth consumption could result in a substantial increase in cost of leased lines for WAN access. In addition, with bandwidth becoming consumed, network response will become sluggish and possibly cause denial of service on a network level.

Asset Analysis

The hosts MY.NET.150.198 (green) and MY.NET.150.44 (purple) are shown below, left in an Augur graph. Traffic is originating from these two hosts to many different external hosts on port 137. The interesting feature of the graphs is multiple ephemeral ports seem to be transmitting. According to a remark on the Internet Storm Center's website (http://isc.incidents.org/show_comment.html?id=85) traffic originating from ephemeral ports to port 137 is indicative of a worm.



The entire viewable file of the this traffic is available on your CD-ROM.



Looking through the entire graph we see a wide array of traffic outbound to and from port 137. In the second graph, above, right, we see that a remarkable amount of traffic is outbound from port 137 on the selected hosts. This traffic could be indicative of an infection by the network.vbs worm,

or a variant. This traffic is correlated in the honeypot article referenced in the correlation section, and an excerpt is below. The host is first scanned on port 137, then the connection is made on port 139.

```
04/06-20:49:14.457168 24.65.232.175:137 -> my.honey.pot.ip:137
UDP TTL:114 TOS:0x0 ID:44829
Len: 58
04/06-20:49:14.457730 my.honey.pot.ip:137 -> 24.65.232.175:137
UDP TTL:128 TOS:0x0 ID:22545
Len: 273
04/06-20:49:14.596311 24.65.232.175:1962 -> my.honey.pot.ip:139
TCP TTL:114 TOS:0x0 ID:45085  DF
S***** Seq: 0x40D4A0   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP NOP Opt 4:
04/06-20:49:14.596604 my.honey.pot.ip:139 -> 24.65.232.175:1962
TCP TTL:128 TOS:0x0 ID:22801  DF
S***A* Seq: 0x1B163955   Ack: 0x40D4A1   Win: 0x2238
TCP Options => MSS: 1460 NOP NOP Opt 4:
04/06-20:49:14.753110 24.65.232.175:1962 -> my.honey.pot.ip:139
TCP TTL:114 TOS:0x0 ID:45341  DF
****A* Seq: 0x40D4A1   Ack: 0x1B163956   Win: 0x2238
00 00 00 00 00 00                              ......
```

I do see active scanning of port 139, so it is possible that a malicious program was inserted manually by an attacker, or at the very least, someone is looking for open doors.

```
01/05-13:36:04.000000 147.29.138.158:1467 -> MY.NET.190.95:139 SYN ******S*
01/05-13:36:04.000000 147.29.138.158:1468 -> MY.NET.190.97:139 SYN ******S*
01/05-13:36:05.000000 147.29.138.158:1470 -> MY.NET.190.102:139 SYN ******S*
```

Correlation

Internet Storm Center
http://isc.incidents.org/port_details.html?port=137
http://isc.incidents.org/top10.html
Port 137 is one of the top 10 ports listed

Global Incident Analysis Center - Special Notice - Followup on a Honeypot Catch
http://www.sans.org/y2k/honeypot_catch.htm

Defensive Recommendations

Implement a block of NetBIOS ports (135 tcp/udp, 137 udp, 139 tcp) both inbound and outbound from the network. See the CERT/CC document referenced in this section for more information. Considering this class is a top twenty vulnerability, this means that this is a high profile, commonly exploited service. File sharing can be accomplished through other means, such as FTP and HTTP (as recommended in the top twenty list).

Ensure that the enterprise virus solution (assuming there is one) is actually running on systems and have up to date DAT files. There is a free virus detection and removal tool produced by Network Associates called "Stinger" which can handle most of the type of worms which produce the above traffic. This could be run by staff who do not have licenses to operate standard virus software.

The URL is: http://us.mcafee.com/virusInfo/?id=stinger

After the first priority of blocking access, and cleaning up infection, systems should be patched – which can be performed automatically through the Windows Update service. Network shares should be required to have authentication. Patched systems with unprotected shares are still open to exploitation.

Further Reading (Material Referenced in this Section)

SANS Top Twenty Internet Security Vulnerabilities
W5 Windows Remote Access Services
http://www.sans.org/top20/

SANS Intrusion Detection FAQ
Port 137 Scan
http://www.sans.org/resources/idfaq/port_137.php

The Internet Assigned Numbers Authority
RFC 3330 - Special-Use IPv4 Addresses
http://www.rfc-editor.org/rfc/rfc3330.txt

Help Defeat Denial of Service Attacks: Step-by-Step
(Filtering IP Addresses)
http://www.sans.org/dosstep/index.php

CERT Coordination Center
Vulnerability Note VU#547820
http://www.kb.cert.org/vuls/id/547820

Network Associates, Inc.
W32/Opaserv.worm
http://vil.nai.com/vil/content/v_99729.htm

Service Exploits (1910 Alerts) — Rank: #4

Summary of Service Exploit Related Alerts	
EXPLOIT x86 NOOP	1698
EXPLOIT x86 setuid 0	34
FTP DoS ftpd globbing	31
EXPLOIT x86 setgid 0	26
EXPLOIT x86 stealth noop	21
RFB - Possible WinVNC - 010708-1	17
EXPLOIT NTPDX buffer overflow	11
DDOS shaft client to handler	6
EXPLOIT x86 NOPS	1
EXPLOIT identd overflow	1
Total:	1910

Overview

Top 5 Alert Sources
131.118.254.130
129.128.5.191
213.46.80.48
61.172.255.109
65.203.33.194

This class of alert is similar to the “Anomalous Traffic” section, but the descriptors are more specific to certain exploits than the fragmentation related alerts. These could allow access to restricted areas of the system, execute code, or halt servers.

Asset Analysis

By far the most noted attack of this section is the “EXPLOIT x86 NOOP.” As described in a detect in the GCIA Practical by Chris Kuethe, this type of attack occurs when no-op instructions are used to pad a malicious command to a vulnerable application. The padding overflows the buffer and places the command in the correct location in memory for the command to be executed. (http://www.giac.org/practical/chris_kuethe_gcia.html)

In the snort signature database (http://www.snort.org/snort-db/sid.html?sid=1394) it is also stated that simply having repetitions of the letter 'a' in the payload could trigger this rule. For these reasons a more definitive answer whether this is malicious or not, should be made by looking at actual packet captures to view the payload. Looking at the captures, it does appear that these alerts are generated due to binary file downloads.

Offender #2: openbsd.sunsite.ualberta.ca (129.128.5.191)
This appears to be a download site for OpenBSD – another likely reason for the high ranking.

For the WinVNC alerts, I cannot put it more succinctly. This is a remote desktop environment which allows a computer to be controlled from anywhere on the internet. The systems with this alert must be investigated.

Action Taken!

Investigated these systems:
MY.NET.97.10 MY.NET.97.20 MY.NET.97.34 MY.NET.97.118
MY.NET.97.160 MY.NET.98.84 MY.NET.111.34
Removed these systems from the network, and disabled WinVNC capability with the System Administrator. All systems were returned to normal use.

Port Access — Rank: #5

Summary of Port Access Related Alerts	
connect to 515 from outside	838
SUNRPC highport access!	314
External RPC call	146
TCP SMTP Source Port traffic	102
[GIACENT NIDS] External MiMail alert	72
connect to 515 from inside	2
Traffic from port 53 to port 123	2
Attempted Sun RPC high port access	1
Total:	1477

Overview

The last section we will cover is alerts due to access to ports identified as important to monitor.

Top 5 Alert Sources
68.32.127.158
148.243.229.134
216.87.56.33
209.249.182.79
128.122.20.14

Core Findings & Asset Analysis

The traffic related to port 515 shows what looks like a worm (Ramen or Adore) searching for an open lpd port (515). The MY.NET attempt looks like traffic to an internal LAN. This 192.168 class of address is non-routable. This could be a rogue device, so if you do not allow such internal LANs, this might be something to look into.

```
01/06-01:21:29.994649  [**] connect to 515 from outside [**] 68.32.127.158:54909 -> MY.NET.24.15:515
01/06-01:21:30.042794  [**] connect to 515 from outside [**] 68.32.127.158:54909 -> MY.NET.24.15:515
01/06-13:14:19.351135  [**] connect to 515 from inside [**] MY.NET.42.4:3398 -> 192.168.0.10:515
01/06-13:14:51.302370  [**] connect to 515 from inside [**] MY.NET.42.4:3400 -> 192.168.0.10:515
```

The next log looks like Ramen scanning for a vulnerable rpc.statd.
CERT Incident Note IN-2001-01
http://www.cert.org/incident_notes/IN-2001-01.html

```
01/09-12:47:46.000000 148.243.229.134:53069->MY.NET.190.212:111 SYN ******S*
01/09-12:47:46.000000 148.243.229.134:53093->MY.NET.190.236:111 SYN ******S*
01/09-12:47:46.000000 148.243.229.134:53096->MY.NET.190.239:111 SYN ******S*
01/09-12:47:46.000000 148.243.229.134:53098->MY.NET.190.241:111 SYN ******S*
01/09-12:47:46.000000 148.243.229.134:53103->MY.NET.190.246:111 SYN ******S*
01/09-12:47:46.000000 148.243.229.134:53105->MY.NET.190.248:111 SYN ******S*
01/09-12:47:46.000000 148.243.229.134:53109->MY.NET.190.252:111 SYN ******S*
01/09-12:47:46.022938  [**] External RPC call [**] 148.243.229.134:53069 -> MY.NET.190.212:111
01/09-12:47:46.235312  [**] External RPC call [**] 148.243.229.134:53093 -> MY.NET.190.236:111
01/09-12:47:46.260214  [**] External RPC call [**] 148.243.229.134:53036 -> MY.NET.190.179:111
01/09-12:47:46.282076  [**] External RPC call [**] 148.243.229.134:53096 -> MY.NET.190.239:111
01/09-12:47:46.284893  [**] External RPC call [**] 148.243.229.134:53037 -> MY.NET.190.180:111
01/09-12:47:46.306431  [**] External RPC call [**] 148.243.229.134:53038 -> MY.NET.190.181:111
01/09-12:47:46.316359  [**] External RPC call [**] 148.243.229.134:53039 -> MY.NET.190.182:111
```

This looks like another RPC worm. This one would most likely be targeted a Solaris systems. See http://isc.incidents.org/port_details.html?port=32771

```
01/09-21:09:50.577116  [**] SUNRPC highport access! [**] 216.239.41.99:80 -> MY.NET.97.34:32771
01/09-21:09:53.199150  [**] SUNRPC highport access! [**] 216.239.41.99:80 -> MY.NET.97.34:32771
01/09-21:09:53.203090  [**] SUNRPC highport access! [**] 216.239.41.99:80 -> MY.NET.97.34:32771
01/09-21:14:42.417400  [**] SUNRPC highport access! [**] 216.239.41.99:80 -> MY.NET.97.34:32771
```

You should also make sure that systems are patched. See this page for more information and patch reference:

CERT Incident Note IN-2003-02
W32/Mimail Virus
http://www.cert.org/incident_notes/IN-2003-02.html

01/09-11:19:33.002226 [**] [GIACENT NIDS] External MiMail alert [**]
218.162.27.63:13924 -> MY.NET.12.6:25
01/09-15:29:53.984366 [**] [GIACENT NIDS] External MiMail alert [**]
68.55.129.228:33749 -> MY.NET.12.6:25
01/09-15:30:24.528229 [**] [GIACENT NIDS] External MiMail alert [**]
68.55.129.228:32866 -> MY.NET.12.6:25
01/09-15:30:24.559879 [**] [GIACENT NIDS] External MiMail alert [**]
68.55.129.228:33746 -> MY.NET.12.6:25
01/09-15:30:31.652830 [**] [GIACENT NIDS] External MiMail alert [**]
68.55.129.228:32776 -> MY.NET.12.6:25
01/09-15:32:18.820502 [**] [GIACENT NIDS] External MiMail alert [**]
68.55.129.228:32861 -> MY.NET.12.6:25
01/09-15:33:24.815765 [**] [GIACENT NIDS] External MiMail alert [**]
68.55.129.228:32953 -> MY.NET.12.6:25

An interesting detect from the “TCP SMTP Source Port traffic” alert, correlated with the scan data.

01/07-03:48:42.000000 MY.NET.1.3:41446 -> 200.170.139.33:53 UDP
01/07-03:51:42.000000 MY.NET.1.3:41446 -> 200.170.139.33:53 UDP
01/07-10:35:45.000000 MY.NET.1.3:41446 -> 200.170.139.33:53 UDP
01/08-05:04:42.901722 [**] TCP SMTP Source Port traffic [**] 200.170.139.33:25 -> MY.NET.20.97:97
01/08-22:00:53.041459 [**] TCP SMTP Source Port traffic[**] 200.170.139.33:25 -> MY.NET.153.101:850
01/08-22:26:38.542312 [**] TCP SMTP Source Port traffic[**] 200.170.139.33:25 -> MY.NET.150.112:246
01/09-01:22:18.716206 [**] TCP SMTP Source Port traffic [**] 200.170.139.33:25 -> MY.NET.24.18:630
01/09-05:09:14.902976 [**] TCP SMTP Source Port traffic [**] 200.170.139.33:25 -> MY.NET.17.67:415
01/09-07:40:36.559016 [**] TCP SMTP Source Port traffic [**] 200.170.139.33:25 -> MY.NET.151.42:364
01/09-09:55:25.830284 [**] TCP SMTP Source Port traffic [**] 200.170.139.33:25 -> MY.NET.64.4:639

It looks to me like MY.NET.1.3 spread it’s worm to 200.170.139.33, then we see the infected computer begin scanning MY.NET using port 25. MY.NET.1.3 was flagged in the scan section of the audit as infected with a worm.

Audit Conclusion

Correcting the issues in this document will lead to a drastically more secure organization. It is clear that you have two targeted services on your network that need attention: web and mail services. All the computers you use to operate these services should be a focus in getting patches up to date, and locking down the network.

There are also a few key technical areas where security needs to be improved. You need enterprise virus software, and regular security auditing efforts, possibly on a quarterly basis. We also see the need for managing patches and updates for systems.

The last area needing attention is administrative. You need to begin developing roles and accountability as it relates to security in the company. We are including materials necessary to implement an *Acceptable Use Policy.* This policy will inform your employees of your intent to monitor systems, your expectations, and the possible consequences. We also think it would be prudent to implement a dial-up access policy for dialing into outside internet service providers.

You have taken a great step in getting your organization secured. As you enter this remediation stage, please remember that we are available to help you in this stage at any level you choose. We would also recommend scheduling a follow-up audit to verify the changes made are protecting you properly. If we perform the remediation, this step will be automatic as a part of our service to you.

Thank you for the opportunity to serve you, and we look forward to working with you in the future!