Global Information Assurance Certification Paper

Stephen M Jones

Securing A Small Academic Computing Environment,

or,

What to Do When It's Already Too Late

Submitted as the practical for the
GIAC Security Essentials Practical Assignment,
Option 2 – Case Study, ver 1.4b

Abstract

This paper discusses a relatively simple academic computing environment, the problems that were encountered in the almost complete absence of any form of security defense, and the measures taken to reverse this situation. My hope in writing it is that it will help other administrators/managers in resource-constrained situations like mine to understand how significantly security can be improved with very limited financial outlays, and that these improvements can be accomplished with relatively low levels of technical sophistication.

The paper first describes the general computing environment and the exploits that occurred in a key server and in a number of staff workstations. It then discusses the measures taken in light of the content of the Security Essentials course, which made it obvious that a great deal of work was needed to bring the computer equipment and the use made of it into compliance with the principles of defense in depth. Due to the severe budgetary restraints common to academic institutions, most of the attention in accomplishing the security enhancements had to focus on making use of free security basics – reviewing our systems against the most common Windows exploits, explicit password management, implementing the principle of least privilege on staff computers, monitoring network operating system and firewall/IDS logs, scheduled downloading and installing of security patches for all of the operating systems and applications, enhanced physical security for servers, formulation and implementation of a security policy and incident handling procedures, and minimizing internet access to and from servers. The exception to the principle of using only free measures was the purchase of an inexpensive firewall/IDS program, BlackICE™[1].

General Environment/Before

I am the manager of a helpdesk/computing center in the library of one of the member universities of a large state university system, and have overall responsibility for this library's computer facilities[2]. This university has approximately 15,000 students, and is considered to be a medium-sized institution within the system. The Library's computing center runs four Windows 2000 application servers, and is also responsible for supporting about 80 staff workstations and 250 public access pcs located throughout the Library for patron use. The campus network and internet access are handled through a central computing department outside the library, which also provides access to Novell NetWare 6, for file and printer sharing, and Irix for email. The central computing department has a security section which uses a network intrusion detection software setup based on SNORT, which alerted us to our first major problem. It

[1] There is a good description of BlackICE's capabilities in Northcutt's Inside Network Perimeter Security, pp. 514-15.

[2] I have a ¾ time person working with me, hence throughout the rest of the paper I will frequently be referring to what 'we' encountered/did, etc.

also monitors network traffic using the CISCO IOS® NetFlow feature and produces reports every six hours. When there appear to be incidents arising from library equipment, we are provided these reports.

Prior to taking the measures described later in the paper, however, the only security guidance we received from the central computing department was "All you really need to do is keep the equipment patched and have passwords." The central computing department does not have a security policy, and has two staff with student support who are supposed to provide security assistance to the entire university. This is obviously inadequate, and nothing in the rest of this paper should be interpreted as my assigning blame to another party. Since encountering the problems described in this paper and attending the SANS training, the relationship between the library's computing center and the central computing department's security section has grown stronger.

The one exception to university's somewhat weak security situation is in the area of virus protection. The university has a site license for an anti-virus software which central computing has configured to push out updated virus definitions in real time to campus machines. This appears to work well. On several different occasions, I have received security information regarding a new virus at about the same time that a user calls to ask me about an antivirus-generated message indicating that it had stopped the new virus.

Library Servers

The security measures we were following before the incident that led to enhancing our security are embarrassing to think about now, namely, we kept the server (originally only one) patched, though without a schedule for doing so, and it had a six letter, alpha password on the administrator account which everyone in the library computing center, including student assistants, knew. In addition, the servers were kept where any of the staff in library computing could access them, which we later learned resulted in software being installed that shouldn't have been installed.

We originally had four applications running on the same Windows 2000 server. Although this was a reasonable thing to do from the standpoint of the server's capacity and the limited processing requirements of the applications involved, we have since discovered (more below) that splitting these applications among separate servers is safer. None of the applications is server intensive, and we have surplus pcs that can easily serve them out. The university system also has an educational contract with Microsoft that allows us to use virtually all of their products at very little expense. So we now have four pcs running Windows 2000 server, so that one application's being compromised, or the computer it is on encountering some other problem, won't take out the other three with it.

Two of the servers run applications that are very little used, and will not be discussed here, though the security measures discussed below have also been applied to them. Details about the other two servers follow.

Print server

The Library uses a network printing application on a Windows 2000/SQL 7 server to allow patrons to send print jobs to centrally located print stations, where they pay for the jobs by swiping campus debit cards, enter a password for the job(s) to protect confidentiality, and then print them. This is a very heavily used system: for the month of November 2002 this system logged roughly 13,000 transactions with approximately 50,000 pages printed (using two HP8150 network printers). Consequently, this is an extremely important system for patrons and a significant revenue generator for the library (patrons are charged ten cents/page). Having it improperly secured led to its being taken out of service for a week, which essentially stopped the ability of library patrons to print online information. Fortunately this incident occurred at a relatively slow period at the end of the semester. Even then, it led to a significant amount of patron and staff displeasure. We clearly needed to secure this server as best we could to minimize the chance of another major disruption in service.

Interlibrary loan server

We use a 3rd party application for this function that also runs on a Windows 2000/SQL 7 server. Since this university is designated as a research university, the Library's interlibrary loan function is also heavily used – the most recent six month period saw over 2000 lending requests and 4000 borrowing requests. The risk associated with having this server inadequately protected is that interlibrary loan department staff cannot perform a major portion of their job duties, and that student and faculty cannot conduct their research in a timely manner.

Staff workstations

At the time we first encountered security problems, most of the staff workstations were running Windows 98. Needless to say, this essentially meant that they were almost completely unsecured. Although we have the ability to provide staff temporary computers when they encounter problems, even switching computers out requires at least half a day of staff time and half a day of our time to accomplish per computer. Another problem with this is that many of the staff are less than sophisticated computer users, so returning computers to service requires that we perform all of the computer's configuration and even very simple functions related to configuring a computer to resemble its predecessor.

Public access pcs

We believe that our public access pcs are not at significant risk. Our first experience in security some years ago resulted from problems associated with configuring public access computers to allow some flexibility in use, while trying to minimize people wittingly or unwittingly making the computers unusable. We experimented with a number of software packages that limited changes to the computer's applications and operating systems. We found these unsatisfactory

because the software required constant updating and tweaking as web functions and other applications changed.

We subsequently found a hardware device that re-installs a hidden image when the computer re-boots. We password protect the bios and prevent people from booting from the floppy drive. This device, however, does not further lock down the operating system or applications, and also creates a temporary area where patrons can download files and even install applications if the installation does not require that the system re-boot. Although nothing is 100% safe, we believe it would take a great deal of effort to get around the hardware device, and to date we have not had any security problems related to these computers that required anything beyond re-booting them.

Problems Encountered

Servers

Since we originally had all of the applications on one server, all of the library's in-house, server-based functions were shut down when it was compromised. Although two of the applications involved are rarely used, having patron printing and a large portion of the interlibrary loan function out of service was a disaster.

We are uncertain what method was used to compromise the server, due to a complete lack of incident handling procedures at the time it occurred. We had a backup pc that we had set up with the same software to accommodate an emergency, or so we thought. When we learned that the primary server had to be taken offline, we installed the backup server and started the complicated process of re-installing the original server. The day after we started this process, however, we were told that the backup had been compromised as well, so we were dead in the water.

We suspect two avenues might have been used to compromise the server. The more probable avenue was getting our password: a six letter alpha password is better than no password at all, but is a long distance from being a strong password. We also used this same password for all administrator accounts, and used "administrator" as the name for the administrator account. (We have since changed all of these practices.) This password in turn was known by both full-time staff and student assistants, which led to another problem.

Though done without malicious intent, we subsequently learned that a student assistant who knew the password had installed Internet Information Server without telling us. Since we were unaware of its presence, we did not take measures to keep it patched. It is thus possible that the server was compromised through a hole in IIS.

So without realizing it, we had a number of major weaknesses in the server's security from a software standpoint, plus we did not have the server physically secure within the department. In many ways we were lucky that we made it as long as we did without incident.

Staff workstations

After the server was hacked, we attempted to increase the security of the staff workstations by upgrading the operating systems from Windows 98 to Windows 2000. Although a good idea, the absence of a security policy to follow in implementing this switchover led to a number of fatal mistakes in its execution. First, operating system changes should have been accomplished through clean installs (Tanase, "Starting from Scratch"). Instead, we bowed to pressures to make this change as quickly as possible and merely upgraded from 98 to 2000, and did not use the opportunity to use lower privilege levels (all staff were made administrators) or enforce strong passwords (most staff kept the passwords they had always used for Novell access, which does not require strong passwords). This also kept intact the malware that we subsequently learned had been installed on these computers before the upgrade.

Consequently, a little over a month after the server attack, I received a call one Friday afternoon from a staff person who said: "Steve, I'm sitting here with my hands in my lap but the cursor is moving all over the screen and opening things." Within a short period of time, we found that four other staff computers had been similarly compromised. At least by this point we had learned to keep the systems up long enough to allow central computing's security section to determine what software the hacker(s) had installed. Within a short period of time, we found that four other staff computers had been similarly hacked.

What We Did/During

Having taken the Security Essentials course, I was well aware that we were in dire need of just about all of the basics. In many ways the risk assessment process had already been taken care of for us by the hackers. The myriad inadequacies in even basic security practices had led to major inconveniences for both staff and patrons, and if left unchanged would lead to more disruptions. Significant measures were needed to correct this situation. As I said initially, however, significant financial and technical resources were unavailable.

More specifically, we needed:

1. strong passwords on all computers, both servers and staff, with different passwords for all of the servers
2. daily operating system patch downloads and installs
3. physical security to minimize student assistants within library computing from having physical access to the servers
4. images of the servers created with as little exposure to the network as possible for rapid deployment if needed, with test installs of these images
5. implementation of the principle of least privilege on staff machines, while maintaining all functionality
6. regular monitoring of server event logs
7. review of the ten most commonly exploited vulnerable services in Windows

8. improved security against potentially dangerous access from the internet to all of the computers, but especially the servers, and, perhaps most importantly,
9. a security policy for all of the Library's computers, but especially for staff workstations, which included incident handling procedures.

Server security

As we considered what to do about server security breaches, we decided to implement seven relatively simple measures – strong passwords, scheduled patching, heightened physical security, imaging for backup, a review of the suggestions in the list of the ten most commonly exploited vulnerable services in Windows (SANS/FBI Top Twenty), limiting internet access, and monitoring of server activity. The central computing department was able to provide us reports regarding suspicious outgoing internet activity, so we did not regard this as an area we needed to monitor ourselves.[3]

First, we changed administrator account names to something other than administrator, and started using long passwords (each unique to the server involved) comprising alphas, numerics, and special characters. Now only two people in the department, myself and the ¾ time person working with me, know these passwords; student assistants are not provided the passwords. We configured the servers to require us to change passwords every ninety days.

Second, we configured the Windows update service to check for updates every day and download and install them automatically, and then configured the servers to re-boot each morning shortly before the library opens. We also checked to make sure that the SQL software was up to date in terms of security patches/service packs. We realize that there are a number of security and functionality issues in automatic configurations such as this. First, there is the possibility that a hacker could use ip/dns spoofing to re-direct such traffic and compromise the servers. Second, patches should be tested before being put into production. However, we operate with very limited resources, and believe that the advantages of having patches installed in a timely fashion outweigh the security and functionality problems involved.

Third, we improved physical security for the servers to minimize access to them by anyone other than the two persons who are supposed to access them (Microsoft, 5-minute Security Advisor). The library computing department occupies two rooms. The door into the department is always locked. However, the door into the room off of this first room was always kept open and unlocked. We arranged for the lock on the door going into the second room to be changed with keys provided only to myself and the other full-time employee (and not the student assistants). We have now moved the servers into this second room.

Fourth, we used Symantec Ghost™ to create backup images of the servers. We have two identical servers that run the printing and interlibrary loan applications. During a slow part of the semester we took both of these servers down and reimaged them using these backup images to make certain that the

[3] Consequently, we chose the PC version, rather than the server version, of BlackICE™ (more below) since we did not regard the added ability of the server version to monitor outgoing traffic as well as incoming as necessary, especially since the server version is $300 vs. the pc version's $50.

images worked. In his section of the Security Essentials training, Eric Cole placed a great deal of emphasis on not only instituting backup procedures, but conducting test restores to make certain that the backups work and can be applied in a timely manner.

Fifth, we reviewed the ten most commonly exploited vulnerable services in Windows and made certain that we complied with the suggested corrections. By the time we reviewed these, we found we were already in compliance with the ones that pertained to us.

Finally, we realized that we were in a very fortunate position in terms of internet access to the servers, namely, that only persons within the university's ip range need to access the applications on these servers. This in turn meant that we could restrict unsolicited internet access to the university's ip range on the one hand and that anyone attempting to hack these servers from this ip range could, conceivably, be traced. In talking with the security staff from central computing, BlackICE™ was mentioned as an inexpensive means of implementing both an intrusion detection system and a firewall.

We bought BlackICE™ and configured it to:

1. accept unsolicited traffic only from the university's ip range;
2. block all unsolicited inbound traffic using auto blocking; and,
3. advise us, and await our instruction, when an application starts that has been altered since installation or when an executable starts for the first time.

We read the BlackICE faqs and other documentation carefully and believe that we have configured it in a manner that will be of best benefit while still allowing the functionality we require. We did this because of an admonition in this regard from Eric Cole: "Most prevention mechanisms that companies put in are either not designed or not configured correctly, which means they are providing minimal protection if any."[4]

Workstation security/security policy

We faced two major problems in dealing with staff pc security, one interpersonal and the other technical.

Since we operate in an academic environment, many staff regard their having complete control over their pc and its applications/files as an extension of their 1st Amendment right to free speech. Even though this belief is questionable at best, the practical reality of the situation was that we had to come up with a way to control account privileges without fomenting a staff revolution.

The other problem we faced is the need to run two proprietary, 16-bit applications used by the online catalog system for library functions (cataloging, circulation, serials, et al.) while avoiding system crashes to the extent possible. Although Microsoft ostensibly guarantees that its applications will run at any user level, we have had problems getting the library applications to run at all, let alone with account access restrictions.

After testing the proprietary software and finding that the two applications would in fact work when used by a Windows 2000 user-level access account, we

[4] Hackers Beware, p. 14.

had to meet with department heads to determine how to make the changeover to lower levels of staff access (almost all staff accounts before this were administrator accounts). The reactions to this proposed change were mixed to say the least. We explained that user levels could be changed quickly if individual problems were encountered. We did, however, have to bow to pressure to make account level assignment a decision that could be made by the department manager on a case by case basis, though we did convince the managers that there should be specific functional requirements for assigning levels higher than user.

Once we had this first hurdle out of the way, I then compiled a simple, draft security policy[5] covering staff accounts, and including incident handling procedures as well as procedures for account deactivation when staff leave the library's employment. The library director appointed a committee of department heads, support staff and myself to come up with a working policy for implementation. Although the subsequent review was time consuming, it helped to raise security awareness across a broad spectrum of the staff.

In this series of meetings we also determined how to make the changeover to strong passwords for all staff, regardless of privilege level. (My initial inclusion in the draft of the requirement that all staff change passwords every ninety days, unfortunately, was dropped from the final version.) We configured a suitable Windows 2000 security template, ran it on each staff machine, and then helped each staff person change their Novell and Windows passwords. This proved to be a time intensive process, and one where we had to use more than average amounts of people skills ("Tell me in plain words why I can't use my daughter's name.").

Conclusion/After

In reviewing the general principles outlined in the Security Essentials course, I believe that our security exposure has improved significantly. In the months since beginning the implementation of these measures we have encountered security breaches only on staff computers that had not yet been brought into compliance with the security measures outlined in this paper. We continue to monitor the operating system and BlackICE™ event logs of the servers weekly, and receive reports from central computing regarding suspicious outgoing activity, if there is any, every two days. As we've reviewed the logs of activity, we find that each machine normally receives at least five port probes a day, often with multiple probes from the same source (some of these going to 300 probes per day). We've also been able to report a number of incidents to isps from which they occurred. We've also started weekly reviews of the event logs in the operating system and thus far haven't found anything suspicious. We

[5] In addition to the materials included in the SANS Security Essentials II: Network Security Overview course book, I also found pp. 1-17 of Walker's Computer Security Policies and SunScreen Firewalls helpful.

are busier now in solving occasional software compatibility problems with staff workstations related to the library software referred to earlier, but this is not excessive.

Though all of the procedures taken were done so in the general absence of highly sophisticated technical resources and equipment/software, we believe that we are now in a much better position to minimize security incidents. It would have been better for all parties involved if these measures had been taken before the problems arose that were caused by the inadequacy of the security that was in place initially, and as we order new computer equipment we make sure that it complies with these policies before it is placed into use.

I would encourage any organization, even/especially small ones with limited resources like the one in which I work, to make use of what are easily implemented security measures, such as those outlined in the SANS/FBI Top Twenty List and on the Microsoft site. Even better, attend SANS training to get a quick grounding in security to help in this process.

I have found, though, that significant security measures can be taken without significant financial expenditures and with access to only relatively low levels of technical expertise. Unfortunately, we had to first learn how significant the losses can be, both financially and in staff and patron time lost, in their absence.

Time will tell, of course, but I believe that even the relatively simple implementations of the general security principles outlined in the Security Essentials course have significantly reduced the possibilities for future security compromises.

References

Cole, Eric. Hackers Beware. Indianapolis: New Riders Publishing. 2002.

Microsoft. 5-Minute Security Advisor - Basic Physical Security. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/5min/5Min-203.asp. 2003

Northcutt, Stephen et al. Inside Network Perimeter Security. Indianapolis: New Riders Publishing. 2003.

SANS Institute. SANS/FBI Top Twenty List: The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus. Version 3.22 March 3, 2003 https://www.sans.org/top20/

Tanase, Matthew. "Starting from scratch: formatting and reinstalling after a security incident." http://www.securityfocus.com/infocus/1692. last updated May 7, 2003.

Walker, Kathryn M. and Linda Crosswhite Cavanaugh. Computer Security Policies and SunScreen™ Firewalls. Palo Alto: Sun Microsystems Inc. 1998

Last Updated: May 28th, 2017

Upcoming Training

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