



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

Minimizing the effects of infected PC's on a Network

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 2 - Case Study in
Information Security

Submitted by: Sean M. Sheil
Location: Kansas City, 2004

Paper Abstract: This paper will provide a case study of the process taken in helping reduce the effects of infected PC's on a campus network.

Table of Contents

Abstract/Summary.....	2
Before	2
Network and Hardware background	2
Domain and PC Configuration.....	3
Policies and Procedures.....	4
Issues and Threats identified.....	4
During	5
Process at the core	6
Collection and Analysis of Traffic	6
Processing Data.....	9
Traffic Manipulation.....	11
After	11
Conclusion	13
References.....	14

List of Figures

Figure 1	7
Figure 2	8
Figure 3.....	9

Abstract/Summary

With this University's ability to provide the reliable high speed network that has been demanded by the Administration, Faculty, Staff, and Students, we have also provided the means for virus and Trojan infections to spread at an extremely rapid pace. Due to the limited numbers of staff available to provide verification of most non University owned network devices, many devices are connected to the network that contain spyware, trojans, virii, etc.

Due to limited budgets, we found it necessary to analyze current software and hardware to find a viable solution to perform the following functions: determine the type of degradation caused by the device, locate the source of the device, minimize the damage caused by the device, and finally locate and notify the owner of the device. In concluding this process, it will be necessary to refine and document the process continuously so that as each new cycle is started, we can isolate problems before academic pursuits are impacted.

Before

The average enrollment of this University is approximately six thousand Students and seven hundred Faculty and Staff. About fifty percent of the Student population lives in campus housing. Almost every room on campus is equipped with an Ethernet port which has been configured with a fixed connection of speed of 10MB/sec half duplex due to older Category 3 wiring.

The Network and Server Services team currently consists of two System Administrators and me as Manger of the department. Due to the small size of the staff all of us perform all duties within the group. We are responsible for managing over sixty-five servers ranging from file/print servers to mainframes, over seventy-five routers/switches, and wireless access points.

Network and Hardware background

We selected Enterasys as our primary network vendor the previous year. At the core of campus we installed an Enterasys Matrix E7¹ chassis and populated five of the slots with Gigabit interface modules (6G306-06) so that we could connect almost every building to this central point with single-mode fiber. These blades each contained six Gigabit ports that could be populated with either single mode or multi-mode fiber gbics. It was decided that due to the hardware already on hand, we would perform routing functions at each building entrance.

¹ Enterasys Matrix E7 Next-Generation Intelligent Access Platform
URL: <http://www.enterasys.com/products/switching/6C107/>

Each building was then equipped with at least one Enterasys 1H582-51² configured as a router with a Gigabit fiber up-link and up to eighty Ethernet ports. If more ports were necessary, an additional 1H582-51 would be added with a multimode fiber connection to the routed 1H582-51. With the purchase of this hardware, we were able to acquire the Enterasys Netsight Element Manager Software package for switch management. This package allowed us to update firmware and perform limited port configuration.

For our firewall solution, we had purchased a Cisco PIX 525³ with a failover unit. This unit was purchased due to its ability to handle large volumes of data reliably. At the same time, we also purchased a Packeteer PacketShaper 4500⁴ bandwidth optimizer so that we would be able to prioritize academic and mission critical traffic. The Packeteer provided us with the ability to shape or block various types of traffic. The Packeteer also enabled us to reduce or stop some of the traffic destined for the firewall.

Domain and PC Configuration

The University is in the unique position in that we provide all Faculty members with a laptop computer, and all Students with one desktop PC per residence hall room. We are able to provide a fairly high level of reliability on these devices by utilizing the following features: A Windows 2003 domain using Active Directory and Group Policy Objects, a Microsoft SUS Server, and Symantec Antivirus Corporate Edition⁵ for desktops and servers. This configuration gave us the ability to rapidly deploy patches and updates to all managed computers.

On the other side of the coin, approximately forty-five percent of the on-campus students bring a network-enabled device such as a PC or game console. We knew from past history that many of these machines would have out-dated anti-virus software or definitions. Many of our younger users have not yet been fully educated with the knowledge to properly maintain their personal machines.

Because of this understanding, we could ascertain with a high degree of reliability that a majority of these devices would arrive on campus infected with at least one active virus or Trojan. We needed to implement a plan using existing hardware and software to mitigate the spread and damage caused by these devices.

² Enterasys Matrix E1 Workgroup Switch

URL: <http://www.enterasys.com/products/switching/1H582-51/>

³ Cisco PIX 525 Firewall

URL: <http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps2118/index.html>

⁴ Packeteer PacketShaper 4500 URL: http://www.packeteer.com/prod-sol/products/packetshaper_topologies.cfm

⁵ Symantec URL: <http://enterprisesecurity.symantec.com/content/productlink.cfm>

Policies and Procedures

The policies and procedures that were in place were very limited in their existence and enforcement. There were not any set methods of determining if a PC happened to be infected. A call to the helpdesk was usually initiated by the user complaining of their PC running slow, or the user questioning why some functionality had quit working properly.

After this call was generated, an individual from the helpdesk would be dispatched to work on the PC. Once the technician arrived on site, the plan of attack was very simple. Once an infected machine was discovered, a determination was made as to the owner of the machine.

If it was determined that this was a University-owned machine, the user was informed that they had been infected with a virus and they needed to make a backup of any and all files that they wanted to save. Once the user had then called back to the helpdesk to notify them that their files were backed up, personnel were again dispatched to replace the computer's hard drive with the standard campus load set.

If the determination was made that this was a personally owned PC, the user was informed that they appeared to be infected with a virus. They were first advised to make sure that their antivirus was up-to-date and valid. Next they were advised to contact one of the local computer vendors for assistance on removing any virus or Trojan that might be on their PC if they needed further assistance.

Several scenarios were involved with these procedures. First and foremost was the increase of virus/Trojans which were spreading at an increasingly rapid rate. In the past, a virus would take several days to reach campus, and then take even longer to spread on campus. This gave us the advantage of updating our centralized anti-virus solution and pushing out updates to the users. We would also be able to notify all users that they needed to update all non-University owned PC's with the latest patches.

Issues and Threats identified

However, we were now in a situation that in a matter of hours, we were seeing infections on campus that were rapidly spreading across many machines. The risks associated with this scenario were devastating. Once one of these infections arrived on campus, it was only a matter of hours until we would start to experience slowdowns and dropped connections within sub-nets and at the core. Once the core segment was affected, we would start to receive calls from all areas of campus reporting problems. This made it very difficult to determine where the root of the problem was located and was very detrimental to the day to day operations of our users.

Along with the risk of our users being unable to function at full capacity, several of the Trojans/virus would affect the management functionality of our routers and switches. After a period of time, we would not be able to connect to our network switches/routers and monitor traffic flows. It would then become necessary to dispatch a technician to power fail the device. We were virtually blind as to what was happening on our network.

Due to prior attendance of SANS conferences, it was very apparent that we needed to devise a solution that would resolve these issues. It would be necessary to form a team consisting of individuals from within the IT staff and other stake holders that would be affected by any proposed solution. It would also be necessary to evaluate currently available resources and how best to use them. Finally, another group would need to evaluate current policies and procedures and determine any applicable changes that would be necessary. Those changes would need to be presented to various groups on campus for consensus.

During

Several meetings were held with various groups to devise the proposed solution. Realizing that we did not possess, nor could we afford an all-in-one solution, it was determined that we had to utilize resources already on site. After this decision was made, it was discovered that there were some emergency funds available to provide for limited purchases. It was also determined that current policies and procedures had not been updated for several years. Now it was time to put all the pieces together and make it work.

Once we started the implementation process, we realized that three applications were needed. We purchased an upgrade to our network management software. The first product upgraded was Netsight Atlas Console⁶, and Netsight Atlas Policy Manager⁷ for network management. To provide some consistent log reporting, we purchased a product called Sawmill Log Analyzer⁸ from a company called FlowerFire.

Unfortunately due to the limited budget, we were not able to send anyone to training on the products that we had. Individuals took it upon themselves to sit down with the various manuals and learn everything possible in a short period of time. We were also able to utilize resources from some of the vendors that we had worked with in the past. Most notably were the engineers working for Enterasys. They were able to provide information that directed us to sections of the manuals that were essential in completing the process.

⁶ Enterasys NetSight Atlas Console Innovative System-Level Management for the Enterprise
URL: <http://www.enterasys.com/products/management/NSA-CD/>

⁷ Enterasys NetSight Atlas Policy Manager Role-Based System Management for the Enterprise
URL: <http://www.enterasys.com/products/management/NSA-PM-LIC/>

⁸ Sawmill Log Analysis Tool URL: <http://www.sawmill.net/features.html>

Process at the core

We started by looking at our core facilities. We were using a Cisco 525 firewall with failover capabilities at our perimeter. One factor that helped tremendously with our firewall configuration is that when originally implemented our perimeter defenses, we had taken the stance of denying all access and only allowing access as needed for academic pursuits. Over the years we were very careful about opening up additional ports. Because of this configuration, we did not have to make a lot of changes in this area. It was determined that we needed to push the logs out to a syslog server. An old server was brought back into service for this purpose. It should be noted that the logging level determined by campus policy did not allow us to log anything greater than failed connections. This was done in part to help guarantee that user traffic was not affected by high utilization. This means that if someone successfully completes a connection through the firewall, there is not a record of the access.

Due to our limited knowledge of the Unix Operating System, it was determined that this machine needed to be logically separated from the rest of campus as much as possible. With the use of a Vlan and access controls, the exposure of this machine to the rest of campus was reduced drastically. By limiting the number of valid IP addresses that could access this machine, we were able to also help reduce exposure. It should be noted that it is possible for an IP address to be spoofed; therefore this method is not foolproof. It is just one more layer of protection that can be applied. Once this process had been completed, the Sawmill application was installed and configured.

Collection and Analysis of Traffic

As provided, the Sawmill product is relatively easy to use. It was necessary to set up a profile for the log files that we would be using. This product has many pre-defined log-file formats. If one is using a format that has not been predefined, it is possible for the user to create their own. In this case, the PIX syslog format was pre-built. The next few steps were straight forward. It was necessary to define the location of the log files on the remote system. It was also necessary to define the amount of memory and disk space that this application would use. One item that was not readily identifiable was the configuration of the cross references table. In configuring the cross-reference table it is necessary to limit the number of links. The more links that are made, the longer it takes to process each day's log file.

The cross-reference table provides the ability for the user to configure a link between different fields from each log file entry. In our case, I wanted several links to tie pieces of information together. The first was based on the source IP address. I wanted to make sure that we would be able to track the source IP address to its destination port either TCP or UDP, and IP address. I also wanted to be able to track a specific protocol back to its source. One case in particular in

which this was very important was with the MyDoom⁹ virus and its' variants. In these cases we would see large flows of traffic destined for TCP port 25 and 3127.

Once configured, the daily process was very simple. Each morning, the log file from the previous day was read into the log file analyzer. This process occurs each day at 4:00 a.m. By the time support personnel arrive, the data has been processed. Support personnel then connect to the web interface and evaluate statistics from the previous day. It was determined that the following process would be followed and documented so that anyone on staff could perform these functions. The PIX log profile is selected from the menu of profiles. Next it is necessary to select the previous day from the calendar view. Next, we select destination port. Sawmill will then generate a page that lists the top ten failed port attempts. See figure 1.

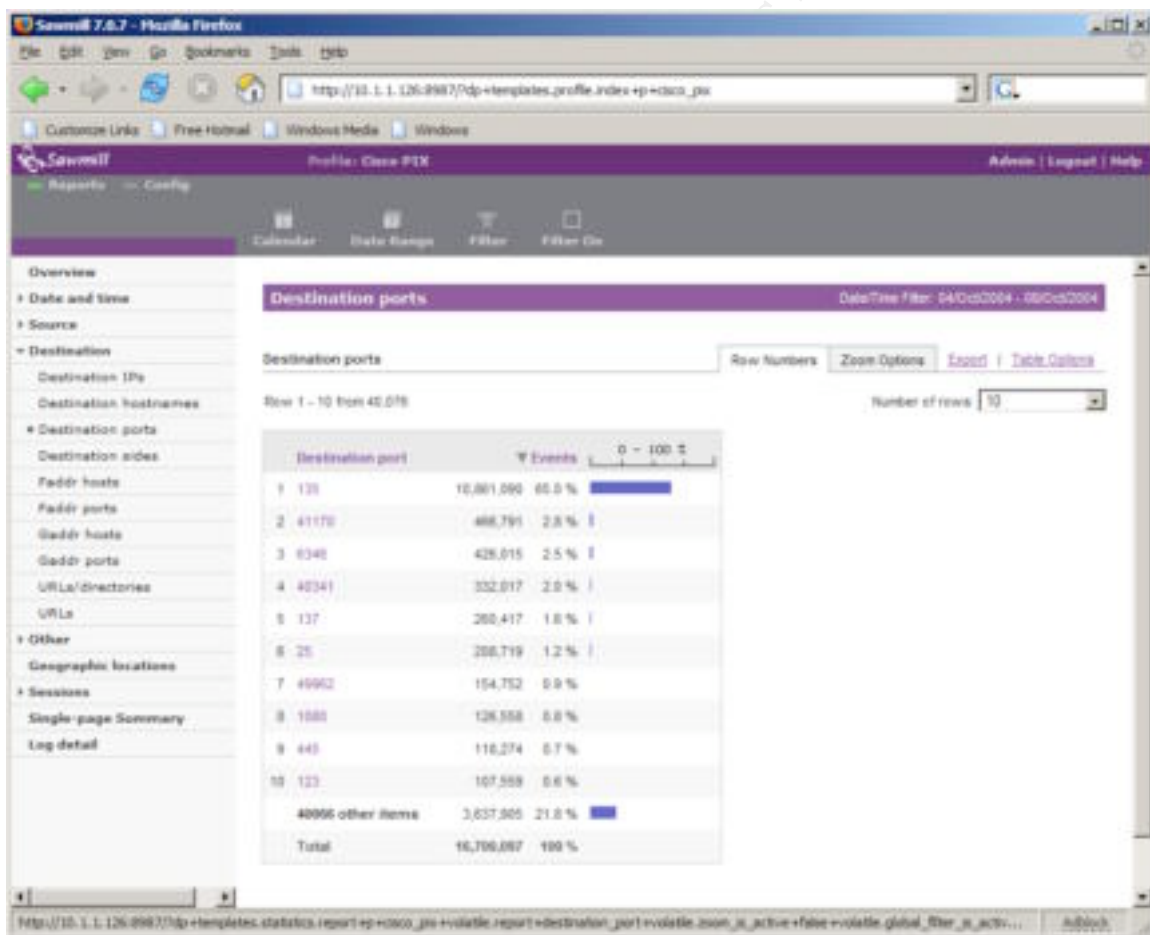


Figure 1

From this page, it is possible to select the port that has been determined to be a problem. By clicking on the port, an additional screen is brought up that allows one to select the appropriate cross reference point. In this case, I usually select

⁹ SANS Internet Storm Center URL: <http://isc.sans.org/diary.php?date=2004-01-29>

source IP address from the drop down box. A page is generated that lists the top IP addresses that have log entries associated with this port. See Figure 2. As noted earlier, the firewall is configured to only log failed attempts. The presence of these entries signify that someone has either configured an application improperly, attempted to run a new unapproved application, or has a process running on their machine that is trying to communicate with the outside world. Analysis of this information is very subjective. If it is noted that a user has a few hundred attempts, this would be noted but not acted upon. However, if a

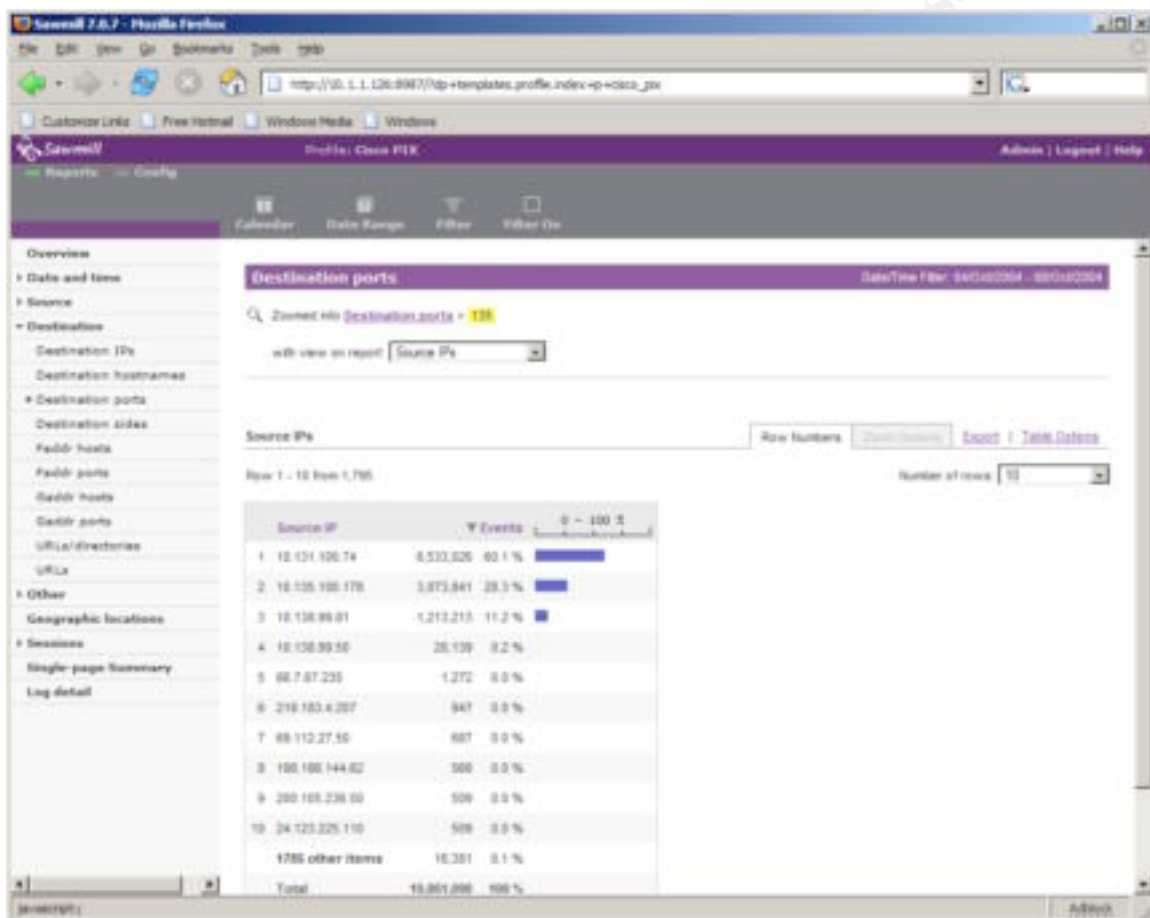


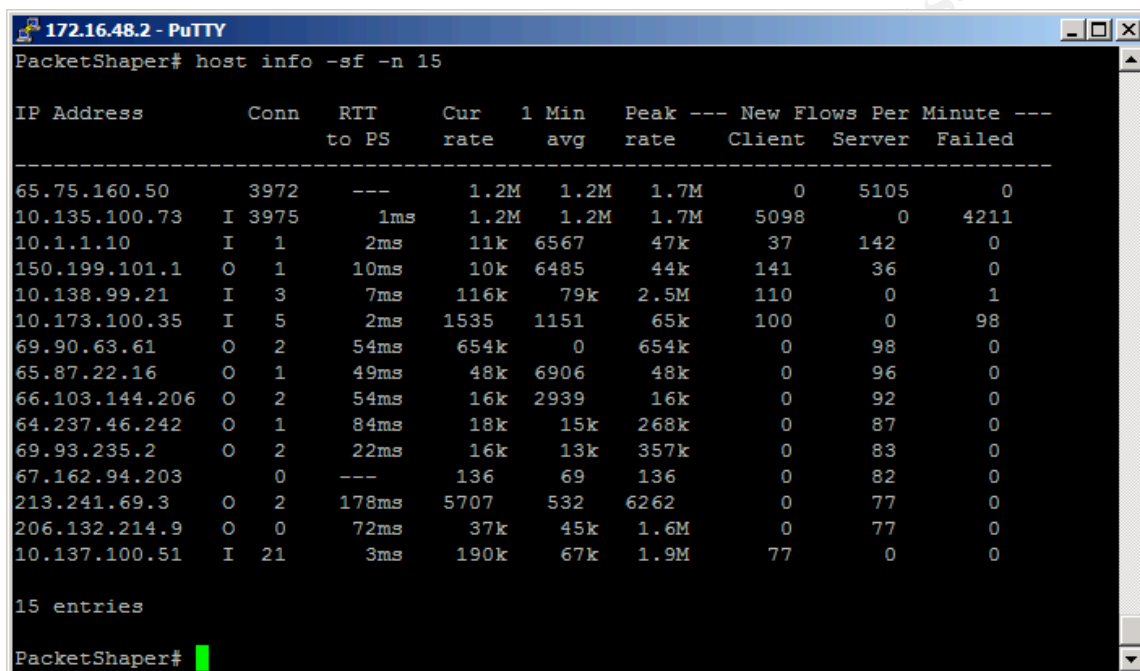
Figure 2

user would happen to have millions of attempts; information would be gathered for the next step in the process

One problem with this process is that the information is from the previous day. By using some of the command line options on the Packeteer, it is possible to collect current information. We have learned that failed flows are most likely caused by the firewall denying inbound/outbound traffic. See figure 3. This procedure is good for a point in time snapshot, but is not useful for historical purposes. We have used both of these methods extensively in locating infected machines on campus. The information provided by the point in time statistics is

very good when disruptions start affecting all users on campus and immediate action has to be taken.

Once a users IP address has been noted for excessive traffic, it is necessary to go to the DHCP server. Three items of interest are gathered from reviewing the DHCP log files. The first item that is determined is if multiple users have requested and received the same address at various times during the day. If there is an indication of multiple users having



```

172.16.48.2 - PuTTY
PacketShaper# host info -sf -n 15

```

IP Address	Conn	RTT to PS	Cur rate	1 Min avg	Peak rate	--- New Flows --- Client Server	Per Minute Failed
65.75.160.50	3972	---	1.2M	1.2M	1.7M	0	5105
10.135.100.73	I 3975	1ms	1.2M	1.2M	1.7M	5098	0
10.1.1.10	I 1	2ms	11k	6567	47k	37	142
150.199.101.1	O 1	10ms	10k	6485	44k	141	36
10.138.99.21	I 3	7ms	116k	79k	2.5M	110	0
10.173.100.35	I 5	2ms	1535	1151	65k	100	0
69.90.63.61	O 2	54ms	654k	0	654k	0	98
65.87.22.16	O 1	49ms	48k	6906	48k	0	96
66.103.144.206	O 2	54ms	16k	2939	16k	0	92
64.237.46.242	O 1	84ms	18k	15k	268k	0	87
69.93.235.2	O 2	22ms	16k	13k	357k	0	83
67.162.94.203	O	---	136	69	136	0	82
213.241.69.3	O 2	178ms	5707	532	6262	0	77
206.132.214.9	O 0	72ms	37k	45k	1.6M	0	77
10.137.100.51	I 21	3ms	190k	67k	1.9M	77	0

15 entries

```

PacketShaper#

```

Figure 3

the same address, each user will eventually be contacted. Once the assignment of an IP address to a machine has been verified, the log file provides us with the hardware address of the offending machine(s). If there is an indication in the log file of a duplicate IP address, it then becomes necessary to look further into the prospect that someone has intentionally assigned themselves a static IP address which is a violation of campus policy.

At this point in the procedure, it is necessary to make some determinations into the severity of the problem. If it appears that there are only one or two machines that have been shown to be causing problems, then the incidents will be handled in a one on one basis. If however, it is determined that many machines appear to have been compromised, then a more aggressive approach will be taken. This second approach is described in detail following this next section.

Processing Data

In the case of a one-on-one scenario, a member of the Network and Server Services team will take the information gathered earlier and proceed to run the

Netsight Atlas Console. At this point, the individual running the program will select the router and switch related to the IP address that was retrieved earlier. Once selected it is then necessary to select the Compass tab. This tab provides the means to search the Enterasys equipment for IP addresses, MAC address, etc. If it was found that only one user had been assigned the IP address, then a search can be done on either the IP address or hardware address. Once the search is complete, the following information is provided: the physical port that the end user is plugged into. This program will also show other physical ports that the user has been connected to.

If Atlas Console shows that the user has been plugged into multiple ports, it makes the task of locating them much harder. Fortunately, most users are still accustomed to having desktops; therefore we do not see a large number of laptops connected to the network. Atlas Console will also provide additional information that is useful in determining which operating system may be installed on the system, which services are enabled, and various counters related to data traffic. These counters include bytes in and out, errors in and out, collisions, fragments, and alignment errors.

Once we are able to identify which physical port this user is located, we then need to access a database maintained by the helpdesk that contains the mapping from the physical switch port to the room number. If the room has more than one Ethernet port, the database will help identify where the port is located in the room. Once this information is collected, it is necessary to execute the helpdesk software and log a call. The helpdesk database allows us to log a call against a room number if the port is located in one of our residence halls. If the computer is determined to be associated with a faculty or staff member, this process gets a little more complicated.

Faculty notebooks are registered in the helpdesk software by their computer name. It is necessary to perform a search on the computer name to locate which Faculty member currently has ownership of the notebook. Currently, there is not a simple method of locating the owner of a staff machine. Staff computers are named based on the building and room number in which they are located. If there are multiple computers in a room, it is necessary for the helpdesk personnel to verify which computer to work on when they arrive.

Under this current process, it can take up to two weeks to resolve an issue that has been identified with a PC. While this was an improvement as far as locating the troublesome PC's, there were several instances where this was not a viable solution at all. This prompted the use of the Netsight Atlas Policy Manager. This product gives us the ability to regulate the traffic flows on our network. Since a vast majority of our network hardware is from the same vendor, we are able to manage over ninety-five percent of our hardware from one console.

Traffic Manipulation

Policy manager allows us to define roles or network policies on a per port basis. In its simplest form, a role allows us to define which traffic to allow or disallow on certain Ethernet ports. For our initial configuration, we defined three roles. The first is based on administrative (faculty/staff) users. The second was designed to be applied on ports in which printers and servers were located. The third was configured for student and lab users.

Netsight Policy Manger allows us to do several functions on a per port basis. It allows us to perform rate limiting based upon role. It also allows us to allow or deny traffic based on traffic that is sourced or destined for a particular port. In order to keep everything simple in our initial implementation, we decided to only deny certain traffic that is sourced on an Ethernet port.

Information used to define these roles is gathered from various locations. The Anti-Virus vendors, SANS, BugTraq¹⁰ are among a few of the sites that provide the detail necessary to develop the service information configured within the various roles. Our first major test of this procedure came with the release of several mass e-mail infections.

These infections arrived on campus from Faculty bringing laptops back on campus after being connected at home, and students bringing personally owned PC's to campus. Initially, we were able to handle these cases individually. However, as the first full day of classes approached, we started seeing more infections per hour than we could handle.

With this infection, we were lucky in that we do not allow any e-mail servers outside of the central computer room. We were then able to create a service entry with the specification that each port was not to allow the sourcing of port 25 (SMTP) traffic. Once this policy was defined and tested, it was only a matter of enforcing this policy campus-wide. In a matter of minutes, the SMTP traffic that was being generated by the infected PC's was reduced to zero.

This same procedure can also be used to reduce the exposure of machines from infection by probing. In the case of the MS-SQL slammer or Sapphire worm, we would have been able to disable communications destined for UDP port 1434 on defined ports. In cases where traffic needs to remain active for normal day to day functionality, it is necessary to perform rate limiting.

After

Once we had all the pieces in place, we were ready to take on the new semester. The students started arriving in mid August with minor problems. By using the monitoring methods that we had set up, we were able to resolve the minor issues

¹⁰ NTBugtraq URL:<http://www.ntbugtraq.com/>

as they arose. Network degradation was minimized to very short periods of time. As soon as the Network & Server Services team was notified of any network issue, even if it was not related, someone would start the investigative process.

The first step that was initiated was a connection to the Packeteer to identify any immediate anomalies. If anything was identified, the helpdesk was notified and a service ticket initiated. As an added precaution, the individual reporting the problem was contacted and all details of the disruption were verified.

Each morning a report would be generated of the previous days firewall logs. Anything that was found to be suspicious was logged into the helpdesk system for further follow-up. The Network and Server Services team kept a copy of all calls that were logged so that trends could be followed.

After the first week of school, it was noted that we were not experiencing any signs of mass e-mail traffic, any signs of the SQL Server infections, or any DNS issues originating from our residence halls and computer labs. We were however, encountering sporadic bursts of icmp traffic and unusual port 135 traffic. It was discovered that with only two machines with this type of infection, users would start to complain.

After we had determined what effect even two infected machines could have on our network, it was determined that the current procedure for correcting an issue with a PC needed to be modified. Due to scheduling conflicts, missed appointments, and avoidance issues, some issues were taking up to three weeks to get resolved. At this point we provided the helpdesk and upper management with information regarding the consequences of slow response times. This information included reports from library staff about repeated disconnects from their remote databases. It was then decided that individuals would be given a twenty-four hour window to respond. If contact was not made, or the issue not resolved, we were to be notified by the helpdesk manager to disable the users Ethernet port. This usually generated a response from the user with just a few hours.

Once it had been determined that the network was stable, it was time to start proactively looking for infected PC's. Since we could easily add and remove traffic policies on a per port basis, we decided to see what else was being controlled by our policies. At this point, we started removing various restrictions for short periods of time. The following day, extra care was given to the daily reports with respect to the policies that were relaxed the previous day.

Network policies are adjusted based on reviews on information obtained from the Internet Storm Center¹¹ and various Anti-Virus vendors. Internally, the firewall logs are monitored for new and unusual traffic patterns.

¹¹ Internet Storm Center URL: <http://isc.sans.org/>

Conclusion

In the educational environment, it is always a struggle to maintain the perceived freedoms of the users and the necessity of maintaining a reliable and stable high speed network. In this case study, I have detailed a portion of one process that has been accomplished at this University. While there are several flaws that still exist in this process, we are continually striving to eliminate them. As technology advances in the hardware and software arena, these efforts will become more manageable.

The overall results of this case study were very positive. The initial goals that I established were met. Network degradation was drastically reduced. My team is now able to ascertain in a short period of time the overall health of each subnet and of the core network. We are now able to pro-actively shutdown or minimize the impact of new virii and Trojans before they are able to infiltrate poorly managed PC's on the network. Throughout this process, my team and other individuals have had the chance to review current policies and procedures and make determinations as to how they should be updated or enforced.

It is still my belief that one of the best ways to reduce these outbreaks and increase stability is to educate the end users on the proper methods of properly maintaining their systems.

© SANS Institute 2005, Author retains full rights.

References

- 1) Enterasys Matrix E7 Next-Generation Intelligent Access Platform
URL: <http://www.enterasys.com/products/switching/6C107/>
- 2) Enterasys Matrix E1 Workgroup Switch
URL: <http://www.enterasys.com/products/switching/1H582-51/>
- 3) Cisco PIX 525 Firewall
URL: <http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps2118/index.html>
- 4) Packeteer PacketShaper 4500
URL: http://www.packeteer.com/prod-sol/products/packetshaper_topologies.cfm
- 5) Symantec
URL: <http://enterprisesecurity.symantec.com/content/productlink.cfm>
- 6) Enterasys NetSight Atlas Console Innovative System-Level Management for the Enterprise
URL: <http://www.enterasys.com/products/management/NSA-CD/>
- 7) Enterasys NetSight Atlas Policy Manager Role-Based System Management for the Enterprise
URL: <http://www.enterasys.com/products/management/NSA-PM-LIC/>
- 8) Sawmill Log Analysis Tool
URL: <http://www.sawmill.net/features.html>
- 9) SANS Internet Storm Center
URL: <http://isc.sans.org/diary.php?date=2004-01-29>
- 10) NTBugtraq [URL: http://www.ntbugtraq.com/](http://www.ntbugtraq.com/)
- 11) SANS Internet Storm Center URL: <http://isc.sans.org/>