# Global Information Assurance Certification Paper

SANS Practical – version 1.4b, Option 2 – Case Study in Information Security
By Melissa Wise

# Inheriting a Network:
# Performing a Security Analysis on an Existing Network

Abstract

Coming into an existing network is always full of unknowns and surprises, even when you have an upper hand. I recently switched jobs to run the MIS Department for a facility for mental retardation patients. I had worked for this company previously and actually installed and ran their network for four years before leaving for another position. After four years and three MIS Directors, I returned to my old job.

My first task was to do a security analysis of the network, since HIPAA deadlines are quickly approaching. Management was not very confident of the network's security since it had been so long without a MIS Director in place. What I found was very eye opening to the management and actually shocked me because I knew how the network was setup initially. What I came back to held little resemblance to the network I left four years prior. Little did I expect to find rampant disregard for even basic network security, attempts to run personal email servers on company-owned servers, illegal and/or unauthorized software running on critical servers, and no documentation. With complete management support, I was able to quickly get the situation under control and not only bring us closer to HIPAA compliance, but also to make us a harder target for the ever-searching hackers.

## Before

For the sake of anonymity, we will call this facility Springhills. Springhills had gone through several MIS Directors after I left and had been without a MIS Director for 18 months before I was hired. In that time, the two technicians put out fires, kept things running and had little technical oversight. The only oversight was from a central office, who made sure purchases submitted to them were done according to approved specifications and with approved vendors. In addition, it was suspected that a previous MIS Director had been monitoring systems without authorization.

To complicate it a bit more, the domain our facility network belongs to, spans the entire state and the Primary Domain Controller (PDC) is housed in another city. I needed to keep this in mind when making any changes, as it could have repercussions on other sites. The technicians are members of a domain group named SH_IS, which is then, a member of the domain's Server Operator group. The MIS Director is a member of the domain SH_IS group and Domain Admins group.

I had several objectives in mind when starting the security analysis.

- Confirm whether or not unauthorized monitoring of systems occurred from the MIS Department and ensure it did not continue if found.
- Confirm whether or not the facility network had security risks that would conflict with HIPAA regulations and eliminate/minimize any found.
- Confirm whether or not suspected unauthorized activities were being done by past/current MIS staff and eliminate/minimize any found.
- Ensure only authorized software usage on servers.
- Ensure proper documentation of servers, network, and critical applications.
- Ensure elevated accounts and rights were justified and documented.
- Ensure company MIS practices were being followed.
- Ensure the facility network is not vulnerable from the outside.

Little did I know what a Pandora's box would be opened and the shocking part was, that all the security risks were in plain site and should have been spotted before and addressed. Granted, it made my job of correcting them easier, but it also unsettled me, as I knew how the network and servers were when I left the company four years ago. It is amazing how little time it takes for all your hard work to fall into shambles and literally be thrown into the garbage. Previous documentation of the servers, all the software, a facility-wide software inventory system, network layouts, and MIS practices were disregarded and thrown away during my absence.

The Security Analysis

The first thing I did was reviewed elevated accounts and rights. I needed to know who my privileged users were and what level of accounts they had. The technicians were using a generic Server Operator-level account to do all their work. On top of not being able to audit any activities done under this account to a specific user, it also had a static, weak password (6 small letters, dictionary word). None of the computers are set to clear the last logged on user, so the name of this generic account could be seen throughout the facility as work was done on the computers. I immediately disabled this account, removed it from the SH_IS group, and set it to a very strong password. This would still allow audit trails to reflect this account's name, but keep any one from using it. I instructed the technicians to use their individual accounts in the future. Fortunately, all the NT and Windows 2000 computers were configured to have the SH_IS group in their local Administrator groups; removing the account from the domain SH_IS group effectively removed it from the local Administrator groups as well.

The technicians' reasoning for having the generic account is that users would forget to change the username on computers as they logged in, and it would lock the technician's accounts out if they had recently logged on to it. The technician

would then have to contact corporate IS to have the account unlocked, which could take hours to days to accomplish. While appreciating the inconvenience this could cause, the risk was not justified to save them occasional inconvenience. In addition, now that I was on-staff, I was a member of the Domain Admins group and could unlock the accounts as needed. Six months later, I have yet to have to unlock either of their accounts for this reason.

Another practice was to leave all the servers logged in under this generic Server Operator-level account – with no password protected screen saver activated on them! This left the servers extremely vulnerable. All one needed was physical access to the server room and one could do anything to the servers and the data and applications housed on them. I put an immediate stop to this practice. In addition, all servers were set to a password-protected screensaver activating after 2 minutes of inactivity.

Unfortunately, one of the servers runs an application for our beepers that can not run as a service, so an account has to stay logged on for the application to be available. Since this system also issues STAT beeps to our doctors, it was vital that it be available 24 x 7. I set up a user account for this program only to use and made it just a normal user account, restricted to logon to only this one server. I also started exploring other programs that could replace this beeper program and run as a service so no logon would be necessary for it to run properly. I decided to go with PageGate after running a trial version of it for 30 days. This purchase has been approved and will be installed by January 30, 2003.

This brought to light the physical security implications of the server room. It has a normal lock core and a button-punch locking mechanism, either of which will allow access. The combination on the punch lock had not been changed since I installed it 7 years ago. That means the other people who previously worked in the MIS department could still gain access to the server room if they came into the building. Not all of them left under the best of circumstances, so retaliation was a possibility. The punch combination was changed within the week and only told to staff authorized to enter the server room. Management can gain access as needed with their master key.

Other physical considerations for the server room were fire extinguishers, smoke detectors, and temperature/humidity monitoring equipment. None of these are present and should be considered part of the basic security needs of the room. Maintenance work orders have been submitted to have all three of these items installed in the server room and should be accomplished by January 30, 2003.

In addition to the server room's physical security, I noticed that many communication closets housing networking equipment were unsecured. I have requested our Maintenance Department to put locks on all of these as soon as

possible. Some are located in multi-use rooms, so these will need locked cabinets around them.

I then reviewed members of the SH_IS group and found some accounts that were created for services to run that were no longer installed on the network. Those were immediately removed from the group and disabled. This led me to review other generic user accounts associated to Springhills. I found many that were created for purposes that no longer existed. Others were needed, but undocumented. I documented those needed and disabled the others.

Next, I reviewed the servers for installed services and applications and compared that against their official functions, listed in Table 1. I also checked the various values in the Registry on each server that can initialize programs or services. Table 1 shows what was found and corrective steps taken to address identified issues.

Table 1 – Findings and Corrections of Initial Security Analysis of Servers

| Server Name | Official Function(s) | Findings and Corrections |
|---|---|---|
| Server1 | Backup Domain Controller | • Anti-virus program had not been updated since 1998; updated it and scheduled auto updates.<br>• Found remnants of several programs no longer used; uninstalled/deleted them.<br>• Found program to run broken CD Tower Server; uninstalled it and removed CD Tower.<br>• Found remnants of Surf Control program. Our facility does not own any licenses to this program; uninstalled it.<br>• No auditing activated; activated auditing. |
| Server2 | Personnel Software, Pager Software, Installation share (for MIS use only) | • Found several shares set to Everyone Full Access that were no longer needed; unshared and deleted them.<br>• Found remnants of a few programs no longer used; deleted/uninstalled them.<br>• Personnel Software was shared such that Everyone had Read access. This would allow anyone to connect to the share, install the client, and gain Read access to all Personnel information housed in the |

| | | |
|---|---|---|
| | | program. Created a domain group and added users of this program. Reset permission so only this group could gain access to this share.<br>• No auditing activated; activated auditing.<br>• Computer was left logged on 24 x 7 with a generic Server Operator-level account. Created a normal user account to be used temporarily so the Pager software could stay running 24 x 7. Set a strong password to the account and set a password-protected screensaver to 2-minute inactivity time. |
| Server3 | Specialized Hospital Software | • No auditing activated; activated auditing. |
| Server4 | RAS service, Print server, Backup Software, Intranet site | • The Intranet site initially used MS-IIS 2.0. In my 4 years absence, this was changed to LiteServe. The reason stated was "IIS is too insecure". LiteServe also offers FTP, Email, and Telnet services and its configuration was completely unsecured, making it an even higher risk than IIS would have been. I found evidence that an unauthorized person who has no business connection to the facility was granted access to LiteServe's FTP and Email service. FTP service was enabled although our facility has no need to host either sending or receiving FTP. I found evidence that a personal email server setup was attempted. The Intranet site was of little use to our users; it consisted of one static page listing links to other sites such as Reference Desk, The Weather Channel, etc. I obtained permission from management to take the Intranet site down until it could be properly developed and implemented. I documented unauthorized setup configurations and uninstalled LiteServe as it was a |

| | | |
|---|---|---|
| | | high security risk.<br>• Was using an unauthorized program called Macro Angel to schedule tasks to run; deleted this and moved scheduled tasks to the AT command.<br>• No auditing activated; activated auditing.<br>• Deleted remnants of 32 unauthorized programs including Remote Anything, Mail Direct, World Client, Email Guardian, Ikonboard, Jana Server and Neo Watch Monitor Service. Some of these may be connected to the unauthorized monitoring or unauthorized personal email servers. Also deleted Registry entries associated to them. Documented programs that may have been used in unauthorized activities.<br>• Found several shares with Everyone Full Access that were no longer needed; unshared them then deleted them.<br>• Documented all printers hosted on this server.<br>• Backup was using an unauthorized program called Nova Backup. In my previous employment at the facility, we used Seagate Backup Exec but it could not be found anywhere. Found ArcServe was the current standard and started purchase request for ArcServe.<br>• Used RASUSERS from the NT Resource Kit to review all accounts in the domain with RAS permissions. Scrutinized those at our facility and checked with management on accounts I suspected did not need this access. Removed RAS permission from 35 accounts determined not to need it.<br>• WINS service was active. Disabled it as all WINS on our domain are |

| | | |
|---|---|---|
| | | hosted on corporate servers.<br>• Found evidence of at least one illegally hacked program. It appears a trial version of this program was downloaded and posted hack was used to gain unlimited full use of the program. The hack was still on the server and it listed its source URL. Documented my findings and uninstalled the program as it was not related to a vital function. |
| Server5 | Home directories, departmental shares, patient data, DHCP server | • Has RAS service active; disabled it.<br>• NTFS permissions on patient data subfolders were incorrect. Under each patient name are approximately 20 subfolders, one for each department. Only the target department should have Change access to their folder, though all departments should have Read access to all subfolders. Current permissions allowed all departments Change access to all departments folders. I wrote a batch file to use to CACLS command to reset permissions of all department subfolders (approximately 4,000 total subfolders) granting Change access to only the department needing change access, Read only access to all other departments, and Full access to the SH_IS group.<br>• NTFS permissions of several user home directories were set incorrectly and allowed other users to access them. I reset the permissions on those home directories to allow just the specific user access.<br>• Found remnants of several programs no longer used; uninstalled/deleted them.<br>• No auditing activated; activated auditing.<br>• Found a personal email server installed. Documented its existence, disabled it, and reported my findings |

| | | |
|---|---|---|
| | | to management. Verbally warned technician not to use company equipment for personal use and uninstalled the program.<br>• Found remnants of LANauditor, Sniffer, GoverLAN and Site Scope, may have been used for the suspected unauthorized system monitoring by a previous employee. Management had given no permission for their use nor had any knowledge that they had been installed on company systems. Documented findings and deleted remnants.<br>• Server was using Server Check to ping all servers on a regular schedule and would notify technicians if a ping failed. While a good function, it was configured to use the personal SMTP server of one of the technicians. I deleted the program and will explore options to reimplement it using a business SMTP server to send notifications. |

These findings revealed many security issues:

- Physical security vulnerability of servers
- Virus vulnerability
- Data security poorly maintained and executed
- Unauthorized activities by current and/or former MIS Department employees
- No server auditing
- Unauthorized program installation and usage on critical servers
- No server maintenance as far as removing programs no longer needed
- No documentation of servers or programs ran on servers, or the configuration of the applications.
- Vulnerable paths for unauthorized users to gain access to facility systems and data.
- High-level account was left logged on unsecured systems.
- Password strength for high-level accounts is weak.
- Unnecessary services running on critical servers.

This confirmed management suspicions that facility servers were vulnerable and that unauthorized activities had and were taking place in the MIS Department,

though the acting MIS Director (one of the technicians) had assured them that everything was secure, above-the-board, legal, and by facility policy. This also brought to light that one of the technicians had issues with authority and following proper procedures. This was demonstrated by his actions of running personal email servers on company computers and his reasoning for using non-approved, unauthorized software instead of software available on the company's approved software list. When questioned as to why the unauthorized programs were being used to run vital functions, reasons given reflected the person's frustration at having a corporate office dictate what we could and could not use and an almost fanatical dislike of any Microsoft product. The purchase and subsequent use of these unauthorized products was not accomplished through approved purchasing practices. Other risks were addressed by taking corrective actions on the servers. The human risk is a bit trickier to address. In this case, it was addressed through our personnel system and the user has been restricted on what computers he can access and tasks he can perform.

Secondary tasks to ensure further infractions from the MIS Department do not occur include the following.

1. Auditing on all servers has been activated and is reviewed on a regular basis by the MIS Director. Any suspicious activities by any user are investigated and any unauthorized activities are immediately reported to management.
2. I am in the process of developing MIS Guidelines for standard tasks. This will ensure MIS staff knows what actions are expected of them for most tasks. This will also help ensure all MIS staff does standard tasks the same way, which will help ensure consistent results regardless of who performs the task. This will help keep a consistent setup on all computers and should reduce calls to the Help Desk as users move between workstations.
3. Physical access to servers and server room is restricted to me as MIS Director and an appointee. One technician has shown he is willing to act according to facility policy and has exhibited a high ethical conscious; he has been granted necessary access to perform basic server tasks in my absence.
4. Only the MIS Director will do any NTFS permission settings, as the technicians have not demonstrated sufficient understanding of how NTFS permissions work. The MIS Director will review NTFS permissions with them until they have a sufficient working understanding to be able to adjust them appropriately.

When I received a new copy of the facility policy/procedure manual, all MIS policies I had developed years ago were gone. I am currently developing these, using SANS' policy templates[1] as a quick starting point. Once completed, they will be presented to management for approval. We will also need to conduct user training on the new policies. According to a recent survey by SurfControl plc and NOP Research Group, "…75% of employees never receive formal

security training on how to use the Internet and e-mail at work in a way that minimizes network security problems…"[2]. As the article goes on to explain, it is difficult to expect users to follow policies they may not understand or understand the need for them. With the growing risks faced involving computer usage, it is imperative that users understand the risks involved in conducting business on computers and how breaches could negatively impact business and possibly even their jobs.

Lastly, I obtained permission from facility management and corporate IS to perform a port scan of our network, since this is one of the most popular ways for outside hackers to gain information to assist them in breaking into networks. Since Springhills is on a separate subnet from the rest of the company's domain, I could limit the scan to just our facility.

I downloaded a trial of GFI's LANguard Network Security Scanner. According to their web site,

> GFI LANguard Network Security Scanner (N.S.S.) is a tool that checks your network for all potential methods that a hacker might use to attack your network. By analyzing the operating system and the applications running on your network, GFI LANguard N.S.S. identifies possible security holes in your network. In other words, it plays the devil's advocate and alerts you to weaknesses before a hacker can find them, enabling you to deal with these issues before a hacker can exploit them. [3]

In order to get a scan from the outside world, I used my personal Internet connection from home to conduct the scan. It is important to note that many internet service providers (ISP's) monitor for scanning activity and it is against their usage policies to conduct scans without their prior permission[4]. Disregarding their usage policy could allow the ISP to terminate your account. I contacted my ISP and explained why I needed to perform a port scan. They requested I email this to them and was granted permission to conduct this scan.

What I found was almost as frightening as what I found on the servers. Our entire subnet was completely open to the Internet. All it would take is time for a hacker to stray upon our subnet. Given the fact that port scanners are freely available on the Internet and can reveal more than ample information for hackers to get their "foot in the door", this security hole needed to be addressed immediately. Table 2 shows what was discovered on Server5. Similar information was reported for the other servers as well.

Normally, if protected behind a firewall, a port scan should only return a response, letting the scanner know little more than the IP address is or is not responding to requests[5]. However, the firewall maintained by Springhills' corporate IS office is not very restrictive, and Table 2 shows just how much

information was able to be gathered by this common tool. Information has been sanitized to protect the confidential network information of the company.

Table 2 – Results of LANguard Network Scanner

```
Computer :  xxx.xxx.xxx.xx (xxx.xxx.xxx.xx)


 Computer  Details          Hostname  Username  Operating System
xxx.xxx.xxx.xx              SERVER5 SERVER5  Windows NT 4.0


xxx.xxx.xxx.xx  [ SERVER5 ]   ( Windows NT 4.0 )

 IP Address : xxx.xxx.xxx.xx
 HostName : SERVER5
 MAC : yy-yy-yy-yy-yy-yy (Compaq Computer Corp.)
 UserName : SERVER5
 LAN Manager : NT LAN Manager 4.0
 Domain : OurDomain
 Operating System : Windows NT 4.0
 Computer usage : NT/2k Member Server
 Service Pack 6
 Time to live (TTL) : 128 (128) - Same network segment

 NETBIOS names (6)
  SERVER5  -  Workstation Service
  OurDomain  -  Domain Name
  SERVER5  -  Messenger Service
  SERVER5  -  File Server Service
  OurDomain  -  Browser Service Elections
  SERVER5  -  Messenger Service

 Shares (14)
     ADMIN$  - Remote Admin
     IPC$  - Remote IPC
     C$  - Default share
     D$  - Default share
     Share1  -
     Share2  -
     Share3  -
     Share4  -
     Share5  -
     Share6  -
     print$  - Printer Drivers
     Share7  -
     Share8  -
```

```
        Users  -

    Groups (6)
        Administrators - Members can fully administer the computer/domain

        Backup Operators - Members can bypass file security to back up
    files
        Guests - Users granted guest access to the computer/domain
        Power Users - Members can share directories and printers
        Replicator - Supports file replication in a domain
        Users - Ordinary users

    Users (2)
       Administrator ( )
          FullName :
          Privilege : Administrator (*)
          Homedir :
          Comment : Built-in account for administering the computer/domain
          UserComment :
          ScriptPath :
          Workstations :
          Last Logon : 6 Oct 1999, 23:6:30
          Password age : 2 hours, 18 minutes, 25 seconds
          # Logons : 4
          Bad Passwords Count : 0
       Guest ( )
          FullName :
          Privilege : Guest
          Flags : ACCOUNT_DISABLED ,
PASSWORD_CANNOT_BE_CHANGED
          Homedir :
          Comment : Built-in account for guest access to the
    computer/domain
          UserComment :
          ScriptPath :
          Workstations :
          Last Logon : never
          Password age : 1024 days, 14 hours, 29 minutes, 51 seconds
          # Logons : 0
          Bad Passwords Count : 0

    Services (30)
        awhost32 - pcAnywhere Host Service
        BROWSER - Computer Browser
        CPQNicMgmt - Compaq NIC Management Agents
        CPQRCMC - Compaq Remote Monitor Service
```

CpqWebMgmt - Insight Web Agent
CQIMDSVC - Compaq Enhanced IMD Idle Screen
CqMgHost - Insight Host Agents
CqMgServ - Insight Server Agents
CqMgStor - Insight Storage Agents
DHCPServer - Microsoft DHCP Server
EventLog - EventLog
LanmanServer - Server
LanmanWorkstation - Workstation
LmHosts - TCP/IP NetBIOS Helper
McShield - Network Associates McShield
McTaskManager - Network Associates Task Manager
MESSENGER - Messenger
NETLOGON - Net Logon
NtLmSsp - NT LM Security Support Provider
PlugPlay - Plug and Play
ProtectedStorage - Protected Storage
RasMan - Remote Access Connection Manager
RPCLOCATOR - Remote Procedure Call (RPC) Locator
RpcSs - Remote Procedure Call (RPC) Service
SNMP - SNMP
SPOOLER - Spooler
SysDown - Compaq System Shutdown Service
TapiSrv - Telephony Service

Network devices (5)
\Device\NetBT_N1001 (ww-ww-ww-ww-ww-ww)
\Device\NetBT_N1001 (ww-ww-ww-ww-ww-ww)
\Device\NwlnkIpx (ww-ww-ww-ww-ww-ww)
\Device\NwlnkNb (ww-ww-ww-ww-ww-ww)
\Device\Nbf_N1001 (ww-ww-ww-ww-ww-ww)

Local Drives (4)
A:
C:
D:
E:

Remote TOD (time of day)
Time of day : 8 Aug 2002 , 1:58.20 , GMT - 4
UpTime : 2 days, 3 hours, 40 minutes, 5 seconds

Password policy
Minimum password length : 8 chars
Maximum password age : 0 days
Minimum password age : no delay

```
        Force logoff : never force
        Password history : no history

    Registry
        RegisteredOwner : MIS
        RegisteredOrganization : SERVER5
        ProductName : SERVER5
        CurrentBuildNumber : 1381
        CurrentType : Uniprocessor Free
        CurrentVersion : 4.0
        PathName : C:\WINNT
        ProductId : 11111111111111111111
        SoftwareType : SYSTEM
        SourcePath : D:\i386\
        SystemRoot : C:\WINNT
        VendorIdentifier : GenuineIntel
        Identifier : x86 Family 6 Model 7 Stepping 3
        ~MHz : 498
        Physical Memory : 256 MB
        Display : ATI Technologies Inc. 3D RAGE IIC

        Run (4)
            SYSTEMTRAY=SYSTRAY.EXE
            SHSTATEXE="C:\PROGRAM FILES\NETWORK
ASSOCIATES\NETSHIELD 2000\SHSTAT.EXE" /STANDALONE

        HotFixes (1)
            Q147222

    SNMP info (system)
      sysDescr : Hardware: x86 Family 6 Model 7 Stepping 3 AT/AT
COMPATIBLE
   - Software: Windows NT Version 4.0 (Build Number: 1381 Uniprocessor
Free )

      sysUpTime : 2 days, 3 hours, 39 minutes, 4 seconds
      sysName : SERVER5
      Vendor : Microsoft

    Open Ports (4)
        53 [ Domain => Domain Name Server ]
        135 [ epmap => DCE endpoint resolution ]
        139 [ Netbios-ssn => NETBIOS Session Service ]
        5631 [ pcANYWHEREdata => Remote Control Software ]

    Alerts (12)   (Legend :   - High   - Medium   - Low   - Information)
```

```
    Service_Alerts (2)
        Administrator account exists
          Description : It is recommended to rename this account
        User Guest ( ) never logged on
          Description : It is recommended to remove this account if not
used

    Registry_Alerts (10)
        A modem is installed on this computer
            Description : Modems can be a network security threats
                  because they allow insiders to make unfiltered connections


                  using the telephone system
        AutoShareServer (1)
            Description : The administrative shares (C$,D$,ADMIN$,etc)
                  are created on this machine.If you don't use them set


                  AutoShareServer to 0 to stop creating this shares
          Bugtraq ID/URL :
http://support.microsoft.com/support/kb/articles/Q245/1/17.asp
        Cached Logon Credentials
            Description : Could lead to information exposure. Should be
                  set to 0
          Bugtraq ID/URL :
http://archives.indenial.com/hypermail/ntbugtraq/1998/April1998/0003.html

        DCOM is enabled
            Description : DCOM is used to execute code on remote
                  computers.Should be disabled if not used.
          Bugtraq ID/URL :
http://support.microsoft.com/support/kb/articles/Q158/5/08.asp
        Fragmented IGMP Packet
            Description : It is possible to crash a system by sending a
                  fragmented IGMP packet
          Bugtraq ID/URL : 514
        Last logged-on username visible
            Description : By default, NT/2k displays the last logged-on
                  user
          Bugtraq ID/URL :
http://support.microsoft.com/support/kb/articles/q114/4/63.asp
        LM Hash
            Description : It is recommended to use NTLM authentification
                  instead of LM
```

Bugtraq ID/URL :
http://support.microsoft.com/support/kb/articles/q147/7/06.asp
Malformed LSA Request
Description : A malformed LSA request can cause the system to stop responding
Bugtraq ID/URL :
http://www.microsoft.com/technet/security/bulletin/ms99-020.asp
NetBIOS Name Server Protocol Spoofing
Description : Custom crafted packets can cause NETBIOS Name Service to stop responding
Bugtraq ID/URL :
http://www.microsoft.com/technet/security/bulletin/ms00-047.asp
Spoofed LPC Port Request
Description : A malicious user can gain SYSTEM privileges
Bugtraq ID/URL :
http://www.microsoft.com/technet/security/bulletin/ms00-003.asp

Wednesday, 7 August 2002 - 09:59 PM

Generated by LANguard Network Scanner v(2.0)
Copyright © 2001 GFI Software Ltd.
http://www.languard.com/

From this simple scan, you can tell Server5 is a Compaq Server running NT4, service pack 6. One of the shares shown is the user's home directory root share – a prime target for hackers. You can also see Compaq installed a system shutdown service that is running. Now what would it take to send a shutdown command to this server? An administrator account. You have a list of local account names and you can see which ones are Administrators. That is half of the information needed to logon! Now all you need is to hack away at this account's password. The scan shows you that there is a modem attached. Now you have another way to access the network without even being physically on-grounds. LANguard even goes as far as identifying security weaknesses, making it even easier for a would-be-hacker to know exactly what methods can be exploited on this system to gain access to it. You can see the server uses LM hashes for authentication. Now you can use a sniffer program to grab the password and hack it at your leisure.

LANguard identified another security flaw that can be utilized to gain Administrator-level access to this server. In the list of services is "CpqWebMgmt - Insight Web Agent". By doing a simple web search engine search, I was able to quickly locate a known problem with this web agent – "Compaq Web-enabled Management Software Buffer Overflow"[6]. If the patch has not been applied, I could use this exploit to remotely gain Administrator access to the server through any Internet browser. From my house, I was able to connect anonymously to this server and bring up the Compaq Web-Based Management screen. In addition to

seeing various settings on the server, I could also click on the Login button and attempt to logon to the server under the Administrator account without it being logged in the server's Security Event Log.

The next few weeks were spent fixing identified weaknesses, documenting what was done, and double-checking the results. Another step in fixing our exposure to the outside world was to request we be moved to a private IP address range. I completed the necessary forms, documented all hard-coded IP nodes, and planned the change over. By moving to a private IP range, we would effectively be hidden from everyone outside our domain. Connection to the Internet would be accomplished by a NAT server at our corporate office. Within two weeks, our entire facility network was moved to the assigned private IP range and the majority of our exposure paths to the outside were eliminated.

Conclusions

The security analysis confirmed all of management's suspicions. Unauthorized monitoring of systems appeared to have been done but was not currently happening. The facility network had many security risks that would have kept our network from being HIPAA compliant. Unauthorized activities were being performed by past/current MIS staff.

Finding remnants of so many network and system monitoring programs (Surf Control, Remote Anything, LANauditor, Sniffer, GoverLAN and Site Scope) infers that some sort of monitoring had occurred or at least had been attempted in the past. However, none of these programs were fully installed on any of the servers audited, only remnants that were not cleaned up after an uninstall. This indicated that current monitoring was not occurring. While there are valid reasons for having any of these programs, Springhills does not hold licenses for any of these programs and management had given no permission for their use, so any monitoring done with these programs was unauthorized. It was believed a previous employee, not a current employee, had installed these programs. At this point, the only necessary action was to remove the remaining bits and pieces of these programs.

All the security risks on the servers were addressed quickly. Moving to the private IP range took care of most of our exposure paths to the outside. We still have RAS enabled on one of the servers, but corporate IS recently adopted VPN (virtual private networking) as its preferred method of remote access for users. VPN accounts have been requested and granted for all remote users at our facility and they will be moved to VPN as soon as possible. Once this is accomplished, RAS will be eliminated from the facility server and that exposure path will be eliminated. Until then, RAS has been configured to use "call back" to further ensure the authentication of RAS users.

Unauthorized activities of past MIS staff have been disseminated to management for reference. Current MIS staff are aware that the company has decided to actively monitor MIS staff activity and expectations have been clearly identified. Any questionable activities are immediately investigated and any forbidden activities will be addressed through our personnel system.

Following is the list of objectives I had when starting this security analysis and their status to-date:

- Confirm whether or not unauthorized monitoring of systems occurred from the MIS Department and ensure it did not continue if found – found and documented evidence, complete.
- Confirm whether or not the facility network had security risks that would conflict with HIPAA regulations and eliminate/minimize any found – found and documented, corrected as found, on-going.
- Confirm whether or not suspected unauthorized activities were being done by past/current MIS staff and eliminate/minimize any found – found and documented evidence, complete.
- Ensure only authorized software usage on servers – eliminated all unauthorized software from servers. Most have been replaced with approved software packages; PageGate is the only program installation pending and that is only awaiting software delivery from the vendor. Estimated completion date: January 30, 2003.
- Ensure proper documentation of servers, network, and critical applications – current to-date, on-going.
- Ensure elevated accounts and rights were justified and documented – complete.
- Ensure company MIS practices were being followed – developing policies. Estimated completion date: February 28, 2003.
- Ensure the facility network is not vulnerable from the outside – eliminated most known vulnerabilities. In the process of replacing RAS modems with VPN solution. On-going.

Within six months of the initial security analysis, Springhills' network has seen a marked improvement in network security. However, security continues to be an ongoing task. Now that immediate security risks have been addressed, we are moving on to being proactive rather than reactive in our approach to security. A first step in this direction is to purchase a firewall to be installed locally at Springhills so we can further protect ourselves from vulnerabilities from the outside, such as through ports we do not need. We are also evaluating software-based IDS programs as an added layer of defense. There is still much work ahead, but we now at least have a solid base on which to build.

---

[1] SANS Institute Resource. "The SANS Security Policy Project." URL: http://www.sans.org/newlook/resources/policies/policies.htm (12 December 2002).

[2] Migliore

[3] GFI. "GFiLANguard Network Security Scanner Overview." URL: http://www.gfi.com/lannetscan/index.htm (12 December 2002).

[4] ConnectNC. "Acceptable Use Policy." URL: http://www.connectnc.com/policy/policy.php (13 December 2002).

[5] ITWorld.com. "Tapping on the Walls." Unix Insider. 17 November 2000. URL: http://www.itworld.com/Comp/1423/swol-1117-buildingblocks (13 December 2002).

[6] CIAC. "Compaq Web-enabled Management Software Buffer Overflow." The US Department of Energy Computer Incident Advisory Capability Information Bulletin. L-042. 7 February 2001. URL: http://ftp.cerias.purdue.edu/pub/advisories/ciac/l-fy01/l-042.Compaq.Web.Enabled.Management.Software.Buffer.Overflow.txt (13 December 2002).

List of References

CIAC. "Compaq Web-enabled Management Software Buffer Overflow." The US Department of Energy Computer Incident Advisory Capability Information Bulletin. L-042. 7 February 2001. URL: http://ftp.cerias.purdue.edu/pub/advisories/ciac/l-fy01/l-042.Compaq.Web.Enabled.Management.Software.Buffer.Overflow.txt (13 December 2002).

ConnectNC. "Acceptable Use Policy." URL: http://www.connectnc.com/policy/policy.php (13 December 2002).

GFI. "GFiLANguard Network Security Scanner Overview." URL: http://www.gfi.com/lannetscan/index.htm (12 December 2002).

ITWorld.com. "Tapping on the Walls." Unix Insider. 17 November 2000. URL: http://www.itworld.com/Comp/1423/swol-1117-buildingblocks (13 December 2002).

Jamieson, Shaun. "The Ethics and Legality of Port Scanning." 8 October 2001. URL: http://rr.sans.org/audit/ethics.php (16 December 2002).

Migliore, Matt. "Survey Reveals Holes in E-Mail and Internet Monitoring Strategy." Security Strategies. 11 December 2002. URL: http://www.esj.com/news/article.asp?EditorialsID=353 (16 December 2002).

Nutter, Ronald. "Planning for TCP/IP Implementation." Windows NT Administrator Report. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winntas/tips/techrep/tcpimp.asp (12 December 2002).

Perception. "Perception LiteServe." URL: http://www.cmfperception.com/liteserve.html (12 December 2002).

SANS Institute Resource. "The SANS Security Policy Project." URL: http://www.sans.org/newlook/resources/policies/policies.htm (12 December 2002).