GIAC
CERTIFICATIONS

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 permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

GSEC Practical
Assignment 1.4b – option 2
Wayne Fielder
Title: Recovering From a Failed Security Audit – A Case Study

"Pride goes before destruction, a haughty spirit before a fall."
- The Holy Bible, Proverbs 16:18 (NIV)

Abstract

In the spring of 2001 my pride was shattered when an independent auditor revealed a number of basic security problems with the network for which I am the Senior Network Administrator including null passwords and SNMP services with vendor default public and private strings. Further internal investigation revealed many security and behavioral issues within the Agency (the term I will use for my employer throughout this document) including anonymous FTP accounts enabled, no written policies, and sensitive data being mishandled.

This case study opens with recognition of the security and privacy issues within the Agency and walks through the process of remediation, securing the use of sensitive data, development and implementation of strong policies, and initiating a solid monitoring system at very low cost due to a deteriorating budget scenario. The results of our efforts made for a much more secure environment as well as increased productivity for the users.

Before - Arrogance run amok.

The Agency is associated with post secondary education. We determine policies and guidelines for colleges and universities based on statistical analysis of enrollment, degree completion, and student retention data among other things. The network was based on Microsoft NT Server and Microsoft Workstation on the clients. The Agency had never had a serious security or privacy posture.

Vacations are wonderful things. I was enjoying some much needed time off in the Spring of 2001 when I received a call from the office asking that I come in for a meeting. The meeting closed and I was about to leave when my boss asked that the technical staff remain. He presented to us two reams of paper with directory listings for several critical workstations in our office. He went on to explain that over the past several weeks an independent auditor had been performing very basic penetration tests on a variety of networks in our organization. Suddenly all my illusions of security were shattered. The penetration test revealed some particular problems and promised deeper issues could be discovered. The fact of a shrinking budget meant all of our efforts had to be based on a near zero cost budget.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The penetration tests were not intrusive. They were simply surface scans of the network to find the glaring problems. Essentially they were looking for null passwords of all varieties. The final report listed three specific issues; an IIS vulnerability that exposed SQL Server usernames and passwords, SNMP devices with vendor default public and private strings, and local workstation administrator accounts with null passwords.

The report was a harsh wakeup call for me. I could not believe I would leave workstation administrator accounts with null passwords. I knew I had something to prove at that point so I pulled my staff together and developed a plan to find as many issues as we could. I did not want to be surprised like this again.

We used Enum[1], a free netbios scanner, and Fscan, a free port scanner now named Scanline[2], in conjunction with Active State's free Perl interpreter[3] to write a script to loop through our entire IP range with the results being piped into text files. The raw output from Enum can be difficult to read when multiple workstations are scanned. We wrote another Perl script to parse the Enum results file into three separate files where all server related information (shares, quotas, password policy etc) is in one file, group information (group names and membership) in another file, and local user information (username and attributes) in another file. This approach allowed us to assign specific tasks to specific individuals during the remediation effort, as we will discuss later. The port scan revealed four print servers with embedded web, ftp, and tftp services running, three unauthorized ports being used by streaming audio applications, and all of our web and FTP services. Since the auditors had found the web vulnerability we decided to test the FTP servers for anonymous write permissions and found one server. The netbios scan revealed several user accounts with null passwords, no password policies anywhere, users in the local administrators group, and workstation-based shares.

During preliminary investigation of the workstation-based shares, a privacy issue was revealed. The Agency unit responsible for analysis of student data was storing working data sets as text on a workstation-based share. This data is protected under the Family Education Rights and Privacy Act (FERPA). FERPA is a Federal law that protects the privacy of student education records[4]. We have to be very careful in how we handle student data. We can present the data in aggregate form but we cannot release, publish, or otherwise expose data that could be used to identify individual students. The share was simply created with the default "Everyone – Full Control" permission thus exposing the data to the world. This share was immediately closed but a larger question remained. How is the data being handled generally? The staff realized the data was sensitive but didn't see a problem as long as they didn't post it on a website or some other obviously public medium. They regularly exchanged this information with 9 separate organizations via FTP, email attachments, and US Mail on CD and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

diskette. The FTP connection and the email server were unprotected by SSL or any other type of encryption.

Many employees started their tenure with the Agency when the personal computer was just being introduced to the marketplace. They were used to working in an environment where they felt the only possible threat from outside the Agency was loss of power. While the revelation of the penetration test was a wake up call to those of us in the Technical staff, the whole episode went unnoticed by the rest of the staff. There would have to be a successful education effort made on the part of the technical staff before any other security measure could begin to take hold.

During – Humble Pie makes for a bitter feast

All the data being gathered, we began to assess the overall risk of each issue using the formula Risk = Threat X Vulnerability[5].

Threats come in all shapes and sizes and we can't protect against all of them[6]. Most of our issues threatened the network itself for example; the SNMP devices with vendor default strings threatened the integrity of our network. The FERPA Compliance issue had another threat vector all together. Not only did our behavior threaten the privacy of student information but also threatened the Agency with legal action.

We determined the threats and vulnerabilities of each issue as they pertained to the Agency, assigning a value from 1 to 10 for each. It was difficult at times to keep in mind that the final chart was not a to do list with the remediation of some issues taking a back seat to other issues. I continually reminded my staff that all of the issues were critically important. The Risk Assessment formula made the list graduated but this should not imply that a written Disaster and Recovery Policy was any less important that the FERPA compliance issue. In fact, the decision to address the issues first enabled us to essentially write the various policies as we resolved the issues.

Issue	Risk Level	Threat	Vulnerability
FERPA Compliance	High	10	10
Web Vulnerability exposing SQL Server credentials	High	10	10
SNMP Devices with vendor default Public and Private strings	High	10	9
Print Servers w/embedded services	High	9	10
FTP Servers w/Anonymous enabled for read and write	High	9	10
Local Administrator	High	9	9

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

accounts with null PW			
Unauthorized Ports	High	8	7
Users in Local Administrator Groups	Medium	7	7
Password Policy	Medium	8	5
User Education	Medium	6	2
Security Policy	Medium	7	1
Disaster and Recovery Policy	Medium	4	1

Of the high priority issues, we decided first to address those issues that had the greatest impact to the security of the network and that would be the quickest to resolve.

Hardware print servers commonly include web-based administration. This sounds like a great idea but unfortunately these embedded web servers are often impossible to patch. These web services then become breeding grounds for viruses such as Code Red and Nimda. We chose to disable all embedded services on these devices[7]. As part of the process we performed a hard reset and were surprised to find the web, ftp, and tftp services returned. We once again disabled them and decided this would be included in the incident response section of the Security Policy that will be discussed later.

The oversight of the Anonymous accounts on the FTP server raised serious concerns about our installation procedures or lack thereof. The existing practice included noting installation of services in logs but there was no best practice checklist for configuration options. This would no longer be the case as we decided to create a checklist for IIS installations including disallowing anonymous access to all ftp services. In the event anonymous access FTP is required, a separate machine configured on a separate network would be used. Resolving the issue itself was accomplished by removing anonymous access altogether.

Simple Network Management Protocol (SNMP), as defined in RFC1157, was developed to "allow diverse network objects to participate in a global network management architecture"[8]. Network objects are the various pieces of network infrastructure such as routers and switches. Communication between these devices is authenticated through the use of two "passwords" collectively known as community strings. There are two strings, public and private. Public community strings govern read operations to the device. Private community strings govern write operations to the device. Typically, vendor defaults for these strings are "public" and "private" respectively. If the defaults are not changed access to the devices is a simple task through the use of commercial SNMP tools such as Hewlett Packard's Openview and Nortel's Optivity or any number of open source SNMP tools. Once SNMP devices are compromised your network is no longer your network. We decided to include the SNMP public and private

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

strings in our Password Policy so the public and private strings would change as the policy dictates. Strong passwords were generated as defined in the Password Policy and assigned to the strings for the devices.

Resolving the local administrator null password issue consisted of visiting the various workstations and entering a strong password. How the password became null was the real question. Workstations at the Agency are divided into three categories regular users, network administrators, and developers. An image for each category of workstation is created and applied to each workstation within the category. We found that only one category of workstation had the null password issue and it was, of course, the largest. The "regular user" category includes the Agency's business office, legal office, and senior management. We decided to create a checklist for image creation that would include workstation operating system, applications to be installed, and renaming the Administrator account and assigning a strong password as defined in the Password Policy. The image was rebuilt using the checklist.

Part of the image rebuild included the installation of the virus scan product. During the installation my staff discovered why the users were placed in the local administrators group on all the workstations. The installation asks what level of security you wish the service to run under. On the existing image the option chosen was that which would run the service under the current user's permissions. If the user was not in the local administrators group the service could not update virus signatures automatically. We changed the option to that which would run the service using the System account, removed each user from the local administrator group, and created a workstation installation checklist that will check for this issue.

The above issues were considered obvious problems that could be readily exploited with little or no technical expertise. Next we turned our attention to issues that would require more resources to resolve.

The issue of unauthorized ports being active on certain workstations proved to be particularly difficult to resolve from the user behavior perspective. This only reinforced the need for ongoing user education within the Agency. The users couldn't understand why we were "forcing them to stop listening to the radio". We used Fport and Ethereal and discovered these ports were not simply listening for data but also sending information to other workstations inside the Agency. Typically with streaming media applications you will see the TCP handshake occurring where the "Syn" and "Ack" communication are the only outbound communications from the workstation. In this case however there was streaming data being pushed from the workstation as well. Further investigation revealed the plug in "… enables consumers with sufficient bandwidth to act as Virtual Multicast Routers (VMR) - seamlessly sending streams to additional users"[9] which opened two additional TCP ports, one for the data itself and one for control. We had to explain to the users that they were "leaving the keys in the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

front door" of the network when they used this particular streaming media plug in. We had no reason to suspect the plug in was capable of malicious activity but we were not comfortable with having random ports pushing information around our network. In the event the plug in was compromised the Agency could be exposed to viruses, Trojans, or Denial of Service attacks originating from workstations using the plug in. We considered simply removing the plug in from the workstations but realized we had no way of knowing if the plug in was completely removed and we didn't know what other areas of the workstation the plug in had "configured". Finally, we decided to apply the new image to these workstations. The new image, with local users removed from the local administrator group, would prohibit the users from installing the plug in again, and we could be certain there was no remnant of the plug in on the system. There are other applications available that could be used for streaming audio, some built in to the workstation operating systems.

The Netbios scan revealed several user accounts for users who were no longer with the Agency and three global groups with no members. All network shares were accounted for and permissions were set correctly aside from the one workstation-based share that was closed before our official remediation effort began. One member of the Technical Staff and one intern were given the Users report and the Groups report respectively and assigned the task of resolving the issues. The files associated with the "vacant" user accounts were backed up to tape and the user accounts were disabled for two weeks. No one reported loss of access to anything during the two week period so the accounts were deleted. The unpopulated groups were simply deleted.

The web vulnerability found by the auditors, Microsoft TechNet article Q260069 - Malformed HTR Request Returns Source Code for ASP Scripting Files[10], revealed a username and password used by the Agency's website to access the SQL Server. The username in question was not SQL Server's SA account but the threat was still very real since most every database call used the same credentials revealed by this vulnerability. Microsoft had released a patch for the vulnerability but we had never installed it relying instead on service packs to provide protection. Experience is a harsh teacher. Using HFNETCHK[11] we found a wide array of patches available for IIS. I assigned a staff member to the task of bringing all of our servers, including IIS installations up to date on patches. We decided that whenever a patch is released for any application in use by the Agency, the patch would be installed within 48 hours of the release date. In the event of a significant threat to the network, such as the Sapphire, or Slammer, SQL Server worm, the patch would be installed immediately. Some vendors have a reputation for releasing patches that sometimes do more harm than good to the server they are designed to protect. The 48-hour delay allows us to monitor certain newsgroups and discussion forums to see if there are reports of unintended effects to servers and networks brought about by the patch. The forums and mailing list archives at Security Focus[12] are excellent resources for monitoring the stability of Microsoft patches.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

While the technical staff under my direction was addressing the technical issues above, I began addressing the privacy issues with the Statistical Analysis unit and Senior Management of the Agency. Closing the workstation-based share immediately ended the exposure of the student data but the handling of the data was still an issue. The transmission of the data across the internet via unsecured FTP, email, and US Mail had to be addressed immediately. The information had to be shared among the organizations but something had to be done to protect the data. Since the final solution would effect all 10 organizations I met with technical representatives of the organizations and explained the situation. I offered two solutions. First, all the organizations could purchase SSL certificates. I recommended Thawte's Web Server Certificates. The cost would be $349 for a two-year certificate or $199 for a one-year certificate[13]. This would enable the data to be transferred via the web in a secure manner. The second option used Pretty Good Privacy (PGP) by PGP Corporation. PGP Enterprise would offer a variety of tools and allow the Agency to manage the key rings for the other organizations. It would also allow them to encrypt their datasets and then use any method of transmission. PGP Enterprise would cost $125 per year or $260 for a perpetual license[14]. GNU Privacy Guard[15] would provide the same encryption levels as PGP and because of the GNU General Public License[16] there would be no cost associated with using it. While cost was a definite issue for us, vendor support would also be critical. Information Technology professionals would have no problem finding support through the open source community. Unfortunately, many of our constituent researcher organizations were long on statisticians and short on IT professionals and because of this we dropped GPG from consideration. PGP or the Thawte certificate would address the need to protect the data. The Agency had considered building a web based system that would allow other researchers both associated with postsecondary education institutions as well as independent researchers to query the data through the web. The solution from Thawte would be a good step toward the web based searchable database. However, due to the deepening budget crisis, the recurring cost associated with the Thawte solution was prohibitive. The group agreed to use the PGP option. This would satisfy our FERPA obligations by securing the transmission of the data by encrypting data sets with 4,096 bit keys before transmitting. The Agency would use PGP Key Server to manage the keys of the other organizations and provide training sessions and materials for the organizations as needed.

Having addressed the issues reported by the auditors as well as those we discovered ourselves, we took the lessons learned and looked to writing effective policies that would govern the use of our technology in the future.

A favorite insurance sales slogan is "No one plans to fail, they only fail to plan." This is also true of network security. Had I taken the time to develop sound policies I would not have been shocked, embarrassed, and had my job

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

threatened by the fact that my network was a disaster waiting to happen. We began the development of our policies by looking at our existing procedures.

Our backup procedures were effective and had worked wonderfully after a severe file server crash. Creation of a Backup and Disaster Recovery policy consisted of committing to writing our existing procedures. The policy consists of the following:

- Nightly Full backups across all servers
- Thursday backups removed offsite
- Friday backups are retained for 4 or 5 weeks (dependent upon number of Fridays in month)
- End of Month backups permanently stored offsite and cycled annually
- Annual backups permanently stored offsite
- Five years of annual backups are retained. Sixth year backup tapes are destroyed
- Test restores are performed on the 15th of every month testing every monthly and annual tape in retention
- Backup logs checked daily and backup checklist completed

The backup checklist included fields for date of backup; any anomalies such as verify failures on particular files, tape drive cleaning date, and username of administrator. Once completed the checklist is submitted to the Senior Network Administrator for review. I investigate and resolve any anomalies. We are currently considering the development of a web-based solution for the checklist.

Before the auditors made their presence known, there was no security policy for the Agency. We had to get something effective and enforceable in place. Realizing that any policy should be a living document we decided to review the policy monthly for the first year of its life and quarterly thereafter. The Security Policy for the Agency includes several sections. The section names and synopsis of contents are as follows:

Password Policy Section

- SNMP community strings will be treated as other passwords
- Telnet passwords for external print servers and infrastructure devices will be treated as other passwords
- Passwords should contain alpha, numeric, and special characters
- Passwords should not contain proper names
- Passwords should not be shared under any circumstances
- Passwords will be rotated every 35 days and may not be repeated for 5 cycles

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Change Control Section

- Any configuration changes to network devices including servers will be performed after business hours on Fridays
- All configuration changes will be reviewed by Technical Staff and logged
- Vendor patches will be installed within 48 hours of release date contingent upon patch stability as determined by Senior Network Administrator
- All server restarts will be preceded by 10 minute warning page to users except in event of emergencies
- Change Control Log will be reviewed quarterly

Incident Response Section

- Power Failures will trigger the following
  - All embedded services on external print services will be disabled
  - Servers logs checked for UPS functionality
- Three failed login attempts will be considered an unauthorized intrusion attempt. The account will be locked out for one hour.
- Viral infection of workstations will trigger the following
  - Workstation immediately removed from network and replaced
  - Investigation of infected workstation to determine method of infection and current virus signature version
  - If virus signatures are current, notify Wide Area Network partners of virus name (if known), method of infection, and current virus signature version
- Suspicious (hacking) behavior will immediately trigger the following
  - Saving all log files as text files
  - Emergency device shutdown
  - Analyze log files to determine nature of behavior
  - Consultation with Senior Management
  - Notification of Authorities if appropriate

Security Posture

- Server event logs and infrastructure device logs will be reviewed daily
- Network Port, NetBios, and Patch (HFNETCHK) scans will be performed bi-monthly
  - Results will be retained for six months on removable media
  - Results will be encrypted using Technical Staff PGP key
- All workstations and servers will be locked or logged out when left unattended

The Password section maintains the confidentiality of our network by insuring proper password management. The Change Control section maintains the integrity of our network by insuring current patch levels, requiring consensus among technical staff before configuration changes are implemented, and allowing time to revert to the previous configuration in the event a configuration change fails. The Incident Response and Security Posture section maintains the availability of our network by providing clear steps to be taken in event of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

intrusion, active monitoring of logs, regular scanning of network periphery, and requiring workstations and servers to be locked when unattended. The policy was entered into the official Agency policy manual. A violation in the Security Policy by any employee could now be grounds for disciplinary action including termination.

An intense effort to educate the user base was initiated by scheduling a series of Network Awareness seminars. The first topic of the series was a broad overview of Network Security including password management, the threat of social engineering, and access control. These issues are continually reinforced through non-threatening friendly reminders. The users themselves chose topics for the following seminars, we teach them what they want to learn. Since the users are already interested in the topic it is much easier to cover related areas particular to the threat of the day.

After – Remaining Vigilant…and humble.

Before the initial penetration test the Agency's network was a disaster. My pride and over confidence had blinded me to the necessary steps that must be taken to maintain a secure network environment. Resolving the issues revealed the information necessary to develop our Security Policy. Basically, whatever caused the problem should be prevented in the future by including it in the policy. Reviewing the Security Policy quarterly gives the Agency the flexibility and accountability required to keep the "teeth" in the policy.

While the new security posture has restricted the permissions of the users on the network, the new stability and omnipresent monitoring has provided a comfort level that is evident in the behavior of the users. The knowledge gained through the Network Awareness seminars has had a direct positive impact on overall productivity.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

1) BINDView RAZOR, Jordon Ritter, Enum
URL: http://razor.bindview.com/tools/desc/enum_readme.html
Last Accessed April 7, 2003

2) Foundstone Inc, Scanline
URL: http://www.foundstone.com/resources/proddesc/scanline.htm
Last Accessed April 7, 2003

3) ActiveState, Active Perl
URL: http://www.activestate.com/Products/ActivePerl/index.plex
Last Accessed April 7, 2003

4) US Department of Education, Family Education Rights and Privacy Act, August 21, 1974
URL: http://www.ed.gov/offices/OM/fpco/ferpa/index.html
Last Accessed March 27, 2003

5) The Sans Institute, GSEC Courseware, SANS Security Essentials II – Network Security Overview, page 1-11, 2002

6) The Sans Institute, GSEC Courseware, SANS Security Essentials II – Network Security Overview, page 1-9, 2002

7) Hewlett-Packard, Disabling or Enabling a Protocol Using Web JetAdmin, Telnet, or Embedded Web Server
URL:
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj01110
Last Accessed March 28, 2003

8) The Protocol Directory – TCP/IP, SNMP
URL: http://www.protocols.com/pbook/tcpip7.htm#SNMP
Last Accessed March 28, 2003

9) ChainCast Networks
URL: http://www.chaincast.com/technology/chaincasting.html
Last Accessed March 30, 2003

10) Microsoft, Malformed HTR Request Returns Source Code for ASP Scripting Files
URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q260069&sd=tech
Last Accessed March 30, 2003

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

11) Microsoft, HFNETCHK
URL: http://www.microsoft.com/technet/security/tools/tools/hfnetchk.asp
Last Accessed April 7, 2003

12) Security Focus, Home Mailing List: FOCUS-MS
URL: http://www.securityfocus.com/archive/88
Last accessed March 30, 2003

13) Thawte, Web Server Certificates
URL: https://www.thawte.com/ucgi/gothawte.cgi?a=w35280040567004000
Last Accessed March 30, 2003

14) PGP Corporation
URL: https://store.pgp.com/default.php?cPath=65
Last Accessed March 30, 2003

15) GNU Privacy Guard
URL: http://www.gnupg.org
Last Accessed April 7, 2003

16) GNU General Public License
URL: http://www.gnu.org/copyleft/gpl.html
Last Accessed April 7, 2003

© SANS Institute 2003, Author retains full rights.