Audit of a Corporate Security Systems Domain Controller

Steve Graham
November 12, 2004

GSNA Practical Version 3.2
Option 1

Abstract

The following is a technical audit of a Corporate Security Systems Domain Controller. This audit will begin by researching information about the system. It will provide a risk evaluation and review some current states of practice. Following this will be a check list, the audit itself and a report.

The purpose of this audit is to assess the vulnerabilities and risk levels of this security systems server and to provide recommendations and a comprehensive report detailing the findings.

Table of Contents

System Research and Risk Evaluation

Company Information and Overview

The company this audit is focused on develops hardware for the semi-conductor industry. The manufacturing and servicing of this hardware required this company to decentralize its operation. With this organizational model it becomes difficult to monitor and enforce many of the companies policies and procedures. Applying building security systems to this model is an equally challenging task.

Although networked security systems have been around for a few years they are still relatively new. However, it is becoming increasingly more common for mid to large size organizations to rely almost completely on network based technology to secure their physical and (at times) intellectual property. Some organizations use a single security application that incorporates digital video recorders with access control and security alarm systems. Others use individual applications for each security system. The one key focus they all have in common is their primary form of communication, “The Network.” It is true that many security systems have the ability to use a phone dialer as a backup to the network, but often times these connections are slow and unpredictable.

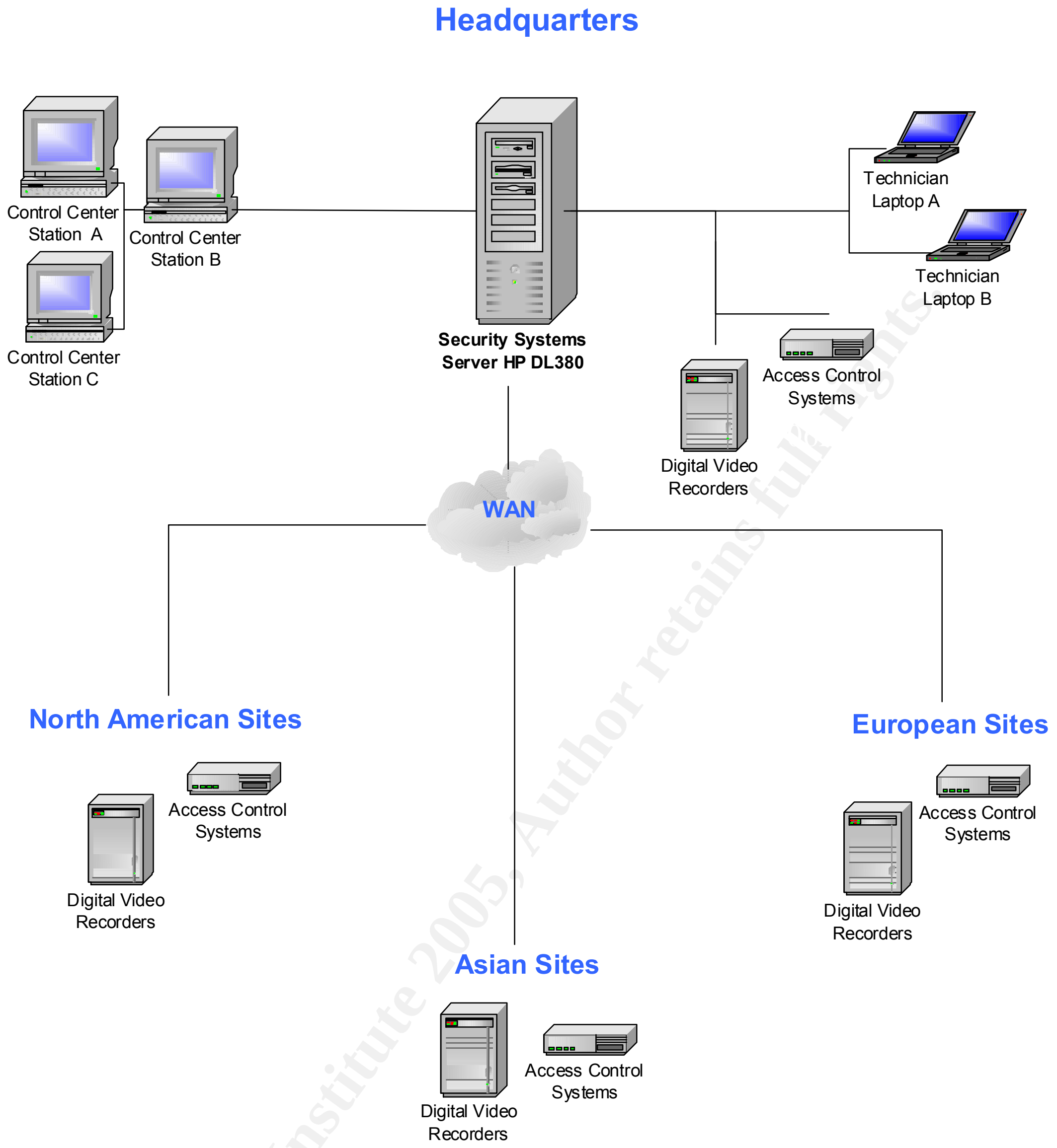
With limited budgets and shared network recourses it is not uncommon to find security system servers that have multiple rolls. Such is the case with the security server this audit is focused on.

Target Systems Organizational Role

The target of this audit is a single HP ProLiant DL380 server running Windows 2000 Server with Service Pack 4 (see below):

Item	**Value**
OS Name	*Microsoft Windows 2000 Server*
Version	*5.0.2195 Service Pack 4 Build 2195*
OS Manufacturer	*Microsoft Corporation*
System Name	*----------------------------*
System Manufacturer	*HP*
System Model	*ProLiant DL380 G3*
System Type	*X86-based PC*
Processor	*x86 Family 15 Model 2 Stepping 7 GenuineIntel ~2389 Mhz*
Processor	*x86 Family 15 Model 2 Stepping 7 GenuineIntel ~2389 Mhz*
Processor	*x86 Family 15 Model 2 Stepping 7 GenuineIntel ~2389 Mhz*
Processor	*x86 Family 15 Model 2 Stepping 7 GenuineIntel ~2389 Mhz*
BIOS Version	*01/31/03*
Windows Directory	*C:\WINNT*
Locale	*United States*
Time Zone	*Pacific Daylight Time*
Total Physical Memory	*2,096,660 KB*
Available Physical Memory	*87,196 KB*
Total Virtual Memory	*6,132,204 KB*
Available Virtual Memory	*2,087,604 KB*
Page File Space	*4,035,544 KB*

This machine plays several roles ***(see figure 1).*** It runs the access control head end application, network monitoring applications and is the Domain Controller for the entire security systems global network. This domain controller is utilized by a 24 hour Security Operations monitoring group including several technicians. It also supports 25 or more Digital Video Recorders and 30 or more access control sites. This server provides services and applications to internal users only.



Network Diagram Figure 1

Risk Evaluation

Perhaps the main role and certainly one of the most important functions of this Server is its management of the communications for the security domain as the Domain Controller. As the root of the forest for this security domain this stand alone server provides the DNS and WINS service in conjunction with the Global Catalog which makes it versatile yet vulnerable as the only DC (Domain Controller) supporting this security domain. On closer inspection a number of risks are associated with this particular network scenario and certainly apply to the server targeted for this audit.

First we should take a look at what defines a Risk and how it will be identified throughout the remainder of this audit. In basic terms we are creating a Risk when we allow an Exposure to exist. When we add Vulnerability to a Threat we get Exposure:

Vulnerability + Threat = Exposure

Exposure Figure 1.2

With this in mind we will take a look at these elements and how they affect the target of our assessment.

Threats

Threat	Description	Capacity to Cause Damage
1. Malicious Code	Attack from malicious code such as Add-Ware, Spy-Ware or Computer Virus	**High** – The introduction of malicious code to this system could allow a virus or some form of malware to gather confidential information and/or completely destroy critical programs, services and databases
2. Unauthorized Access	The ability of an unauthorized person to gain access to the Server	**High** – The ability to gain access to the system through a network share, remote software or direct access using unauthorized credentials could potentially allow the unauthorized user full control of all security systems
3. Power Outage	Power loss to system and/or redundant power supply failure	**High** – A power loss to this system would cause the Security Control Center to be blind to potential breaches in the physical security systems of the corporation and for the duration would render Security helpless
4. Damage or Theft	The ability for unauthorized personnel to access the physical system with the	**High** – Damage or Theft of this system would not only destroy all centralized security support

	intent to steal or damage	for the corporation involving Access Control, Alarm Conditions and Digital Video Surveillance, but would introduce the possibility of a new threat utilizing the newly acquired data and information resident on the system to remotely compromise all security systems
5. Permissions Abuse	Users who are granted permissions above their needs have the ability to compromise the security structure of the server and create vulnerabilities	**High** – Users with elevated privileges could pose a number of threats from the accidental (Database Corruption) to the malicious (unlocking all card access doors to a highly secured area)

Vulnerabilities

Vulnerability	Degree of Exposure	Potential Impact
1. Insufficient Patch or Update management Process	***High***	Systems Services may fail to execute or become corrupt. Data could also become corrupt or acquired through Adware/Spyware. Organization could be severely crippled.
2. No Password Protected screen savers on Server	***High***	If a user with administrative privileges were to log on to a Server in a multi-user Server Room environment and forget to log off another user with mal-intent could completely compromise the security systems.
3. Easily Guessable Passwords (Server Policy does not enforce Passwords to meet complexity requirements)	***High***	Once the credentials have been appropriated and a successful logon attempt has been made full authoritative access will be given to the user. The potential impact to the organization could be severe.
4. Minimum UPS standby time	***Medium***	A prolonged power loss could exhaust the backup power of the UPS causing the server to

		go offline and security controls rendered useless.
5. Unused or Missing Redundant Power Supply	***Medium***	In the event the primary power supply of the server fails and the secondary power supply is unavailable the server will go offline and security controls will be rendered useless.
6. Server stored in unsecured location	***High***	If the server becomes damaged or falls victim to theft the organization stands to lose full control of security systems as well as critical data.
7. Elevated Permissions	***High***	A user with high enough credentials would have the ability to completely compromise the security systems server and all data within.
8. Open Shares	***High***	Through Open Shares a user can easily gain access to confidential data as well as control the server remotely.
9. Remote Desktop Applications	***High***	If a user gained access through a Remote Desktop Application they could potentially have as much control of the system as if they were sitting in front of it. If an administrator did not log off or lock the system the remote user could cause sever damage to the organization.

The Security Systems domain controller directly affects several areas of the organization. Some of these areas reach beyond the security group. Some of these groups operations are almost solely dependant on the data and function of this server. Below is a list of the assets this server brings to the Corporation:

Assets

Asset	Description
1. Control Room Operator (Access Control and Digital Video Data)	Security Control Room Operators rely heavily on the data from this server to Manage building access and Digital Video for the company globally

2. Investigator Data	Investigators use the data from this server as a key tool that provides information from the access control system as well as assisting in the retrieval of archived (time and date stamped) video clips.
3. Badge Office Data	The Badge Office is constantly updating and modifying the Access Control user database located on this server
4. Human Resources Data	Human Resources utilizes this access control server for the formal activation and deactivation of access badges for the company.
5. Building Physical Security	The Security Systems Domain Controller is the nerve center for all electronic security for the company worldwide. Security relies heavily on the functions of this server to extend their reach and enable them to physically secure all business offices around the globe.

Current State of Practice

In support of this audit you will find a list of sources below that have been or can be used as a reference during this process.

Resource	Comments
1. Securing Windows 2000 Server http://www.microsoft.com/downloads/details.aspx?FamilyID=9964cf42-e236-4d73-aef4-7b4fdc0a25f6&DisplayLang=en	Excellent Comprehensive resource and analysis tools from Microsoft itself including a Test, Delivery and Support Readiness Guide.
2. National Security Agency (Security Recommendation Guidelines for Windows 2000) http://nsa1.www.conxion.com/win2k/download.htm	Good reference and gives you a peak at what the NSA is doing (recommending) to secure Windows 2000

3. Securing Windows 2000 Server (Sans) http://www.sans.org/rr/whitepapers/win2k/189.php	Gives you a decent overview on Securing Windows 2000 Server and some good basic guidelines on securing the file system, share permissions, etc.
4. Protect Against Weak Authentication Protocols and Passwords http://www.windowsecurity.com/articles/Protect-Weak-Authentication-Protocols-Passwords.html	A great look at Authentication Protocols in depth (from the oldest to the latest)
5. Auditing Windows 2000 http://www.winnetmag.com/Articles/Print.cfm?ArticleID=9633	This article reviews the Windows 2000 Auditing Categories and the Audit Policy. To see the Figures you must click on the hyperlinks.
6. UCB Windows 2000 Server Security Guidelines http://www.colorado.edu/its/windows2000/adminguide/w2ksecguidelines.html	These guidelines are primarily set for File and Print Servers, but have been a good source of information.
7. Auditing the Corporate Access Control System: An independent Auditor's Perspective http://www.giac.org/practical/GSNA/Scott_Steiner_GSNA.pdf	A very good and thorough Audit of a Corporate Access Control System.
8. 5-Minute Security Advisor - Basic Physical Security http://www.microsoft.com/technet/community/columns/5min/5min-203.mspx	Good guidelines on Auditing the Physical Security

The Security Systems Audit Checklist

Check that the Server is Physically Secured

Item 1	Data/Comments
Reference	Microsoft 5-Minute Security Advisor - Basic Physical Security http://www.microsoft.com/technet/community/columns/5min/5min-203.mspx

Risk	- Too often companies spend a great deal of time and money securing their Network when their greatest vulnerability could be the theft of the computer itself. - **Vulnerability** addressed is number 6. Server stored in unsecured location - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *High*
Testing Procedure	- Locate and Visit the facility where the server is housed - Verify that access to the room is controlled and that only required personnel can gain access - Verify that the server is in a locked server cabinet/rack
Test Nature	- Objective
Evidence	
Findings	

Check for the existence of Open Shares

Item 2	**Data/Comments**
Reference	UCB Windows 2000 Server Security Guidelines http://www.colorado.edu/its/windows2000/adminguide/w2ksecguidelines.html#physical Chapter 2.D ii & iii
Risk	- One of the most common ways an intruder can gain access to a computer is through an open share. - **Vulnerability** addressed is number 8. Open Shares - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data - **Likelihood** that a threat could exploit this vulnerability: *High*
Testing Procedure	- Locate server and log on as a domain user - Right click on the My Computer Icon - Left click on Manage - In Computer Management under System tools click on "Shared Folders" then click on Shares - Verify there are no Unauthorized/Open shares
Test Nature	- Objective
Evidence	
Findings	

Password Protected Screen Saver Enabled

Item 3	Data/Comments
Reference	I have referenced Personal Experience for this Checklist Item. In my experience you may come across someone remotely logged on to a server by simply traversing through the control console (switchbox)
Risk	- If an administrator walked away from a system and did not log off or lock it “and” a Password Protected Screen Saver was not enabled anyone local or remote could take control of that system. - **Vulnerability** addressed is number 2. No Password Protected screen savers on Server - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *High*
Testing Procedure	- Locate server and log on as a domain user - Right click on the desktop and select properties - Under display properties select screen saver - Verify that a screen saver is selected and that the Password Protected button is checked - Also verify that the Wait time is set no longer than 15 minutes
Test Nature	- Objective
Evidence	
Findings	

Check that “Passwords must meet complexity policy” is enabled

Item 4	Data/Comments
Reference	Protect against weak Authentication Protocols and Passwords http://www.windowsecurity.com/articles/Protect-Weak-Authentication-Protocols-Passwords.html
Risk	- An easily guessable password has the potential to allow an intruder full access to that system. Forcing users to create a complex password greatly reduces that risk. - **Vulnerability** addressed is number 3. Easily Guessable Passwords (Server Policy does not enforce Passwords to meet complexity requirements) - **Assets** affected by a successful exploitation are:

	1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *Medium*
Testing Procedure	- Locate server and with a Domain Admin present log on as a domain administrator - Click on Start, Programs, Administrative Tools and Active Directory Users and Computers - Right click on the server you want to administer and select properties - Under the Server Properties select group policy - In the list of Policy Object links Double click "Default Domain Policy" - Under Computer Configuration select Windows Settings, Security Settings, Account Policies and Password Policies - Verify that "Passwords Must Meet Complexity Requirements" is enabled
Test Nature	- Objective
Evidence	
Findings	

Verify UPS Configuration

Item 5	Data/Comments
Reference	I have referenced Personal Experience for this Checklist Item. The UPS backup units are often overlooked in the way of maintenance and may be unable to support the devices connected to it for very long if at all.
Risk	- Server Up-time is critical to the functionality of several groups. If a server is on a failing UPS and there is a power loss the organization will suffer greatly. - **Vulnerability** addressed is number 4. Minimum UPS standby time - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *Medium*
Testing	- Locate room where server is housed

Procedure	- Identify UPS Power device - Verify at least one of the two power cables are plugged into the UPS - Check the make/model and power capabilities of the UPS - Verify the unit is in good working condition
Test Nature	- Objective and Subjective
Evidence	
Findings	

Are both Server power supplies connected and operational

Item 6	**Data/Comments**
Reference	I have referenced Personal Experience for this Checklist Item. Overcrowded Server Rooms and inadequate power distribution may result in the deployment of a server utilizing only one of its two power supplies.
Risk	- Up-time will once again be affected by a failed power supply. For servers with dual power supplies this risk can be greatly reduced and up-time can be retained if the second power supply is connected and operational. - **Vulnerability** addressed is number 5. Unused or Missing Redundant Power Supply - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *Medium*
Testing Procedure	- Locate Server and power connections (typically on back of unit) - Verify that both power cables are connected to server power supplies - Verify that power indicator lights are lit on both power supplies and their status is "good"
Test Nature	- Objective
Evidence	
Findings	

Verify Patch or Update management process

Item 7	**Data/Comments**
Reference	Securing Windows 2000 Server (Sans) http://www.sans.org/rr/whitepapers/win2k/189.php
Risk	- An un-patched system connected to a network is

	extremely vulnerable to viruses and mal-ware. Insuring there is a good process in place to manage patches and updates will decrease the vulnerability level of the system. - **Vulnerability** addressed is number 1. Insufficient Patch or Update management Process - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data - **Likelihood** that a threat could exploit this vulnerability: *High*
Testing Procedure	- Locate and interview the Administrator for the target system - Verify the existence of policies and procedures outlining the Patching and Updating process - Locate server and with a Domain Admin present log on as a domain administrator - Click on Start, Control Panel and then "Add/Remove programs" - Under "Change or Remove Programs" Identify All Microsoft Updates, Hot Fixes and Service packs - Compare these against the latest versions on the Microsoft Security Updates Bulletins Page http://www.microsoft.com/security/bulletins/default.mspx - Verify that all applicable patches are installed and current
Test Nature	- Objective and Subjective
Evidence	
Findings	

Does the Server have Remote Desktop Applications

Item 8	Data/Comments
Reference	UCB Windows 2000 Server Security Guidelines http://www.colorado.edu/its/windows2000/adminguide/w2ksecguidelines.html#filesystem Chapter 4.C

Risk	- It is important to check for the presence of remote desktop applications. They are simply another common access point that can be exploited. - **Vulnerability** addressed is number 9. Remote Desktop Applications - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *High*
Testing Procedure	- Locate server and with a Domain Admin present log on as a domain administrator - Click on Start, Control Panel and then "Add/Remove programs" - Under "Change or Remove Programs" Identify any Remote Desktop Applications - Under "Add or Remove Windows Components" Identify any Remote Desktop Applications
Test Nature	- Objective
Evidence	
Findings	

Do the Remote Desktop Applications require passwords

Item 9	**Data/Comments**
Reference	UCB Windows 2000 Server Security Guidelines http://www.colorado.edu/its/windows2000/adminguide/w2ksecguidelines.html#filesystem Chapter 4.C
Risk	- Many remote desktop applications offer the ability to remotely gain access to another desktop "without" logging onto the application itself. Presenting the password protection on the remote desktop application adds an additional layer of security that may stop an intruder from gaining full access to the remote computer. - **Vulnerability** Addressed is number 9. Remote Desktop Applications - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security

	- **Likelihood** that a threat could exploit this vulnerability: *<u>High</u>*
Testing Procedure	- Locate server and with a Domain Admin present log on as a domain administrator - Identify Remote Desktop Applications - Launch the Host program (program on the server that allows remote access) and look for Password Protection Options - Verify that the option is enabled
Test Nature	- Objective
Evidence	
Findings	

Check Remote Desktop Application User Administration Process

Item 10	**Data/Comments**
Reference	UCB Windows 2000 Server Security Guidelines http://www.colorado.edu/its/windows2000/adminguide/w2ksecguidelines.html#filesystem Chapter 4.C
Risk	- Although a remote desktop application may be password protected it could still fall victim to a free and open administration process. If anyone can give anyone a username and password we greatly reduce the efficiency of this layer of security. - **Vulnerability** addressed is number <u>9. Remote Desktop Applications</u> - **Assets** affected by a successful exploitation are: <u>1. Control Room Operator Access Control and Digital Video Data</u> <u>2. Investigator Data</u> <u>3. Badge Office Data</u> <u>4. Human Resources Data</u> <u>5. Building Physical Security</u> - **Likelihood** that a threat could exploit this vulnerability: *<u>High</u>*
Testing Procedure	- Locate server and with a Domain Admin present log on as a domain administrator - Identify Remote Desktop Applications - Launch the Host program (program on the server that allows remote access) and look for User Account Administration (the ability to create accounts for remote users) - Verify the correct Administrator(s) have the only accounts with the ability to create other accounts and/or modify privileges - Locate and interview the Administrator for the target system - Verify the existence of policies and procedures outlining the

	Remote Desktop account creation, modification and deletion process
Test Nature	- Objective and Subjective
Evidence	
Findings	

Check Global Catalog User and Computer Administration Process

Item 11	**Data/Comments**
Reference	I have referenced Personal Experience for this Checklist Item. Administrators may create additional user accounts for testing or other purposes. Without a strict process and auditing this can create a great vulnerability.
Risk	- An open or unrestricted administration process could quite possibly be the weak link in the "security" chain. The network can be secured very well, but if anyone can easily acquire administrative or elevated permissions then the security structure is greatly weakened. - **Vulnerability** addressed is number 7. Elevated Permissions - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *High*
Testing Procedure	- Locate and interview the Administrator for the target system - Verify the existence of policies and procedures outlining the user/computer account creation, modification and deletion process
Test Nature	- Subjective
Evidence	
Findings	

Verify the existence of Antivirus Software

Item 12	**Data/Comments**
Reference	Auditing the Corporate Access Control System: An independent Auditor's Perspective http://www.giac.org/practical/GSNA/Scott_Steiner_GSNA.pdf Item 9

Risk	- Antivirus Software is often the main defense against intrusions from computer viruses and other Malware. - **Vulnerability** addressed is number 1. Insufficient Patch or Update management Process - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *High*
Testing Procedure	- Locate server and with a Domain Admin present log on as a domain administrator - Click on Start, Control Panel and then “Add/Remove programs” - Under “Change or Remove Programs” Identify any Antivirus Software Applications
Test Nature	- Objective
Evidence	
Findings	

Check that Antivirus Application is set to Auto Update

Item 13	Data/Comments
Reference	Auditing the Corporate Access Control System: An independent Auditor’s Perspective http://www.giac.org/practical/GSNA/Scott_Steiner_GSNA.pdf Item 9
Risk	- An update process must be in place to insure the Antivirus software is being updated often. We are checking to see that the Automatic updates feature is enabled on this system. - **Vulnerability** addressed is number 1. Insufficient Patch or Update management Process - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *High*
Testing Procedure	- Locate server and with a Domain Admin present log on as a domain administrator

	- Identify Antivirus Software Application(s) - Launch the Antivirus program and search for the option/configuration setting that allows the software to auto-update - Verify this option is enabled
Test Nature	- Objective
Evidence	
Findings	

Check that Antivirus Virus Definitions are up to date

Item 14	Data/Comments
Reference	Auditing the Corporate Access Control System: An independent Auditor's Perspective http://www.giac.org/practical/GSNA/Scott_Steiner_GSNA.pdf Item 9
Risk	- Although a system may have an Antivirus application installed if the virus definitions are not up to date any number of recently created viruses or malware can still attack a system. - **Vulnerability** addressed is number 1. Insufficient Patch or Update management Process - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *High*
Testing Procedure	- Locate server and with a Domain Admin present log on as a domain administrator - Identify Antivirus Software Application(s) - Launch the Antivirus program and search for Virus Definition history - Verify the latest Virus Definitions are up to date
Test Nature	- Objective
Evidence	
Findings	

The Audit

In the pages following you will find the results of the physical audit performed on the Corporate Security Domain Controller. A smaller set of items have been chosen to represent the key focus of this Audit. Select items have been taken from the preceding checklist and placed here. The audit results can be found here in the Item's "Evidence" and "Findings" fields.

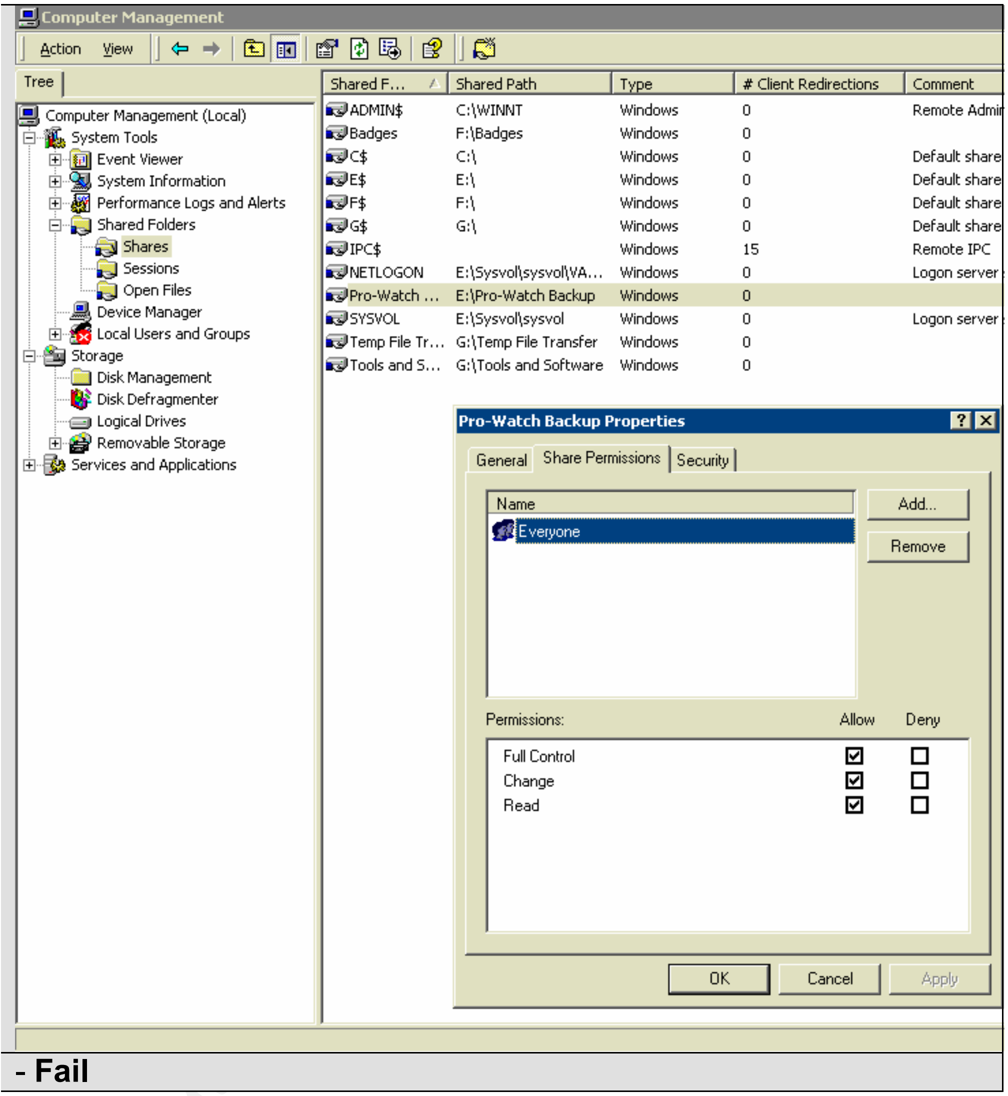
Check that the Server is Physically Secured

Item 1	Data/Comments
Reference	Microsoft 5-Minute Security Advisor - Basic Physical Security http://www.microsoft.com/technet/community/columns/5min/5min-203.mspx
Risk	- Too often companies spend a great deal of time and money securing their Network when their greatest vulnerability could be the theft of the computer itself. - **Vulnerability** addressed is number 6. Server stored in unsecured location - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *High*
Testing Procedure	- Locate and Visit the facility where the server is housed - Verify that access to the room is controlled and that only required personnel can gain access - Verify that the server is in a locked server cabinet/rack
Test Nature	- Objective
Evidence	- The Server is located in a building secured by an Access Control system. - The room that the server is located in is secured by an additional layer of access control utilizing Bio-Metric hand reader technology - Reviewing an access report for this room with the Administrator it was found that only IT personnel with specific requirements have access to this room
Findings	**- Pass**

Check for the existence of Open Shares

Item 2	Data/Comments
Reference	UCB Windows 2000 Server Security Guidelines http://www.colorado.edu/its/windows2000/adminguide/w2ksecguidelines.html#physical

	Chapter 2.D ii & iii
Risk	- One of the most common ways an intruder can gain access to a computer is through an open share. - **Vulnerability** addressed is number 8. Open Shares - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data - **Likelihood** that a threat could exploit this vulnerability: *High*
Testing Procedure	- Locate server and log on as a domain user - Right click on the My Computer Icon - Left click on Manage - In Computer Management under System tools click on “Shared Folders” then click on Shares - Verify there are no Unauthorized/Open shares
Test Nature	- Objective
Evidence	- This Screen Shot displays several open shares some of which hold critical information to the access control system running within the server:

	
Findings	**- Fail**

Shared F...	Shared Path	Type	# Client Redirections	Comment
ADMIN$	C:\WINNT	Windows	0	Remote Admir
Badges	F:\Badges	Windows	0	
C$	C:\	Windows	0	Default share
E$	E:\	Windows	0	Default share
F$	F:\	Windows	0	Default share
G$	G:\	Windows	0	Default share
IPC$		Windows	15	Remote IPC
NETLOGON	E:\Sysvol\sysvol\VA...	Windows	0	Logon server
Pro-Watch ...	E:\Pro-Watch Backup	Windows	0	
SYSVOL	E:\Sysvol\sysvol	Windows	0	Logon server
Temp File Tr...	G:\Temp File Transfer	Windows	0	
Tools and S...	G:\Tools and Software	Windows	0	

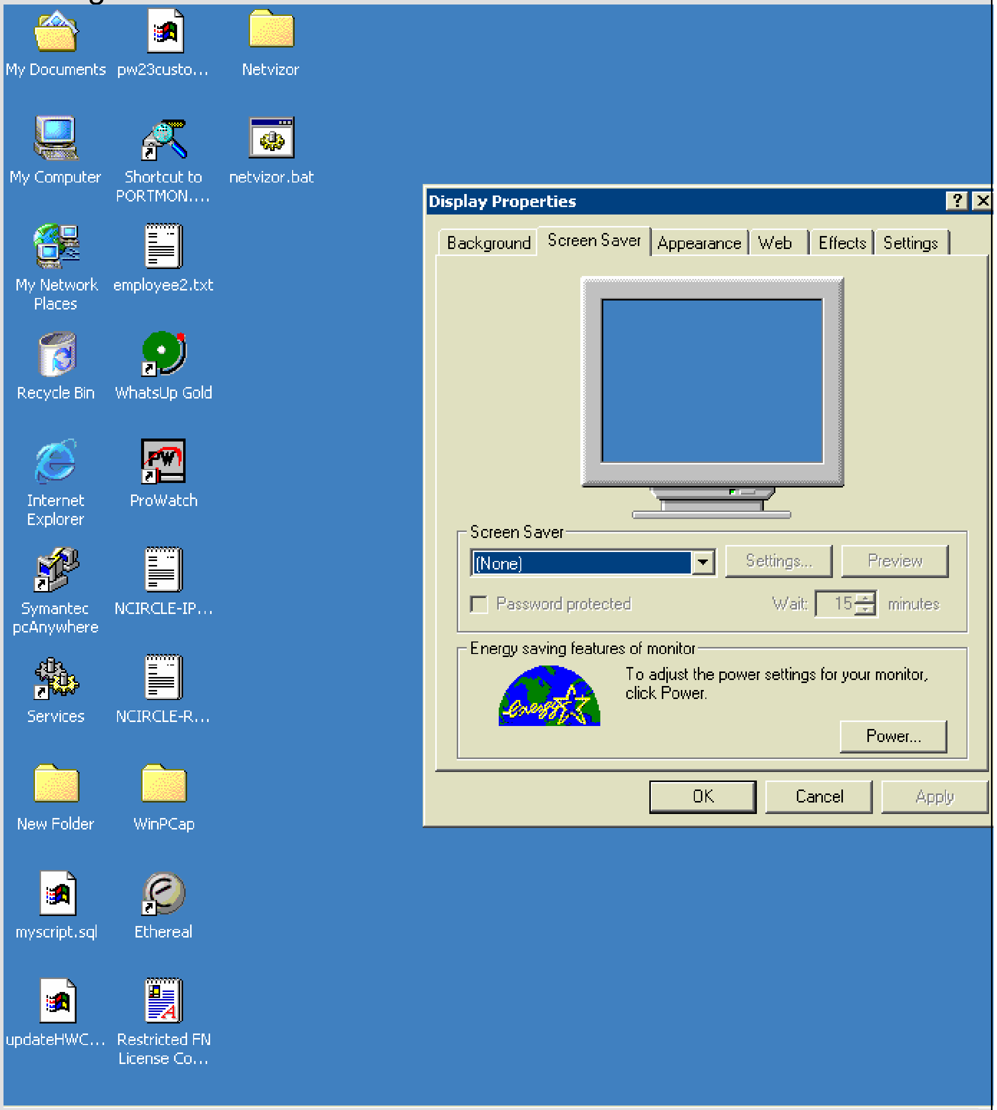
Pro-Watch Backup Properties

Name: Everyone

Permissions:	Allow	Deny
Full Control	☑	☐
Change	☑	☐
Read	☑	☐

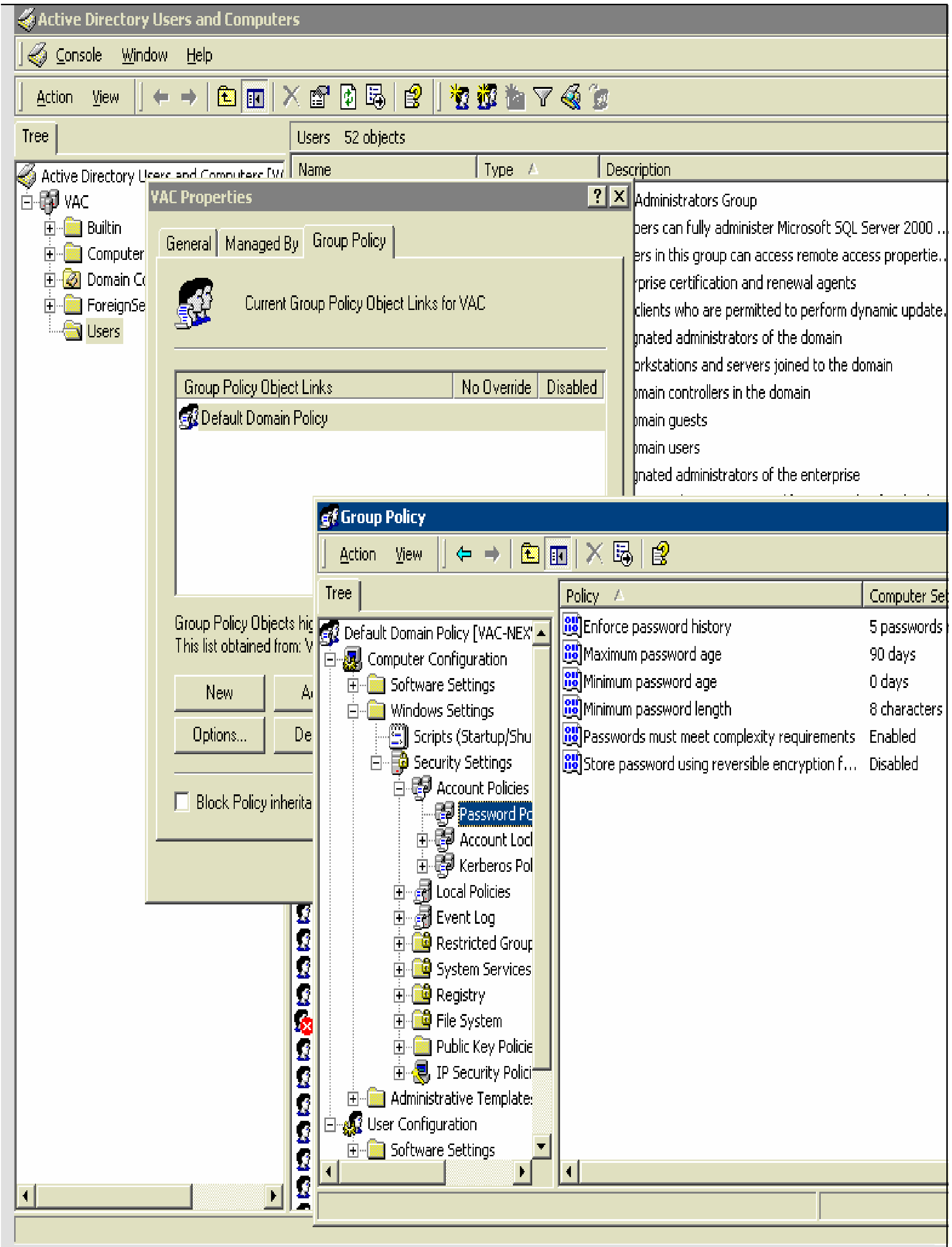
Password Protected Screen Saver Enabled

Item 3	Data/Comments
Reference	I have referenced Personal Experience for this Checklist Item. In my experience you may come across someone remotely logged on to a server by simply traversing through the control console (switchbox)
Risk	- If an administrator walked away from a system and did not log off or lock it “and” a Password Protected Screen Saver was not enabled anyone local or remote could take control of that system. - **Vulnerability** addressed is number 2. No Password Protected screen savers on Server - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data

	5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *High*
Testing Procedure	- Locate server and log on as a domain user - Right click on the desktop and select properties - Under display properties select screen saver - Verify that a screen saver is selected and that the Password Protected button is checked - Also verify that the Wait time is set no longer than 15 minutes
Test Nature	- Objective
Evidence	- This Screen Shot displays the desktop properties screen saver tab. The Screen Saver is not enabled under the Domain User Logon:  Display Properties Screen Saver: (None) □ Password protected Wait: 15 minutes My Documents pw23custo... Netvizor My Computer Shortcut to PORTMON.... netvizor.bat My Network Places employee2.txt Recycle Bin WhatsUp Gold Internet Explorer ProWatch Symantec pcAnywhere NCIRCLE-IP... Services NCIRCLE-R... New Folder WinPCap myscript.sql Ethereal updateHWC... Restricted FN License Co... Background Screen Saver Appearance Web Effects Settings Settings... Preview Energy saving features of monitor To adjust the power settings for your monitor, click Power. Power... OK Cancel Apply
Findings	**- Fail**

Check that “Passwords must meet complexity policy” is enabled

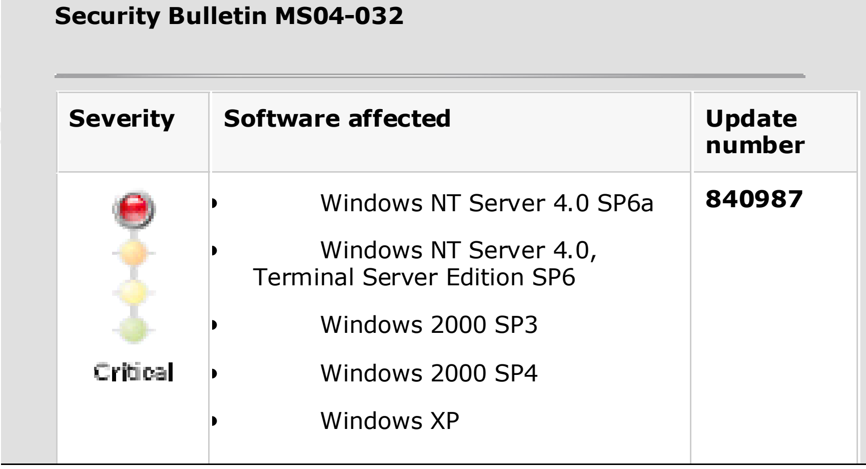
Item 4	Data/Comments
Reference	Protect against weak Authentication Protocols and Passwords http://www.windowsecurity.com/articles/Protect-Weak-Authentication-Protocols-Passwords.html
Risk	- An easily guessable password has the potential to allow an intruder full access to that system. Forcing users to create a complex password greatly reduces that risk. - **Vulnerability** addressed is number 3. Easily Guessable Passwords (Server Policy does not enforce Passwords to meet complexity requirements) - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *Medium*
Testing Procedure	- Locate server and with a Domain Admin present log on as a domain administrator - Click on Start, Programs, Administrative Tools and Active Directory Users and Computers - Right click on the server you want to administer and select properties - Under the Server Properties select group policy - In the list of Policy Object links Double click “Default Domain Policy” - Under Computer Configuration select Windows Settings, Security Settings, Account Policies and Password Policies - Verify that “Passwords Must Meet Complexity Requirements” is enabled
Test Nature	- Objective
Evidence	- This Screen Shot displays the Servers Password Policy. - “Passwords Must Meet Complexity Requirements” is enabled for this server:

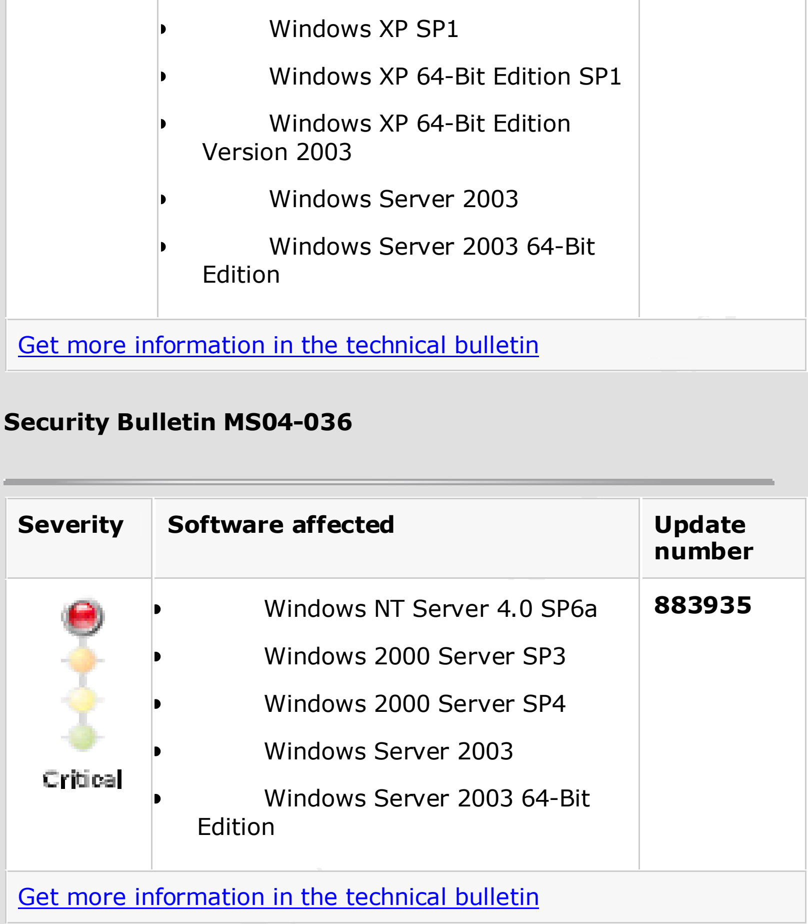
	
Findings	**- Pass**

Policy	Computer Se
Enforce password history	5 passwords
Maximum password age	90 days
Minimum password age	0 days
Minimum password length	8 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption f...	Disabled

Verify Patch or Update management process

Item 7	Data/Comments
Reference	Securing Windows 2000 Server (Sans) http://www.sans.org/rr/whitepapers/win2k/189.php
Risk	- An un-patched system connected to a network is extremely vulnerable to viruses and mal-ware. Insuring there is a good process in place to manage patches and updates will

<table>
<tr><td></td><td>decrease the vulnerability level of the system.
- <b>Vulnerability</b> addressed is number <u>1. Insufficient Patch or Update management Process</u>
- <b>Assets</b> affected by a successful exploitation are:
<u>1. Control Room Operator Access Control and Digital Video Data</u>
<u>2. Investigator Data</u>
<u>3. Badge Office Data</u>
<u>4. Human Resources Data</u>
- <b>Likelihood</b> that a threat could exploit this vulnerability: <i><u>High</u></i></td></tr>
<tr><td><b>Testing Procedure</b></td><td>- Locate and interview the Administrator for the target system
- Verify the existence of policies and procedures outlining the Patching and Updating process
- Locate server and with a Domain Admin present log on as a domain administrator
- Click on Start, Control Panel and then “Add/Remove programs”
- Under “Change or Remove Programs” Identify All Microsoft Updates, Hot Fixes and Service packs
- Compare these against the latest versions on the Microsoft Security Updates Bulletins Page http://www.microsoft.com/security/bulletins/default.mspx
- Verify that all applicable patches are installed and current</td></tr>
<tr><td><b>Test Nature</b></td><td>- Objective and Subjective</td></tr>
<tr><td><b>Evidence</b></td><td>- Interviewed the Security Domain Administrator
- Confirmed through interview that there are no Policies and Procedures surrounding the patch and management process.
- Administrator patches the Security Domain Controller on an as-needed basis
- Below are screen shots displaying the registered patches to this server and a few missed updates from the Microsoft Bulletin page:
-

<b>Security Bulletin MS04-032</b>
<table>
<tr><th>Severity</th><th>Software affected</th><th>Update number</th></tr>
<tr><td>Critical</td><td>• Windows NT Server 4.0 SP6a
• Windows NT Server 4.0, Terminal Server Edition SP6
• Windows 2000 SP3
• Windows 2000 SP4
• Windows XP</td><td><b>840987</b></td></tr>
</table></td></tr>
</table>



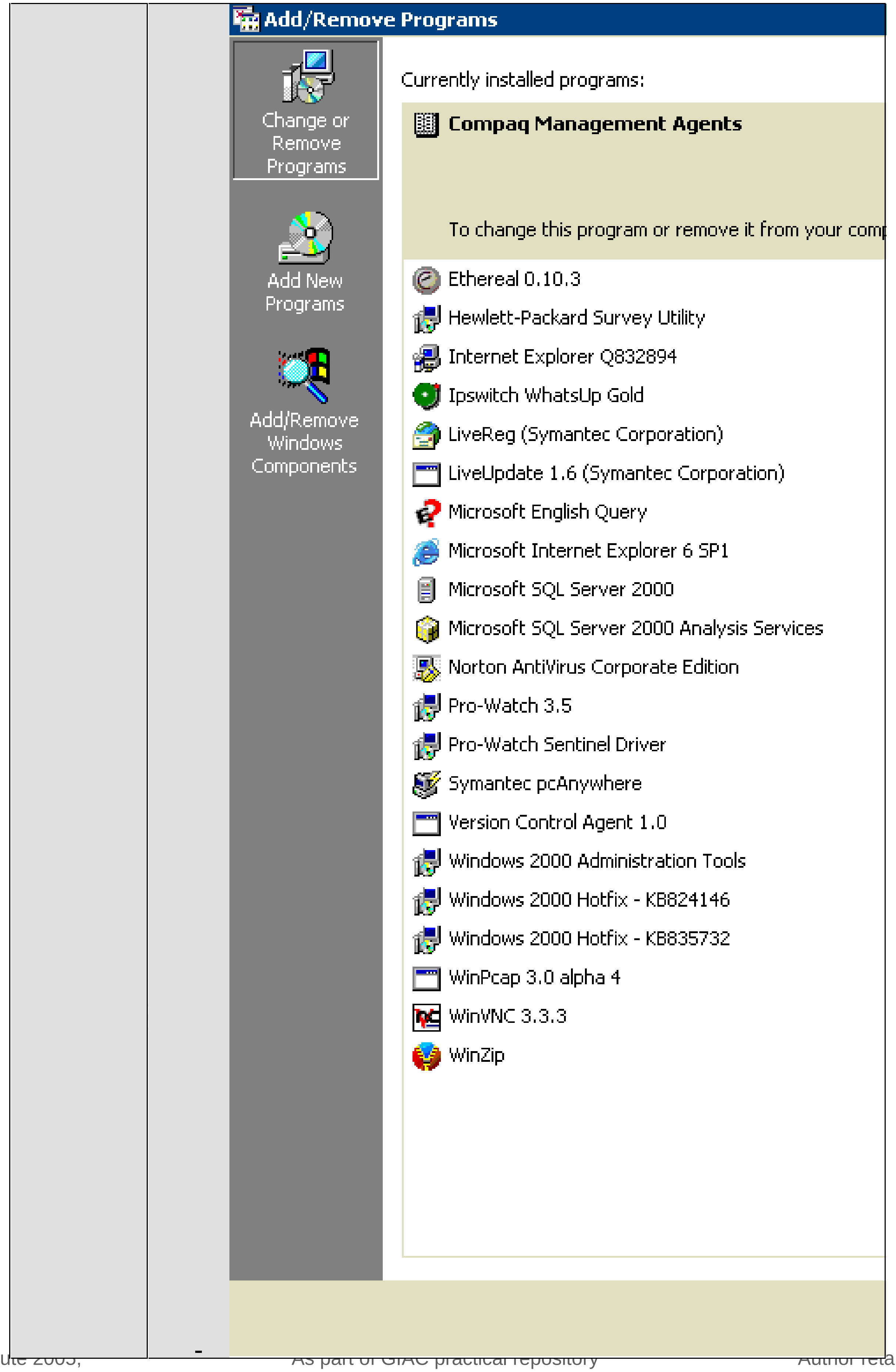
	- Windows XP SP1 - Windows XP 64-Bit Edition SP1 - Windows XP 64-Bit Edition Version 2003 - Windows Server 2003 - Windows Server 2003 64-Bit Edition	

Get more information in the technical bulletin

Security Bulletin MS04-036

Severity	Software affected	Update number
Critical	- Windows NT Server 4.0 SP6a - Windows 2000 Server SP3 - Windows 2000 Server SP4 - Windows Server 2003 - Windows Server 2003 64-Bit Edition	**883935**

Get more information in the technical bulletin



Currently installed programs:

Compaq Management Agents

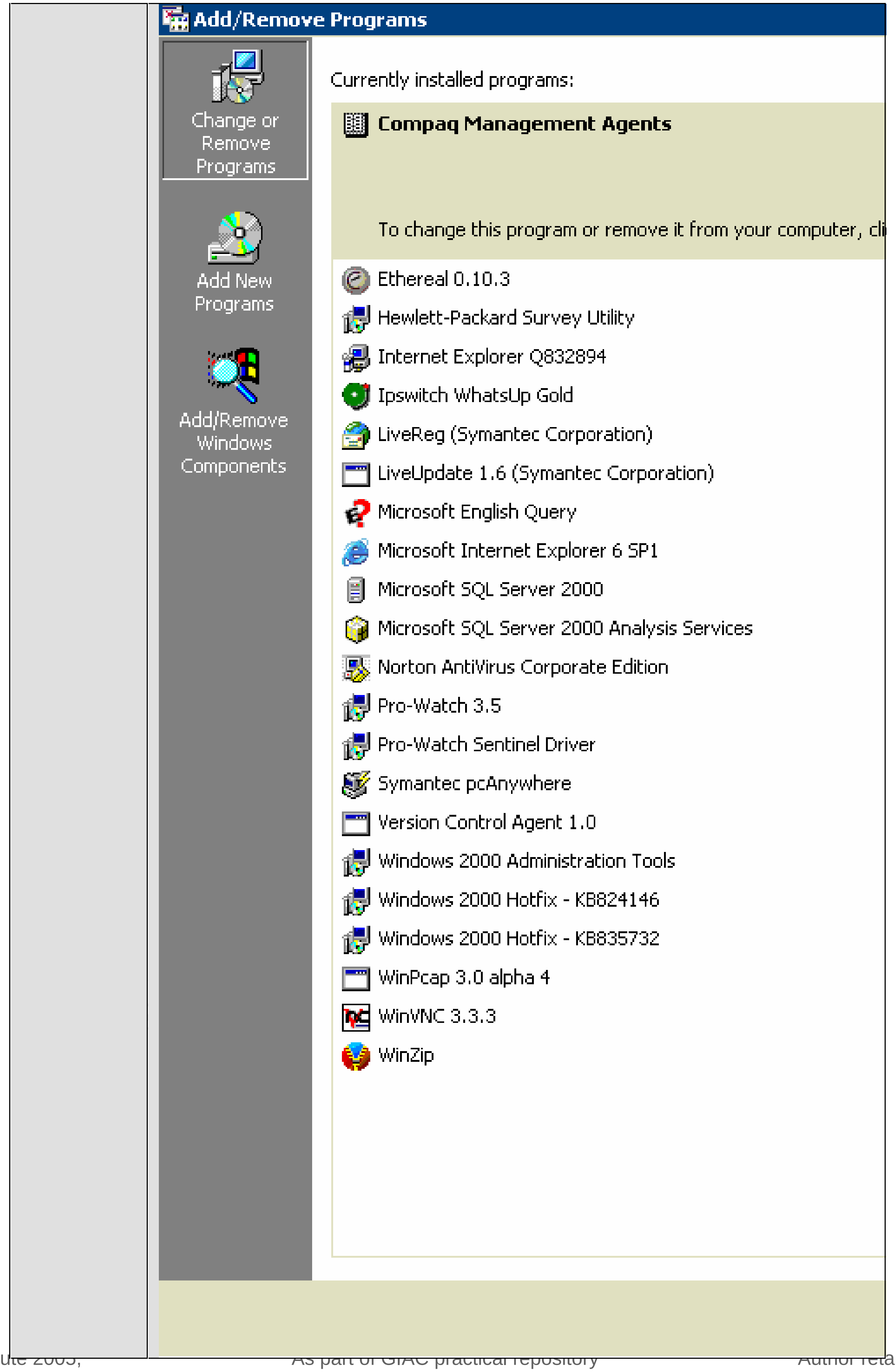
To change this program or remove it from your comp

Ethereal 0.10.3
Hewlett-Packard Survey Utility
Internet Explorer Q832894
Ipswitch WhatsUp Gold
LiveReg (Symantec Corporation)
LiveUpdate 1.6 (Symantec Corporation)
Microsoft English Query
Microsoft Internet Explorer 6 SP1
Microsoft SQL Server 2000
Microsoft SQL Server 2000 Analysis Services
Norton AntiVirus Corporate Edition
Pro-Watch 3.5
Pro-Watch Sentinel Driver
Symantec pcAnywhere
Version Control Agent 1.0
Windows 2000 Administration Tools
Windows 2000 Hotfix - KB824146
Windows 2000 Hotfix - KB835732
WinPcap 3.0 alpha 4
WinVNC 3.3.3
WinZip

Findings	- **Fail** - There are no policies or procedures and no change control processes in place to insure proper checks and balances in the patching or updating of this domain controller - This server is not at the current patch level

Does the Server have Remote Desktop Applications

Item 8	**Data/Comments**
Reference	UCB Windows 2000 Server Security Guidelines http://www.colorado.edu/its/windows2000/adminguide/w2ksecguidelines.html#filesystem Chapter 4.C
Risk	- It is important to check for the presence of remote desktop applications. They are simply another common access point that can be exploited. - **Vulnerability** addressed is number 9. Remote Desktop Applications - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *High*
Testing Procedure	- Locate server and with a Domain Admin present log on as a domain administrator - Click on Start, Control Panel and then “Add/Remove programs” - Under “Change or Remove Programs” Identify any Remote Desktop Applications - Under “Add or Remove Windows Components” Identify any Remote Desktop Applications
Test Nature	- Objective
Evidence	- This Screen Shot shows a display of the applications loaded onto this server - There are two remote desktop applications installed “PCAnywhere” and “WinVNC”:



Currently installed programs:

Compaq Management Agents

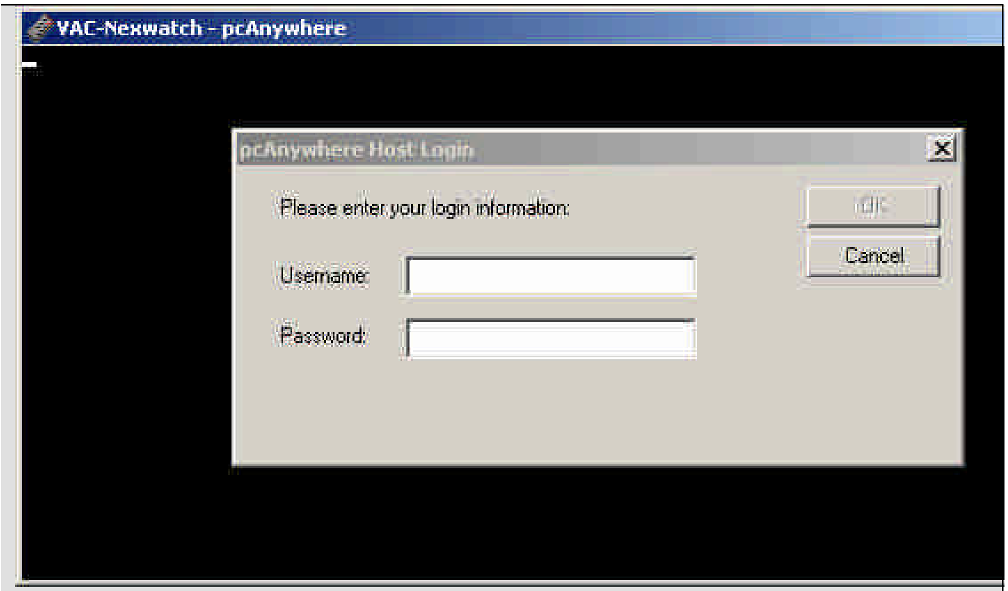
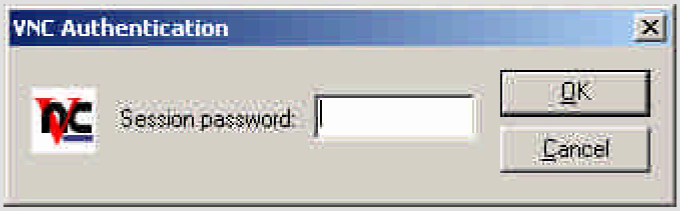
To change this program or remove it from your computer, cli

Ethereal 0.10.3
Hewlett-Packard Survey Utility
Internet Explorer Q832894
Ipswitch WhatsUp Gold
LiveReg (Symantec Corporation)
LiveUpdate 1.6 (Symantec Corporation)
Microsoft English Query
Microsoft Internet Explorer 6 SP1
Microsoft SQL Server 2000
Microsoft SQL Server 2000 Analysis Services
Norton AntiVirus Corporate Edition
Pro-Watch 3.5
Pro-Watch Sentinel Driver
Symantec pcAnywhere
Version Control Agent 1.0
Windows 2000 Administration Tools
Windows 2000 Hotfix - KB824146
Windows 2000 Hotfix - KB835732
WinPcap 3.0 alpha 4
WinVNC 3.3.3
WinZip

Findings	**- Confirmed 2 Remote Desktop Applications Installed on this Server**

Do the Remote Desktop Applications require passwords

Item 9	**Data/Comments**
Reference	UCB Windows 2000 Server Security Guidelines http://www.colorado.edu/its/windows2000/adminguide/w2ksecguidelines.html#filesystem Chapter 4.C
Risk	- Many remote desktop applications offer the ability to remotely gain access to another desktop "without" logging onto the application itself. Presenting the password protection on the remote desktop application adds an additional layer of security that may stop an intruder from gaining full access to the remote computer. - **Vulnerability** Addressed is number 9. Remote Desktop Applications - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *High*
Testing Procedure	- Locate server and with a Domain Admin present log on as a domain administrator - Identified Remote Desktop Applications - Launch the Host program (program on the server that allows remote access) and look for Password Protection Options - Verify that the option is enabled
Test Nature	- Objective
Evidence	- These Screen Shots are a result of a stimulus/response test for both Remote Desktop Applications - With both application remote programs loaded on a separate client machine within the security domain an attempt to connect to the server was made - PCAnywhere required a username/password - WinVNC required a session password

	 VAC-Nexwatch - pcAnywhere pcAnywhere Host Login Please enter your login information: Username: Password: OK Cancel 
Findings	**- Pass**

Check Global Catalog User and Computer Administration Process

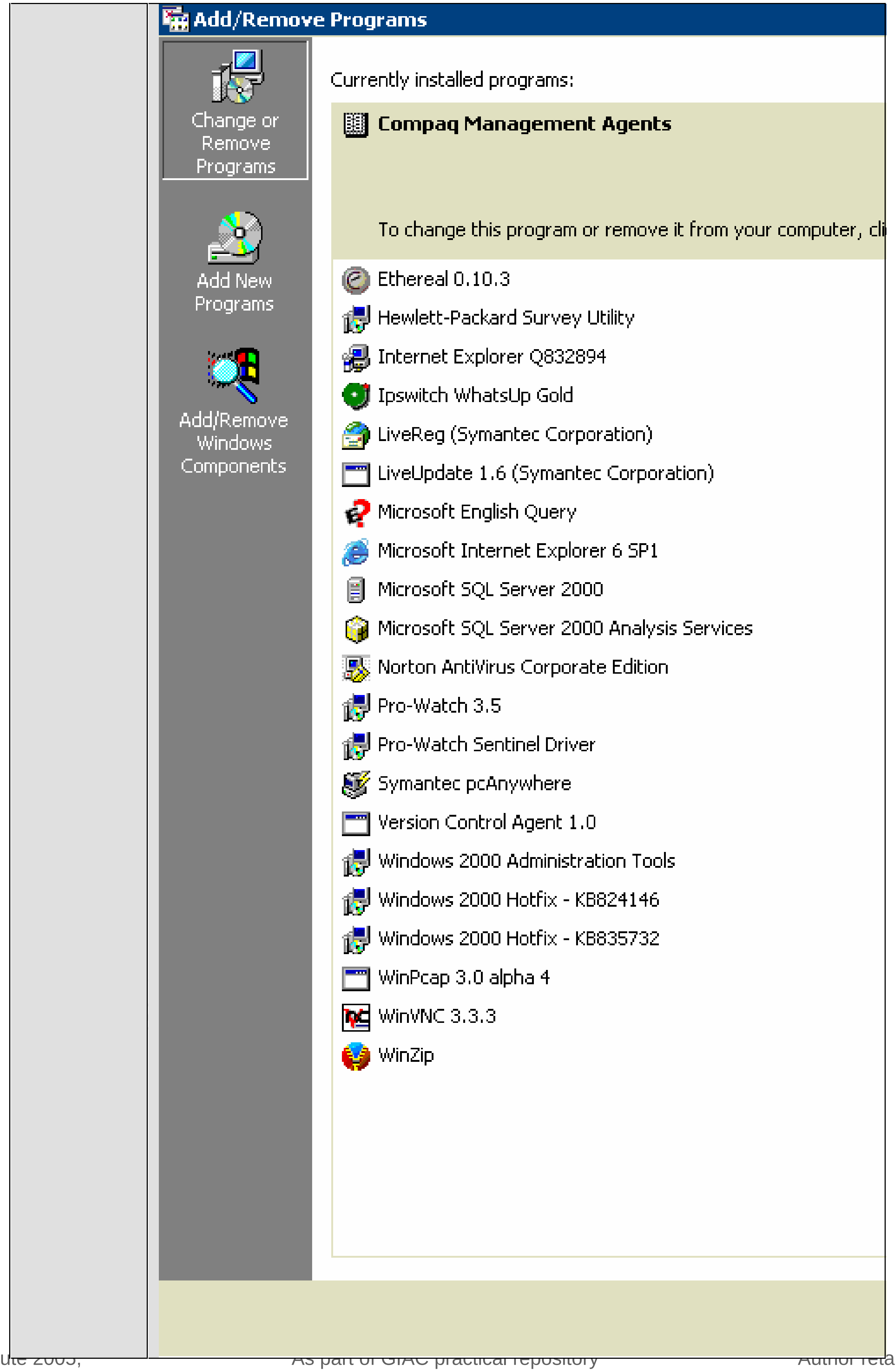
Item 11	Data/Comments
Reference	I have referenced Personal Experience for this Checklist Item. Administrators may create additional user accounts for testing or other purposes. Without a strict process and auditing this can create a great vulnerability.
Risk	- An open or unrestricted administration process could quite possibly be the weak link in the "security" chain. The network can be secured very well, but if anyone can acquire administrative or elevated permissions then the security structure is greatly weakened. - **Vulnerability** addressed is number 7. Elevated Permissions - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *High*

Testing Procedure	- Locate and interview the Administrator for the target system - Verify the existence of policies and procedures outlining the user/computer account creation, modification and deletion process
Test Nature	- Subjective
Evidence	- Confirmed through interview with Administrator of the Security Domain that there are no Policies and Procedures for the creation, modification and deletion of user or computer accounts. - Administrator updates Active Directory Users and Computers on an as-needed basis
Findings	- **Fail** - There are no policies or procedures and no change control processes in place to insure proper checks and balances in the administration of the user and computer accounts on this domain controller

Verify the existence of Antivirus Software

Item 12	**Data/Comments**
Reference	Auditing the Corporate Access Control System: An independent Auditor's Perspective http://www.giac.org/practical/GSNA/Scott_Steiner_GSNA.pdf Item 9
Risk	- Antivirus Software is often the main defense against intrusions from computer viruses and other Malware. - **Vulnerability** addressed is number 1. Insufficient Patch or Update management Process - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *High*
Testing Procedure	- Locate server and with a Domain Admin present log on as a domain administrator - Click on Start, Control Panel and then "Add/Remove programs" - Under "Change or Remove Programs" Identify any Antivirus Software Applications
Test Nature	- Objective
Evidence	- This Screen Shot shows a display of the applications loaded onto

	this server - Norton Antivirus Corporate Edition is loaded onto this Server



Currently installed programs:

Compaq Management Agents

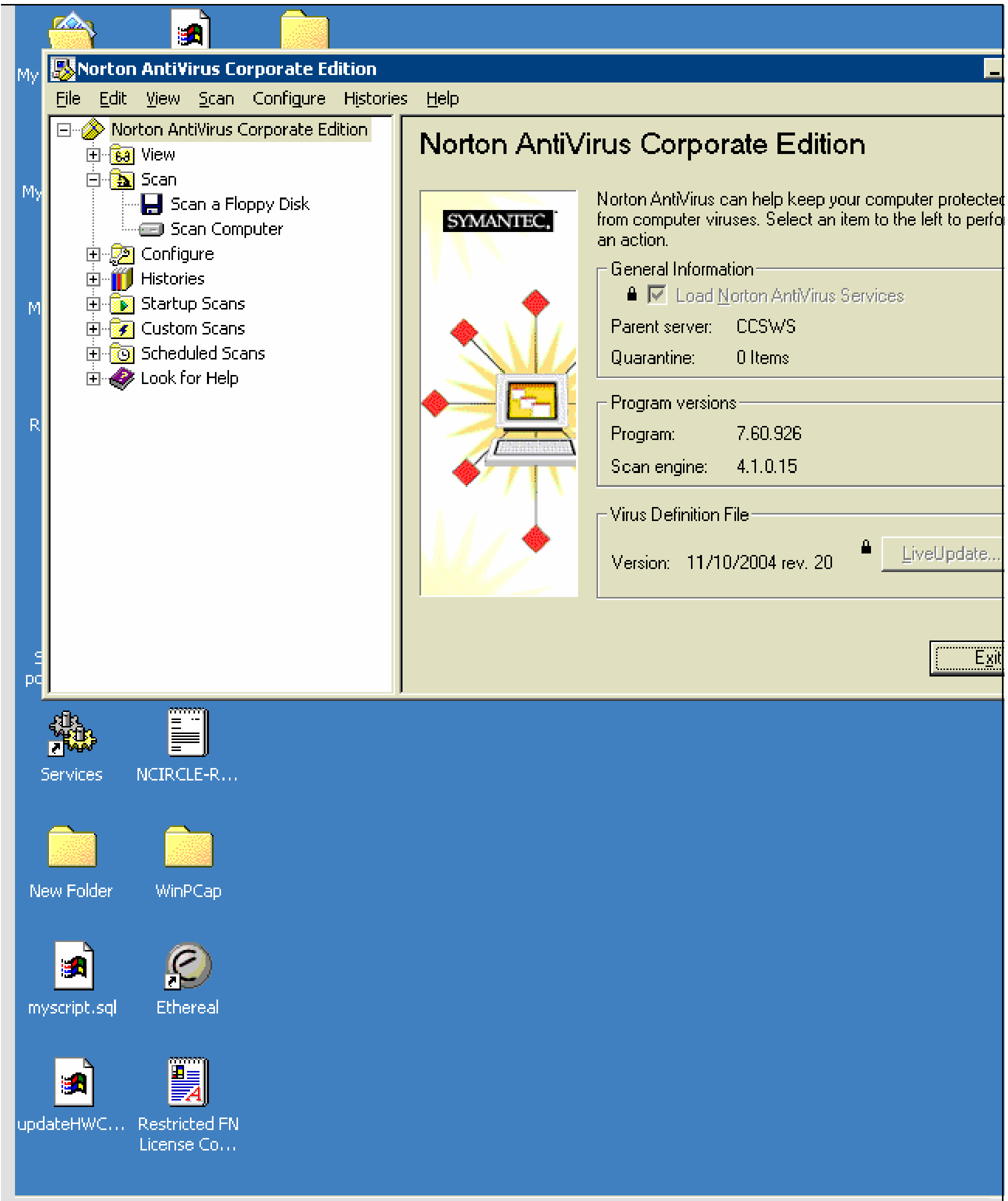
To change this program or remove it from your computer, cli

Ethereal 0.10.3
Hewlett-Packard Survey Utility
Internet Explorer Q832894
Ipswitch WhatsUp Gold
LiveReg (Symantec Corporation)
LiveUpdate 1.6 (Symantec Corporation)
Microsoft English Query
Microsoft Internet Explorer 6 SP1
Microsoft SQL Server 2000
Microsoft SQL Server 2000 Analysis Services
Norton AntiVirus Corporate Edition
Pro-Watch 3.5
Pro-Watch Sentinel Driver
Symantec pcAnywhere
Version Control Agent 1.0
Windows 2000 Administration Tools
Windows 2000 Hotfix - KB824146
Windows 2000 Hotfix - KB835732
WinPcap 3.0 alpha 4
WinVNC 3.3.3
WinZip

Findings	- Pass

Check that Antivirus Virus Definitions are up to date

Item 14	Data/Comments
Reference	Auditing the Corporate Access Control System: An independent Auditor's Perspective http://www.giac.org/practical/GSNA/Scott_Steiner_GSNA.pdf Item 9
Risk	- Although a system may have an Antivirus system installed if the virus definitions are not up to date any number of recently created viruses or malware can still attack a system. - **Vulnerability** addressed is number 1. Insufficient Patch or Update management Process - **Assets** affected by a successful exploitation are: 1. Control Room Operator Access Control and Digital Video Data 2. Investigator Data 3. Badge Office Data 4. Human Resources Data 5. Building Physical Security - **Likelihood** that a threat could exploit this vulnerability: *High*
Testing Procedure	- Locate server and with a Domain Admin present log on as a domain administrator - Identify Antivirus Software Application(s) - Launch the Antivirus program and search for Virus Definition history - Verify the latest Virus Definitions are up to date
Test Nature	- Objective
Evidence	- This Screen Shot shows the main application front end of Norton Antivirus - Virus Definition files are up to date:

	 Norton AntiVirus Corporate Edition File Edit View Scan Configure Histories Help Norton AntiVirus Corporate Edition View Scan Scan a Floppy Disk Scan Computer Configure Histories Startup Scans Custom Scans Scheduled Scans Look for Help SYMANTEC. LiveUpdate... Exit Services NCIRCLE-R... New Folder WinPCap myscript.sql Ethereal updateHWC... Restricted FN License Co... Norton AntiVirus Corporate Edition Norton AntiVirus can help keep your computer protected from computer viruses. Select an item to the left to perfo an action. General Information ☑ Load Norton AntiVirus Services Parent server: CCSWS Quarantine: 0 Items Program versions Program: 7.60.926 Scan engine: 4.1.0.15 Virus Definition File Version: 11/10/2004 rev. 20
Findings	**- Pass**

Report and Recommendations

Executive Summary

This Audit was performed with the expressed permission of the Security Department and in conjunction with the Security Domain Administrator.

There are several considerations to every technical audit so it was very important that the focus of this audit included only the items that a Security Domain Controller might be vulnerable to. Ultimately 10 Items were used to assess the security of this Server. In general the Server did fairly well outside of a few noted exceptions regarding file shares and screen savers. The other note worthy items had more to do with Policy and Procedure rather than System Security.

The purpose of this audit was to assess the vulnerabilities and risk levels of this security systems server and I believe we have achieved that. Before I get to the recommendations I would like to review some of the findings.

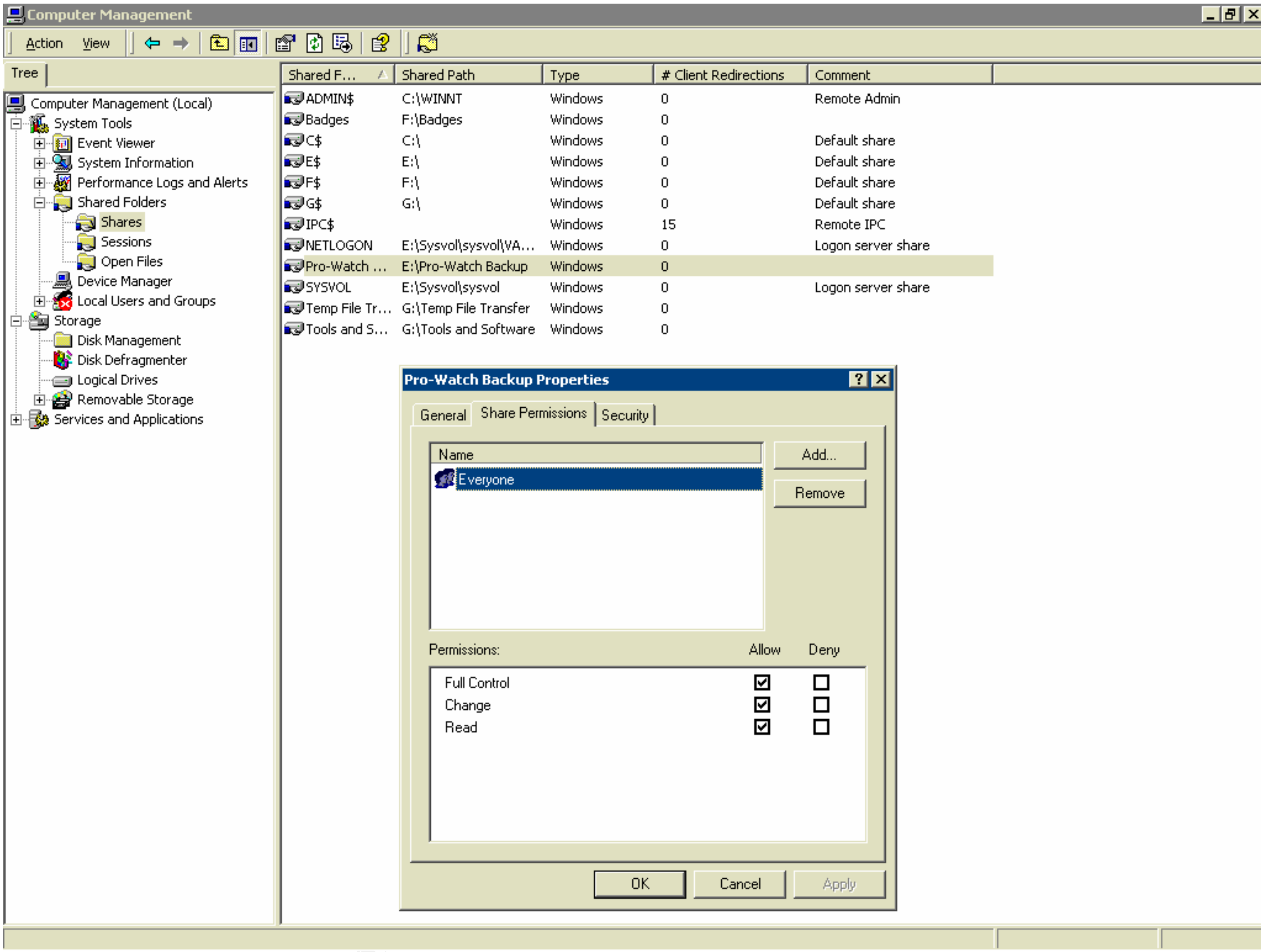
Audit Findings

Item 1 (page 22) Check that the Server is Physically Secured

- The Server **passed** the physical security inspection. A site visit was performed and it was found that the building was secured well with access control. Once inside, the server room was protected with BioMetric “Hand Reader” access control technology. The server was secured well inside the Rack in the server room; however, the door to the rack was unlocked and left open.
- The **Recommendation** is to keep the door to the Server Rack closed and locked when not being used. This will mitigate the risk inherent with the physical access of a multi-user server room. The **Cost** should be minimal (less than $100) to produce additional Rack Door keys and all key-holders should be registered with the security department and human resources in the event of employment termination.
- In the interim or to keep costs down the key to the lockable server cabinet can be given to security where it can be checked out by a user each time it needs to be opened.

Item 2 (page 22) Check for the existence of Open Shares

- The Server **failed** the check for open shares inspection. While accessing the Computer Management Console and reviewing the Shared Folders a number of “open shares” were discovered. Each share was checked for permissions which may allow it to be accessible by the public. This would create a risk. A few of them were open *(see figure 1.3).* Open Shares can be used to propagate viruses and mal-ware.
- The **Recommendation** is to close all open shares and to conduct a monthly inspection of the Shared Folders under the servers Computer Management Console. A screen shot (much like the one in figure 1.3) should be sent to management each month for review. The **Cost** is negligible and only requires a few moments of the Administrators time.



Shared F...	Shared Path	Type	# Client Redirections	Comment
ADMIN$	C:\WINNT	Windows	0	Remote Admin
Badges	F:\Badges	Windows	0	
C$	C:\	Windows	0	Default share
E$	E:\	Windows	0	Default share
F$	F:\	Windows	0	Default share
G$	G:\	Windows	0	Default share
IPC$		Windows	15	Remote IPC
NETLOGON	E:\Sysvol\sysvol\VA...	Windows	0	Logon server share
Pro-Watch ...	E:\Pro-Watch Backup	Windows	0	
SYSVOL	E:\Sysvol\sysvol	Windows	0	Logon server share
Temp File Tr...	G:\Temp File Transfer	Windows	0	
Tools and S...	G:\Tools and Software	Windows	0	

Pro-Watch Backup Properties

Name: Everyone

Permissions:	Allow	Deny
Full Control	☑	☐
Change	☑	☐
Read	☑	☐

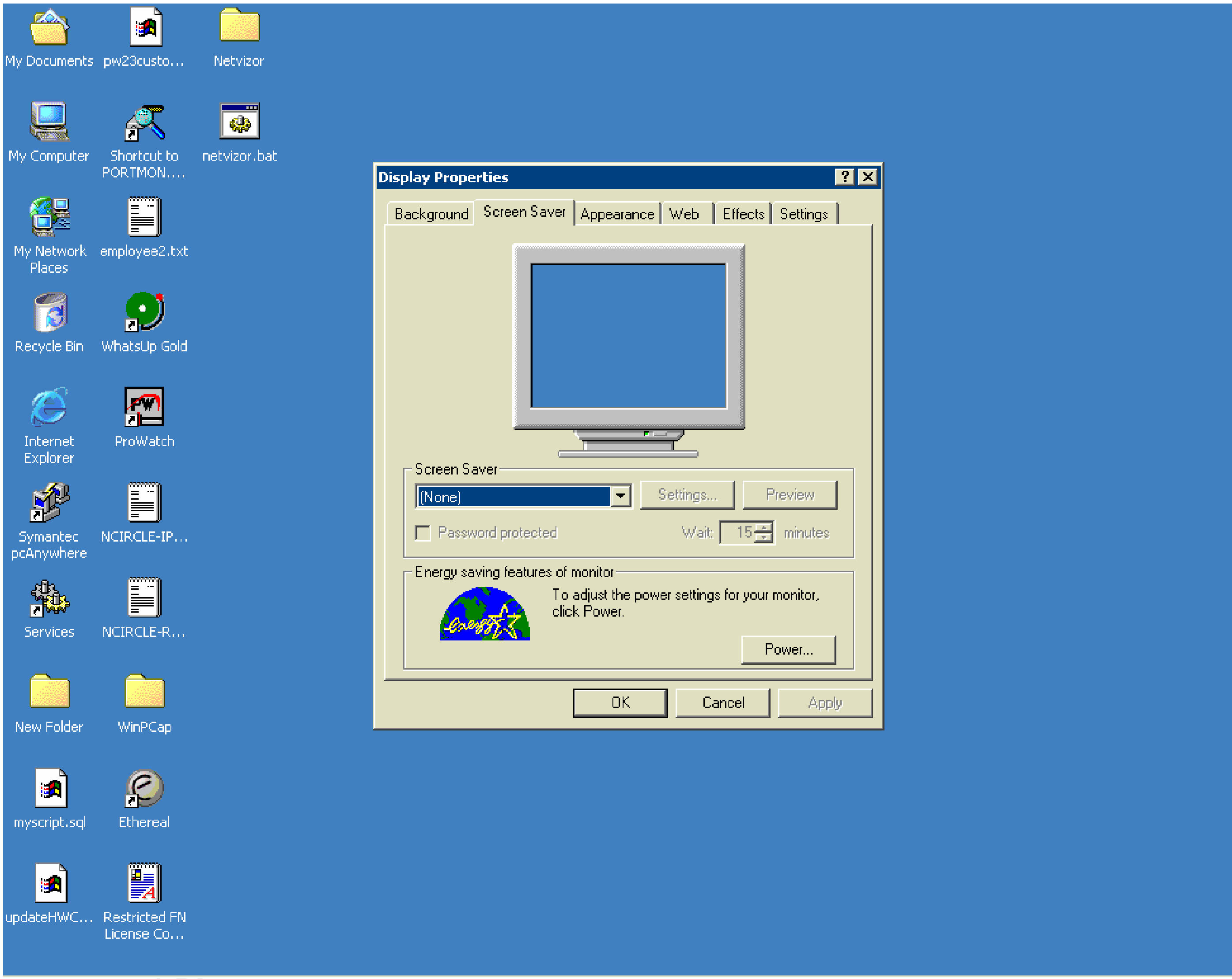
Figure 1.3

Item 3 (page 24) Password Protected Screen Saver Enabled

- The Server **Failed** the Password Protected Screen Saver inspection (*see figure 1.4*). I checked to see if the password protected screen savers (under the "Display Properties" on the desktop of the server) option was enable. As a standard domain user I found the screen saver option was not enabled. If a system does not utilize a password protected screen saver someone can accidentally walk away from a system they've logged onto leaving it open for intruders to find even several months later.
- The **Recommendation** is to incorporate the activation and password protection option as part of an administrators check list when assigning a new account. This would be a manual process, but it would accomplish three things. One is the remediation of a potential exposure, the second is the visual verification by the Administrator that the option has been enabled and

lastly the new account holder will gain an initial impression as to the level of importance the management group places on security.

- The **Cost** to achieve this goal should be minimal. To create a checklist for new account holders will take a few hours of an Administrators time, but the management of it should be quite simple.



Screen Saver: (None)

□ Password protected Wait: 15 minutes

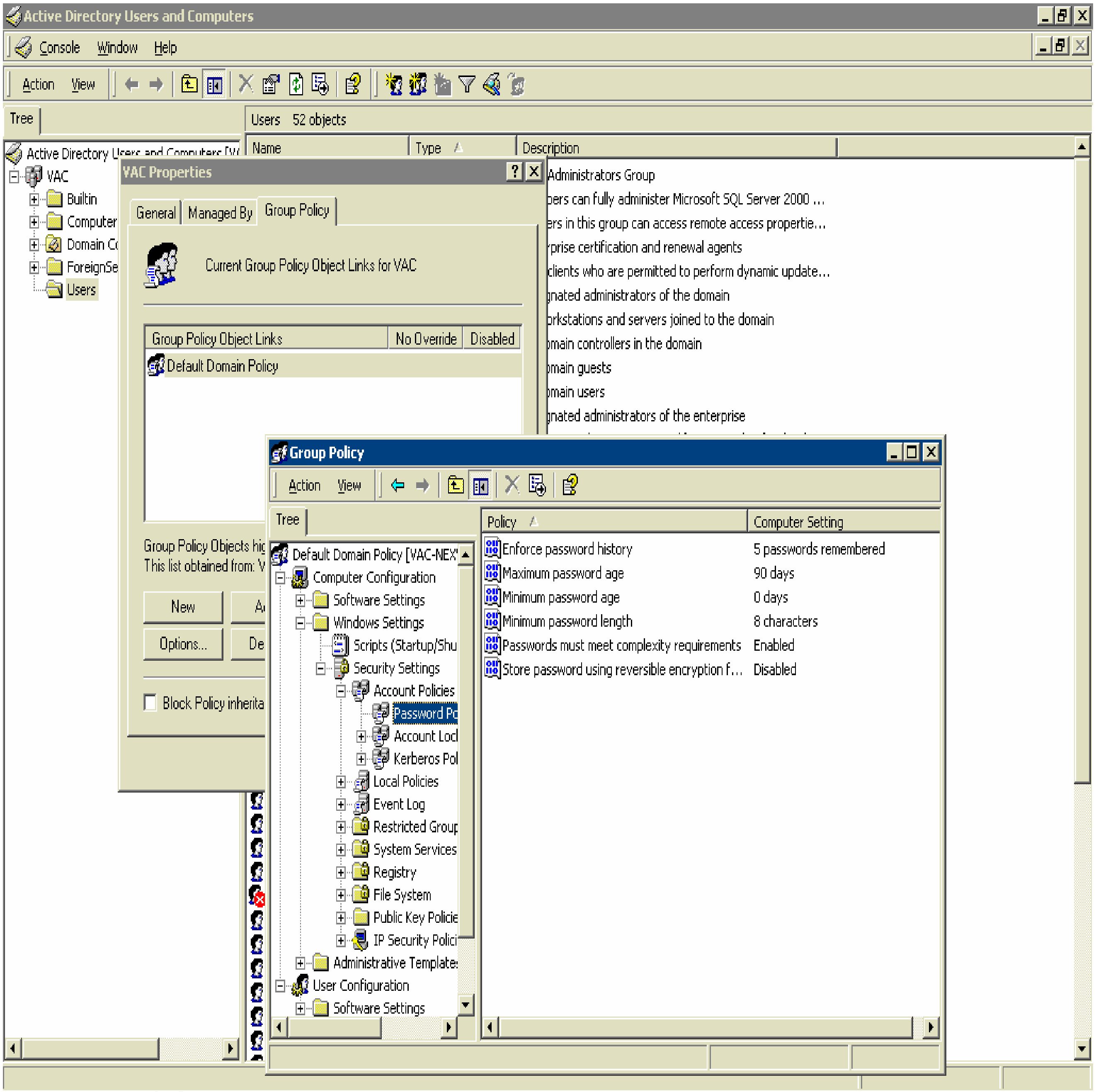
Energy saving features of monitor

To adjust the power settings for your monitor, click Power.

Figure 1.4

Item 4 (page 26) Check that "Passwords must meet complexity policy" is enabled

The Server **Passed** the Password Complexity Policy inspection. Under Active Directory Users and Computers I opened up the Password Policies and reviewed the settings (see figure 1.5). This Password must meet complexity policy option was enabled.


Active Directory Users and Computers
Console Window Help
Action View
Tree
Users 52 objects
Name Type Description
Active Directory Users and Computers [V...
VAC
Builtin
Computer
Domain C
ForeignSe
Users
Administrators Group
bers can fully administer Microsoft SQL Server 2000 ...
ers in this group can access remote access propertie...
rprise certification and renewal agents
clients who are permitted to perform dynamic update...
gnated administrators of the domain
orkstations and servers joined to the domain
omain controllers in the domain
omain guests
omain users
gnated administrators of the enterprise
VAC Properties
General Managed By Group Policy
Current Group Policy Object Links for VAC
Group Policy Objects hig
This list obtained from: V
New A
Options... De
Block Policy inherita
Group Policy
Tree
Default Domain Policy [VAC-NEX
Computer Configuration
Software Settings
Windows Settings
Scripts (Startup/Shu
Security Settings
Account Policies
Password Pc
Account Locl
Kerberos Pol
Local Policies
Event Log
Restricted Group
System Services
Registry
File System
Public Key Policie
IP Security Polici
Administrative Template
User Configuration
Software Settings

Group Policy Object Links	No Override	Disabled
Default Domain Policy		

Policy	Computer Setting
Enforce password history	5 passwords remembered
Maximum password age	90 days
Minimum password age	0 days
Minimum password length	8 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption f...	Disabled

Figure 1.5

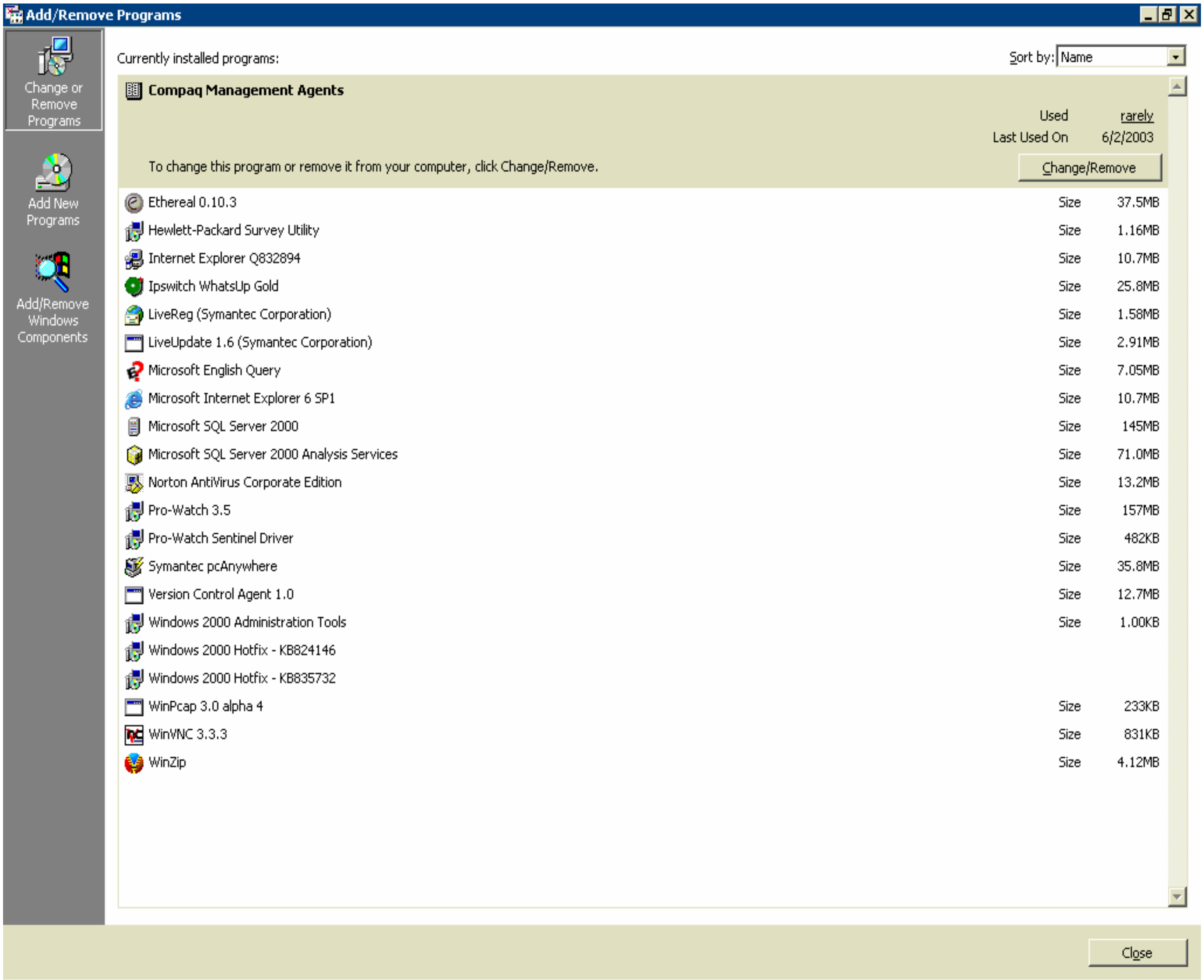
Item 7 (page 27) Verify Patch or Update management processes

- The Server and the Process **Failed** the Patch/Update management inspection. An interview was conducted with the Security Systems Administrator with regards to Policies and Procedures for patching and updating this server. There are no policies or procedures that govern the Patch or Update process. Additionally the Server is not up to the current patch level and therefore remains vulnerable to intruders (see images on pages 29 and 30). An unpatched system is extremely vulnerable to software viruses and hackers. Without a process in place this server will have trouble staying at the current patch level.

- The **Recommendation** is to patch the Server as soon as possible. Additionally, a process needs to be put in place that insures this domain controller will remain current with its patches and updates. A simple process could involve a timeline. The administrator would have 24 hours from the time Microsoft releases a patch or update to get it installed and confirm this with a screen shot of the installed patch. There is no **Cost** to support either of these recommendations aside from a few hours of the Administrators time.

Item 8 (page 31) Does the Server have Remote Desktop Applications

- A **Confirmation** was made that the Server does have remote desktop applications loaded onto it. This was discovered by navigating to the Add/Remove Programs under control panel (*see figure 1.6*). Symantec PCAnywhere and WinVNC 3.3.3 are loaded onto this Server.



Currently installed programs:

Compaq Management Agents

Used rarely
Last Used On 6/2/2003

To change this program or remove it from your computer, click Change/Remove.

Ethereal 0.10.3	Size	37.5MB
Hewlett-Packard Survey Utility	Size	1.16MB
Internet Explorer Q832894	Size	10.7MB
Ipswitch WhatsUp Gold	Size	25.8MB
LiveReg (Symantec Corporation)	Size	1.58MB
LiveUpdate 1.6 (Symantec Corporation)	Size	2.91MB
Microsoft English Query	Size	7.05MB
Microsoft Internet Explorer 6 SP1	Size	10.7MB
Microsoft SQL Server 2000	Size	145MB
Microsoft SQL Server 2000 Analysis Services	Size	71.0MB
Norton AntiVirus Corporate Edition	Size	13.2MB
Pro-Watch 3.5	Size	157MB
Pro-Watch Sentinel Driver	Size	482KB
Symantec pcAnywhere	Size	35.8MB
Version Control Agent 1.0	Size	12.7MB
Windows 2000 Administration Tools	Size	1.00KB
Windows 2000 Hotfix - KB824146		
Windows 2000 Hotfix - KB835732		
WinPcap 3.0 alpha 4	Size	233KB
WinVNC 3.3.3	Size	831KB
WinZip	Size	4.12MB

Figure 1.6

Item 9 (page 33) Do the Remote Desktop Applications require passwords

- The Server **Passed** the Remote Desktop Application password inspection. If you recall from Item 8, page 31 we discovered the existence of remote desktop applications. Under Item 9 an inspection was made to check whether the Remote Desktop applications are using password protection. To do this I chose a Stimulus/Response test. I logged onto a workstation that had both PCAnywhere and WinVNC remote software running on it. From there I made the attempt to connect to the Security Domain Controller. Please see **Figure 1.7 and 1.8** to review the responses from this test.

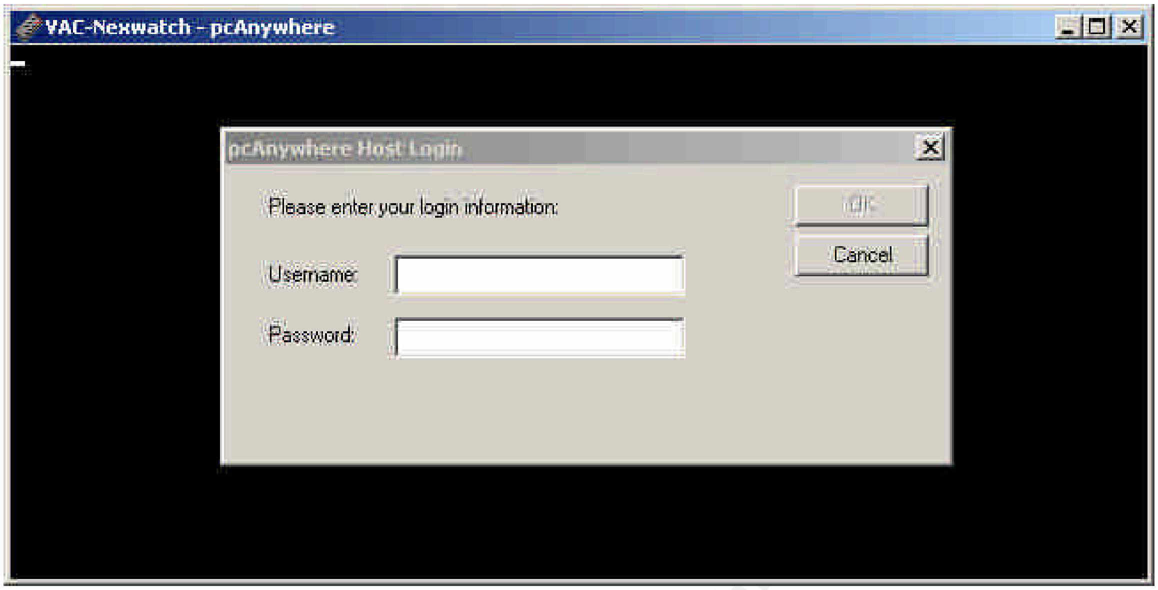

VAC-Nexwatch - pcAnywhere
pcAnywhere Host Login
Please enter your login information:
Username:
Password:
OK
Cancel

Figure 1.7

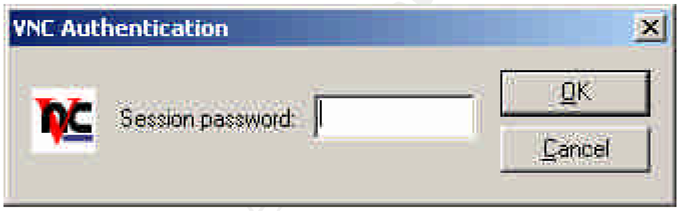


Figure 1.8

Item 11 (page 34) Check Global Catalog User and Computer Administration Process

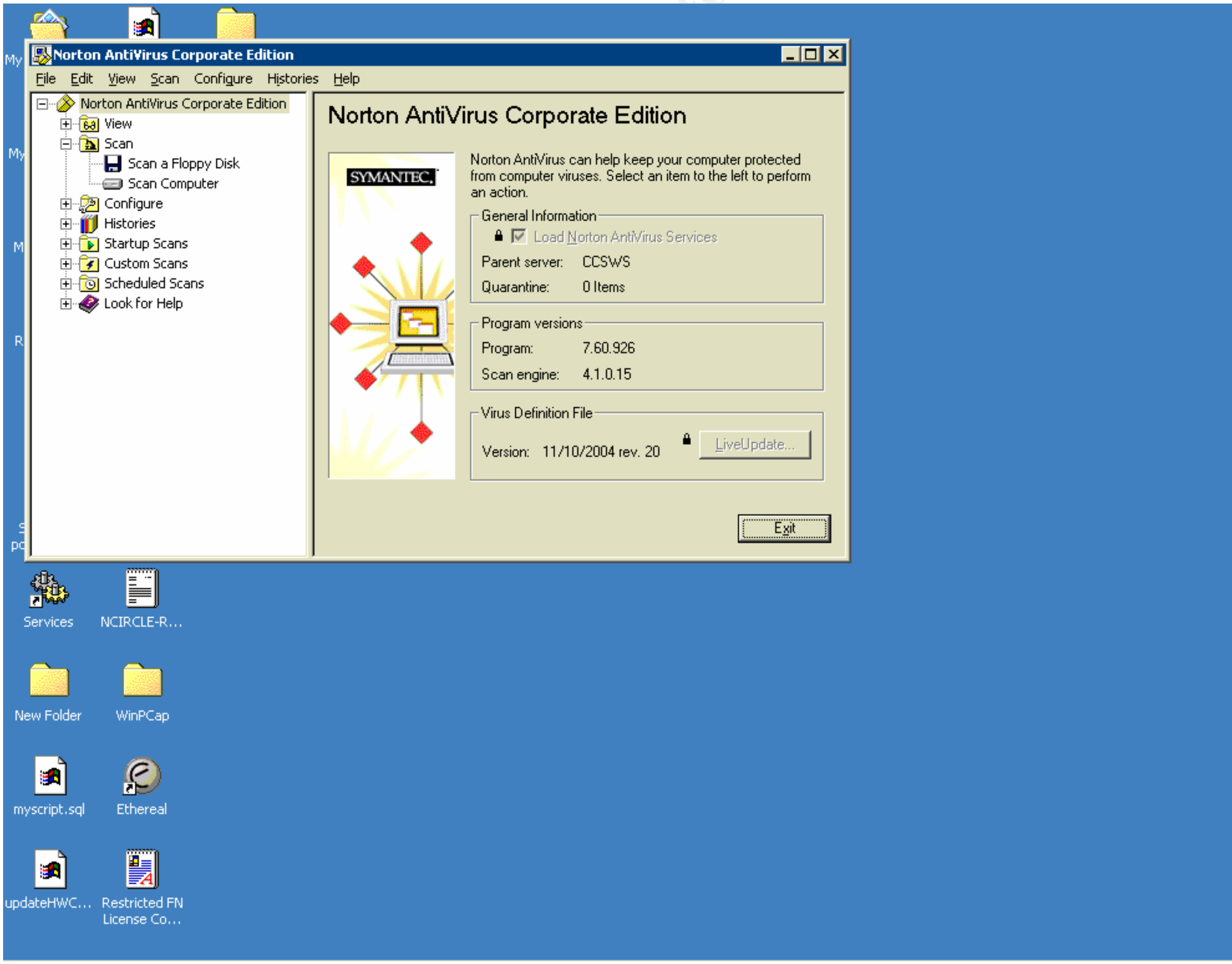
- The Process (in this case) **Failed** the Global Catalog User and Computer Account management inspection. An interview was conducted with the Security Systems Administrator with regards to Policies and Procedures for managing accounts on this server. There are no policies or procedures that govern the account management process. Without a process to manage user and computer accounts users may be able to acquire elevated permissions and accidentally allow exposures to exist.
- I'm **Recommending** a process be put in place that insures accounts on this domain controller will only be updated after acquiring written Management approval to do so. Upon approval the administrator can update the Global Catalog and confirm the new configuration by a screen shot to Management. There is no **Cost** to support this recommendation aside from a few hours of the Administrators time and the time it will take for the Management signature process.

Item 12 (page 35) Verify the existence of Antivirus Software

- A **Confirmation** was made that the Server does have an Antivirus application loaded onto it. This was discovered by navigating to the Add/Remove Programs under control panel (*see figure 1.6*). Norton Antivirus Corporate Edition is loaded onto this Server.

Item 14 (page 38) Check that Antivirus Virus Definitions are up to date

- The Server **Passed** the Antivirus Definitions currency inspection. If you recall from Item 12, page 35 we discovered the existence of an antivirus application. Under Item 14 an inspection was made to check whether the Antivirus application is using password protection. To do this I opened the Antivirus Application to the main page/screen. Please see **Figure 1.9** for the results from this test.



Norton AntiVirus Corporate Edition

Norton AntiVirus can help keep your computer protected from computer viruses. Select an item to the left to perform an action.

General Information

☑ Load Norton AntiVirus Services

Parent server: CCSWS

Quarantine: 0 Items

Program versions

Program: 7.60.926

Scan engine: 4.1.0.15

Virus Definition File

Version: 11/10/2004 rev. 20

LiveUpdate...

Exit

Figure 1.9

Bibliography (References)

1. Securing Windows 2000 Server
http://www.microsoft.com/downloads/details.aspx?FamilyID=9964cf42-e236-4d73-aef4-7b4fdc0a25f6&DisplayLang=en

2. National Security Agency (Security Recommendation Guidelines for Windows 2000)
http://nsa1.www.conxion.com/win2k/download.htm

3. Securing Windows 2000 Server (Sans)
http://www.sans.org/rr/whitepapers/win2k/189.php

4. Protect Against Weak Authentication Protocols and Passwords
http://www.windowsecurity.com/articles/Protect-Weak-Authentication-Protocols-Passwords.html

5. Auditing Windows 2000
http://www.winnetmag.com/Articles/Print.cfm?ArticleID=9633

6. UCB Windows 2000 Server Security Guidelines
http://www.colorado.edu/its/windows2000/adminguide/w2ksecguidelines.html

7. Auditing the Corporate Access Control System: An independent Auditor's Perspective
http://www.giac.org/practical/GSNA/Scott_Steiner_GSNA.pdf

8. 5-Minute Security Advisor - Basic Physical Security
http://www.microsoft.com/technet/community/columns/5min/5min-203.mspx