Auditing Networks, Perimeters, and Systems
GSNA Practical Assignment, Option 1

Auditing the Corporate Access Control System: An Independent Auditor's Perspective

Scott Steiner
10/24/2003

Table of Contents:

1. **Assignment 1 – Research in Audit, Measurement Practice, and Control**
   - Company overview
   - Identify the system to be audited and how it works
   - Evaluate the risk to the system
   - What is the current state of the system

2. **Assignment 2 – Create an Audit Checklist**
   - Item 1 – Physical Security of the Server
   - Item 2 – Service Packs and Hotfixes
   - Item 3 – Rename the Server Administrator Account
   - Item 4 – Server User Accounts and Group Settings
   - Item 5 – System Logon and Policy Auditing
   - Item 6 – Verify Event Logs are Maintained and Reviewed
   - Item 7 – Disable Any Unnecessary Services on the Server
   - Item 8 – Verify Shared Folders on the Server
   - Item 9 – Server Anti-Virus Practices
   - Item 10 – Change Control Policy
   - Item 11 – Patch Management Practices
   - Item 12 – Backup and Restore Process
   - Item 13 –Disaster Recovery Plan
   - Item 14 – Vender Server and Application Access policy
   - Item 15 – Workstation Access Policy for Security Officers
   - Item 16 – ACME Application Account Privileges
   - Item 17 – Verify Authorized ACME Users
   - Item 18 – Verify Authorized ACME Workstations
   - Item 19 – Process of Assigning Clearance to a Controlled Area
   - Item 20 – Security Officer Responses and Incident Handling

3. **Assignment 3 – Audit Evidence**
   - Item 1 – Physical location and security of the server
   - Item 2 – Server Operating System Version, Service Packs, and Hotfixes
   - Item 3 – Server vulnerability check
   - Item 4 – Local Security Policy
   - Item 5 – Additional Data, Applications, Shares, or Services on the Server
   - Item 6 – Patch Management practices
   - Item 7 – Business continuity and disaster recovery plan
   - Item 8 – Vender Server Access policy
   - Item 9 – Application privileges check

- Item 10 – Process of granting a badge holder access to a controlled area
- Measuring Residual Risk
- Is the System Auditable?

4. **Assignment 4 – Audit Report or Risk Assessment**
   - Executive Summary
   - Audit Findings
   - Item 1 – Server Operating System Version, Service Packs, and hotfixes
   - Item 2 – Server Account Password Policies
   - Item 3 –
   - Item 4 –
   - Item 5 –
   - Item 6 –
   - Item 7 –
   - Item 8 –
   - Item 9 –
   - Item 10 –
   - **Background / Risk**
   - **Audit Recommendations**
   - **Costs**
   - **References**

Introduction

This paper is a technical report of the risks and vulnerabilities that exist in the XYZ Enterprises access control system. This report will evaluate those risks based off of a prepared checklist of items, and explain the associated risks, as well as how to correct them. An in-depth report of the individual components of the system will not be performed in this report, instead a technical overview of the system, as well as the policies, practices, and procedures that are utilized on a daily basis will be analyzed. The primary focus of this audit will be the system as a whole, and what it takes to effectively secure the system that is relied upon for the security of the enterprise.

The access control system is a critical system used by the Corporate Security department as their primary defense in protecting the employees, the assets, as well as the network and data of the company. The loss of the access control system would be detrimental to the security of the building as every door transaction, alarm, as well as emergency procedures are relied upon from within the access control application. Securing the access control system is the first step in protecting all of the components that make up the company.

Assignment 1 – Research in Audit, Measurement Practice, and Control

Company Overview

XYZ Enterprises is one of the nation's leading media companies and operators of real-estate auctions. Major operating subsidiaries include XYZ Communications, Inc. ([NYSE: XYZ] which includes cable television distribution, telephone, high-speed Internet access and other advanced broadband services); XYZ Newspapers, Inc. (newspapers, local and national direct mail advertising and customized newsletters); XYZ Television (television, television sales rep firms and research); XYZ Radio, Inc. ([NYSE: XYR] broadcast radio stations and interactive web sites); and House Hold Auctions, Inc., (real-estate auctions, repair and certification services and web-based technology products). XYZ Enterprises also owns an equity stake in a range of Internet businesses, including www.HouseHoldRealty.com, the world's largest and most visited source of new and used homes for sale, for agents and consumers.

The company has over 77,000 employees located throughout the U.S. and abroad, and operates 300 separate businesses. XYZ Enterprises has recently completed the building of a state of the art building, which began construction in the fall of 2000. The majority of the construction completed in the Spring of 2002 and employees began moving into the new building one floor at a time. By October of 2002, the building had become completely occupied. Final construction of the corporate building was completed with the grand opening of the XYZ Company Museum Center on Oct 9, 2003. The corporate headquarters building provides a centralized office space for the executives and supporting staff of each business unit.

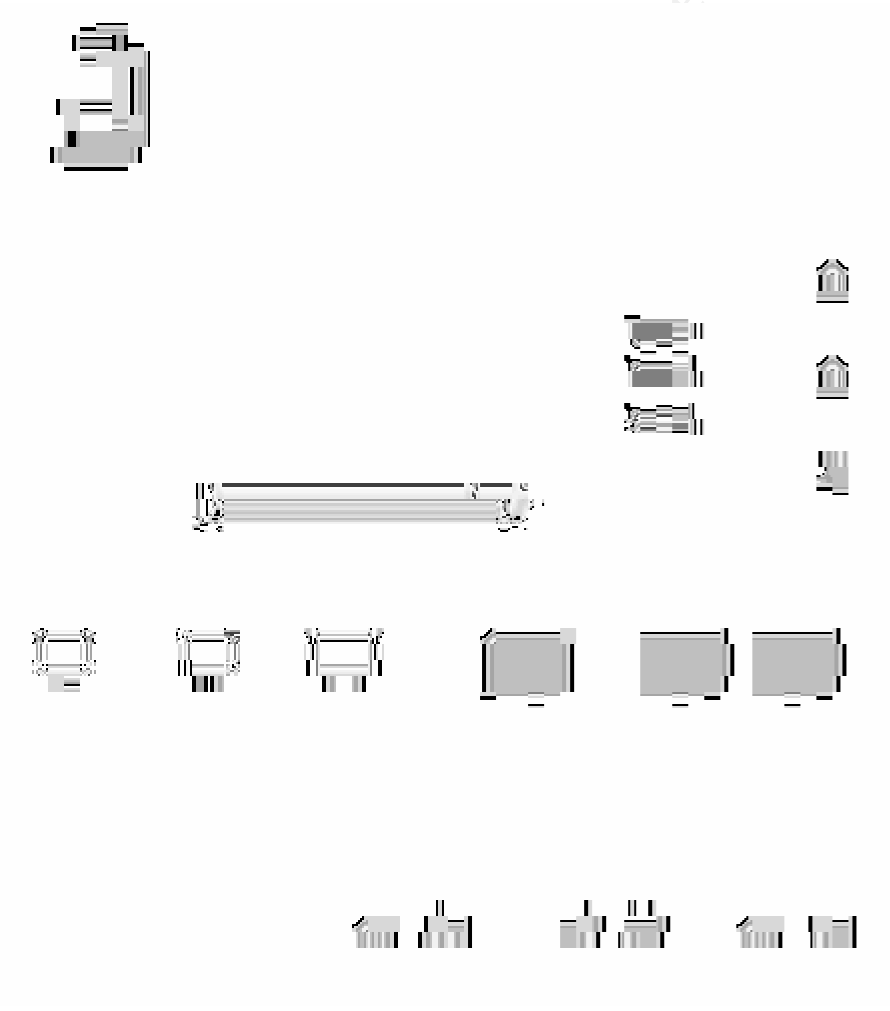
The design and implementation of the access control system is very detailed and sophisticated. To start with, on the ground floor, there is a Security Operations Center which is occupied 24 hours a day, every day of the year which receives door transactions and alarms, both visual and audible. During normal business hours (6:00am-8:00pm) there are over 15 security officers that occupy various posts throughout the building, loading dock, and parking deck. There are 2 officers in the parking deck, one each at the visitor entrance and employee entrance. To enter the building from the parking lot, you must present your employee ID badge to a security officer at the front entrance of the building. This officer does a visual photo check and allows entrance to the building. If you do not have your employee ID badge, or if you are a visitor, you must present a drivers license or state issued photo ID card. At this point, you will be entered into a log book and allowed into the building.

After being permitted entrance into the building, you will enter the unsecured area known as the commons area. The commons area is made up of a company store, cafeteria, museum, and corporate training rooms. This area is not access controlled, and to enter the work environment of the building an access control card must be obtained from the commons area lobby security desk. To obtain a temporary or visitor access control card, you must be signed in and initially accompanied by an employee of the building, even if you are employed at another of XYZ Enterprises business units. To enter the secured area of the building, you must pass through an electronic optical turnstile unit, that is occupied by another security officer. This security officer has a workstation computer and once your access control card is presented to the reader, picture validation would appear on the security officer's computer, giving visual authentication. If a non-valid access control card is attempted to be used, an audible alarm will sound at this post, as well as in the Security Operations Center and entrance to the secured area will be denied. After passing through the electronic turnstiles with an authorized card, you are able to obtain access to the elevator lobby to proceed to the offices of the building. Once beyond the elevator lobby, you are free to move about the entire building, providing you have appropriate level clearance to the are you are trying to access.

Due to the recent completion of building construction, senior management has requested that an external systems audit be performed to identify system vulnerabilities and possible security breeches within the access control system and related components. This security audit will provide a reassurance that the employees, as well as the company assets are secured in a protected environment.

Identify The System To Be Audited And How The System Works

As stated in the company overview, the architecture of the access control system is very detailed and sophisticated. At the corporate headquarters building, there are 6 site panels, which controls 233 logical devices, to include: access control doors, glass break alarms, motion detectors, parking deck and perimeter gates, and panic alarms. Each panel has a network interface card (NIC) which it uses to communicate with the ACME application server. The NIC transmits and receives system information, door transactions, and alarms over the XYZ Enterprises Ethernet Network through an encrypted proprietary security protocol. The application server will process all of these transactions and store them to the database, as well as instantly sending them to the client workstations for view in the alarm monitor. If the network is unavailable, the panels will queue all transactions until connectivity is restored and the panels are able to communicate once again to the ACME application server in the Security Operations Center data room. The architecture of the access control system is as follows:



For a new badge to be created, two requirements must be met. First the person requesting the access control badge must be accompanied by a permanent employee of the building, as well as have a signed authorization form from the manager of the secured area that is being requested. After verifying the credentials of the person requesting the badge, and approval has been granted by the manager, the security officer will then take the person's picture with a digital camera and save this picture to a shared folder on the ACME security server. The security officer creates a new badge profile in the ACME application, imports the picture to the badge profile, assigns the clearance code to give appropriate access, saves the changes, and prints the badge. Once the badge is saved, the ACME application server will immediately transmit the new badge information out to all of the panels at which access has been granted. The panel is updated instantly so the new badge can be used immediately.

When a badge is presented at a card reader, the panel, which is directly wired to the reader, will process the card locally and if the badge has valid access, the panel will process the request and grant access. If the badge does not hold access in the panel, the request will be processed as a failed event and the door will not open. A door transaction will then be sent from the panel to the server for logging. All transactions are then able to be viewed in a color-coded event monitor by the security officers on a client workstation. For alarms and failed access events, an audible .wav file is sounded to alert the security officer that someone has attempted to use a card at an unauthorized area. Depending on the severity, another security officer will be dispatched or if possible, the security officer inside the Security Operations Center will monitor the alarm via the CCTV system.

The client workstations are primarily used for event monitoring, badge programming changes, or generating reports. All other activities are not permitted on the access control client workstations as it would create a distraction from their daily job duties. The client workstations directly interact with the server through the XYZ Enterprises Ethernet network.

The system is ACME systems Access Control and Alarm, Enterprise Edition, which is installed on a Dell 6450 Power Edge Server. The server operating system is Windows 2000, SP3 utilizing a MS SQL 2000 SP3 database.

This audit will focus directly on the server, the client workstations, and the application to discover any risks or vulnerabilities that could be exploited to compromise the access control security system.

Evaluate The Risk To The System

The access control system was chosen for the security audit due to the importance of protection that it provides. It is by far the most complex, and important application within the corporation. If the application or server would become compromised, it could lead to someone bypassing the system by giving inappropriate access to a secured area, to a much higher risk of bringing down the entire system to prevent event and alarm monitoring.

Risk #1 - The ACME application server is not physically secured

Probability	Low
Priority	High
Impact	Potential physical damage to the server may occur as well as the insertion of a bootable disk into the CD-ROM or floppy drive that an attacker could use to overwrite the system files.
Control Objectives	To maintain availability of the ACME server, it must be physically protected as there is not a redundant server that could take the place of the primary server in the event of a failure.

Risk #2 - Failure to maintain a secure server operating system with up-to-date service packs and hotfixes

Probability	High
Priority	High
Impact	The lack of current service packs and hotfixes can compromise the server with malicious code, virus, or a Trojan horse
Control Objectives	To maintain availability of the ACME server, all published vulnerabilities must be must be installed to minimize the likeliness of a denial of service/operation attack from a virus or Trojan horse

Risk #3 - Not having the Server Administrator account renamed could allow an attacker the opportunity to guess the password since the name is default and the account can never be locked out

Probability	High
Priority	Medium
Impact	If the Administrator account password is compromised, the server could become completely unavailable for service as the corruption of system files and data could take place. The server could also become locked out if the password was stolen and changed, as the ability to logon could be removed for everyone except the administrator..
Control Objectives	To maintain availability of the ACME server, elevate the difficulty it would take for a hacker to acquire the administrator username and password by renaming it to a name appearing as a general user account.

Risk #4 – Server users could cause intentional or accidental system changes based on them having privileges that are not authorized

Probability	Medium
Priority	High
Impact	Potential loss of system availability from unauthorized changes by accounts being shared by multiple users or users being assigned to a group with elevated privileges.
Control Objectives	To maintain availability of the ACME server, identify all users of the system and assign all users to an administrator or user group for authorized access, based on their role of support. Sharing account passwords is not permitted.

Risk #5 – An attacker could remain unidentified if system logon and policy change auditing is not enabled

Probability	High
Priority	High
Impact	If system changes or policies get changed, it would be impossible to identify when the changes occurred or who changed them. It would also allow an attacker to go unnoticed by failed logons to the system. With a successful attack against the server, a complete system failure could occur
Control Objectives	To maintain availability and integrity of the ACME server, audit account logons, logon events, account management, object access, policy changes, and system events for successful and failed events.

Risk #6 - The ACME server event logs are not being maintained or reviewed by the system administrators

Probability	Medium
Priority	Medium
Impact	If system changes or policies get changed, it would be impossible to identify when the changes occurred or who changed them. It would also allow an attacker to go unnoticed by failed logons to the system. With a successful attack against the server, a complete system failure could occur
Control Objectives	To maintain availability of the ACME server, the security and system log files need to be reviewed daily

Risk#7 - There are unnecessary services running on the ACME server.

Probability	High
Priority	Medium
Impact	The default installed services could potentially contain a security vulnerability leaving the server open be exploited. Data shares could have incorrectly set security permissions leaving the data exposed. Additional applications could lead to

	the unnecessary use of server resources and cause a CPU overload.
Control Objectives	To maintain the availability and integrity of the ACME server remove or disable all unnecessary services running on the server.

Risk #8 – On the ACME server, there are unnecessary shared folders or improper security settings on the authorized shared data folders.

Probability	High
Priority	Medium
Impact	Critical application data could be intentional or accidentally corrupted, deleted, or modified by someone with elevated access privileges.
Control Objectives	To maintain the availability and integrity of the ACME server and data, access to the data that resides on the ACME server should be restricted to authorized users and administrators.

Risk #9 - Antivirus software is not installed on the ACME server or it is not up to date with the most current signature file

Probability	Low
Priority	High
Impact	Without up-to-date Anti-virus software, the server could be compromised by a worm, virus, or malicious code.
Control Objectives	To maintain availability of the ACME server, anti-virus must be installed and have the most current signature file up to date to prevent a virus outbreak that could compromise the server or corrupt the database.

Risk #10 - There is not a change control process established for the ACME Server, or the change control process is not being followed.

Probability	High
Priority	High
Impact	Without a change control process, unauthorized, undocumented, or non-tested system changes could take place which could leave a server or application failure. Having a change control process will allow documentation to be followed from other systems that may undergo the same maintenance.
Control Objectives	To maintain availability of the ACME server, a change control policy needs to be followed when system changes are required. Changes are to occur after at a specified time when the system is approved for maintenance and deemed less critical for the maintenance to take place.

Risk #11 - There is not a patch management process for the ACME Server, or the patch management process is not being followed.

Probability	Medium
Priority	High
Impact	Without a patch management process, the operating system and application may not receive critical service packs and hotfixes to prevent against malicious code or viruses
Control Objectives	To maintain availability of the ACME server, all published vulnerabilities and exploits must be examined to determine if the server is vulnerable. If the server is at risk due to a published vulnerability, the service pack or hotfix should be given to the change control group for approval of implementation. System administrators should be signed up with credible advisors such as Cert, Microsoft, or Avert Labs for automatic notifications for vulnerabilities and virus updates.

Risk #12 - The ACME database is not being backed up, or a recent restore has not been tested.

Probability	Medium
Priority	High
Impact	The complete loss of data for an extended amount of time
Control Objectives	To maintain availability of the ACME server, a daily backup to tape needs to be performed, as well as a weekly off-site backup plan. Testing of the backups should be performed every 2 weeks to ensure the backups are successful.

Risk #13 – A disaster recovery plan for the security system is not in place.

Probability	Medium
Priority	High
Impact	The loss of data up to 7 days could occur.
Control Objectives	To maintain availability of the ACME data, an off-site redundant server needs to be identified in the event of a complete loss of hardware and data on the primary ACME server.

Risk #14 - A vender or third party has access to the server or application administrator accounts

Probability	High
Priority	High
Impact	If a vender or third party has access to the administrator account on the server or for the application, unauthorized system or application changes could occur, leaving the system vulnerable or the application not functioning properly.
Control Objectives	To maintain availability of the ACME server and application, all venders or third parties should have minimal access rights and be restricted from making system and application level changes. Any of these changes that a vender would need

	performed, should be performed by the administrator and not by themselves with administrator privileges.

Risk #15 - The ACME client workstations are not secure due to the security officers having administrator access or downloading and installing unnecessary applications

Probability	High
Priority	Medium
Impact	A workstation could become unavailable due to malicious code or a virus that the security officer may contact while accessing the internet or email. The security officer may also damage, remove, or modify system files or install system corruption applications if the officer has administrator privileges. Also, by permitting security officers to install or run unnecessary applications, it could cause a distraction to their job-duties of monitoring alarms and building security
Control Objectives	To maintain the availability and integrity of the ACME client workstations, restrict all users from installing any new services or applications. Do not permit the use of the internet by security officers and limit their network access privileges.

Risk #16 - The ACME users may have more access to the application then needed.

Probability	Medium
Priority	Medium
Impact	An ACME user may have more privileges then needed. Security officers, venders, or a third party support technician may have more privileges to the application then needed. This could lead to unauthorized application changes, clearance code modifications, removal of system administrators from the root class or the deletion of approved users, workstations, or badge holders
Control Objectives	To maintain the integrity of the ACME application, the removal of everyone from the root class except the system administrators is necessary. All security officers will not have the ability to add, remove, or modify system information, and venders and support technicians will not have the ability to add, remove, or modify badge holder or clearance code settings.

Risk #17 – There may be ACME application users that are not authorized to access the system.

Probability	Medium
Priority	Medium
Impact	An active ACME account may still exist for terminated or resigned security officers or administrators. This could lead to someone using the account to make unauthorized application

	changes, clearance code modifications, removal of system administrators from the root class or the deletion of approved users, workstations, or badge holders
Control Objectives	To maintain the integrity of the ACME application, the removal of all terminated or resigned security officers and administrators will be removed from the application immediately upon leaving XYZ Enterprises.

Risk #18 – Unauthorized system changes could occur from a remote computer if there are profiles created for workstations within ACME that can not be identified or have not been approved for access.

Probability	Medium
Priority	Medium
Impact	An ACME user may be able to access ACME from a remote locating leading to unauthorized application changes, clearance code modifications, removal of system administrators from the root class or the deletion of approved users, workstations, or badge holders
Control Objectives	To maintain the integrity of the ACME application, the removal of all workstations not approved by the administrator will be removed. Only the system administrator will have the ability to create a workstation profile within the ACME application.

Risk #19 – XYZ Enterprises employees and contractors may have access to secured areas that they may not have been authorized

Probability	High
Priority	High
Impact	A badge holder could gain access to an unauthorized area such as the safe room, records room, or one of the data centers by being assigned to the incorrect clearance code, or from bypassing the guidelines for obtaining a badge.
Control Objectives	To maintain complete building security, strict guidelines and policies must be established for assigning secure and off-limit area’s such as the data center and security operations center to a badge holder. The ability to add, remove, or edit a badge holder must also be kept to a minimum and be written to an application event log that is monitored by the system administrator

Risk #20 - A security officer does not respond to an alarm or incident

Probability	High
Priority	High
Impact	The impact here is limitless, an alarm could range from a door propped open to a panic alarm for a senior level executive. If a security officer is distracted or the alarm monitor is closed on the computer the security officer may not receive the alarm. If

	the system is offline, or the workstation is unavailable, the security officers will not be able to monitor alarms and respond to incidents that may occur.
Control Objectives	To maintain the availability of the ACME application for responding to incidents, maintenance to the server and workstations should only happen during non-working hours. A redundant server should be identified for the application in case of complete failure or corruption, as well as workstations. A standard operating system image should be created for the quick rebuild of a workstation, and all applications that do not promote the access control system should be removed from the workstations to prevent distracting the security officers. The administrator should be monitoring reports and event logs to ensure the alarms being created are valid and not overwhelming to the on-duty security officers.

What Is The Current State Of The System

This audit is focused on a high level overview of the access control system XYZ Enterprises relies upon in their day to day operations of maintaining a secure area for the employees and assets of the company. Resources devoted to auditing an access control system as a whole are limited, but breaking it down into separate modules such as the operating system, database engine, application, physical security, and policies and procedures, resources are more readily available. Opening this audit to the specific technical details of each component would extend the scope of this audit to a much larger capacity, making it much more detailed and complicated, but if you extract the most critical pieces from each component, we will receive a finished report that is much more to our goal of obtaining a high level overview.

The operating system on the ACME server and workstations are Microsoft 2000 Server and Professional, respectively, and the database is using Microsoft SQL 2000. Resources on these three components are plentiful from Microsoft's "TechNet" published at http://www.microsoft.com/technet/ Other resources used are "Mastering Windows 2000 Server" and "Mastering Windows 2000 Professional" both written by Mark Minasi, "Hacking Windows 2000 Exposed" by Stuart McClure (President CTO of Foundstone) and Securing Windows 2000 Professional Using the Gold Standard Security Template" by SANS Press. Various other white papers from the "Reading Room" at www.SANS.org were also looked at for valuable documentation. Security scoring tools such as Microsoft's Baseline Security Analyzer, (http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=e987ab2f-3c97-4fdc-aa7b-21992ff9af7a) and the Center for Internet Security's Benchmark and Scoring Tool (http://www.cisecurity.com/benchmarks.html)were used to find the known state of the workstations and the ACME application server.

For the physical access control system audit, doing global searches on www.google.com, www.msn.com, and www.yahoo.com proved to be of little help in locating resources to use in the audit of the ACME application. An ACME application user guide and system documentation were acquired from a contact on their website www.nexwatch.com. Two resources were found in the SANS Reading Room, "Protect Yourself" by Justin Bois (http://www.sans.org/rr/papers/index.php?id=271), and "Building the Ideal Web Hosting Facility: A Physical Security Prospective" by Seth Friedman (http://www.sans.org/rr/papers/index.php?id=270) were also helpful in identifying risks and providing solutions in their papers.

XYZ Enterprises provided their policies and procedures to assist in the audit of their standard processes.

- Anti-virus practices for Windows 2000 Server and Professional
- Local Security Policy for Windows 2000 Server and Professional

- Patch Management Policies
- Change Management Policies
- Disaster Recover and Business Continuity Practices
- Obtaining Ethernet Network Connectivity Policy
- Badge Approval Policy
- Badge Creation Policy

Assignment 2 – Create an Audit Checklist

Checklist Item #1 – Physical Security of the Server

Reference	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/5min/5min-203.asp
Control Objective	The ACME server must be properly secured in an environment with limited access
Risk	• Physical damage to the server as well as the insertion of a bootable disk in the CD-ROM or Floppy Drive may occur. A complete server failure could occur at the expense of unauthorized physical access to the server • The probability is rated: LOW • The is impact is rated: HIGH.
Compliance	• Physical access to the server will be restricted to the system administrators or other approved support personnel by electronic access control. • The ability to add or delete access to the room where the server is stored will be restricted to the system administrators.
Testing	• Review a copy of the clearance list for employees who can access the room where the server is stored. • Review a list of people who can add others to the clearance list and review to ensure that the system administrators are the only ones with this privilege. • Physically attempt alternate means of entry into the room. Raised floors, removable ceiling panels, and a “drywall only” wall are easy ways to bypass the access control devices and gain access to the secured room. • Ensure that the server cabinet is locked and the key is not available to anyone not on the approved access list.
Objective / Subjective	Objective

Checklist Item #2 – Service Packs, and Hotfixes

Reference	Microsoft Baseline Security Analyzer http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=e987ab2f-3c97-4fdc-aa7b-21992ff9af7a
Control Objective	• Correct published vulnerabilities in the Microsoft Windows operating system to minimize the risk of a denial of service/operation or system compromise from a virus or Trojan horse.
Risk	• Each service pack or hotfix corrects a publicly published vulnerability, of which many have malicious code to exploit the vulnerability. Without applying the patches the server is left in an unsecured state. • The probability is rated: High • The impact is rated: High
Compliance	There are no security patches or updates that apply to this system that are not installed
Testing	Download the Microsoft Baseline Security Analyzer from www.microsoft.com By performing a search on www.google.com other places to download the scanner

	are identified, but not recommended as the source of the tool can not be identified.
Objective / Subjective	Objective

Checklist Item #3 – Rename the Server Administrator Account

Reference	• XYZ Enterprises server password policy • Mastering Windows 2000 Server • http://support.microsoft.com/default.aspx?scid=kb;en-us;320053&Product=win2000
Control Objective	Elevate the difficulty it would take for a hacker to acquire the administrator username and password by renaming it to a name appearing as a general user account.
Risk	• The Windows 2000 Server Administrator account has a default name of "administrator". Since this account can not be locked out, someone could attempt to guess the password with brute force as many times as they wish without ever getting locked out. Leaving the name set to its default settings makes it much easier to locate a user account with administrator privileges. • The probability is rated: LOW • The impact is rated: HIGH
Compliance	The administrator account is renamed from its default name
Testing	• Right-click on My Computer and select Manage from the list • Expand the System Tools folder • Expand the Local Users and Groups folder • Open the Users folder • Browse the list for a user named Administrator.
Objective / Subjective	Objective

Checklist Item #4 – Server User Accounts and Group Settings

Reference	• XYZ Enterprises User Account and Password Policy • Mastering Windows 2000 Server • http://windowsecurity.com/articles/Passwords_Improve_Windows_Security_Part1.html
Control Objective	Identify non-authorized local user accounts on the server, as well as members of the administrator and users group that do not have a need to log on to the server
Risk	• Non-authorized local accounts or elevated privileges on the server could allow accidental or intended loss of data or system corruption. • The probability is rated: LOW • The impact is rated: HIGH
Compliance	Local user accounts and group privileges are approved by the system administrator and all passwords meet the requirements specified in the XYZ User Account And Password Policy.
Testing	• Right-click on My Computer and select Manage from the list • Expand the System Tools folder

	- Expand the Local Users and Groups folder - Open the Users folder - Identify unauthorized local user accounts and remove those. - Open the Groups folder - Open each of the Administrators, Backup Operators, Guests, Power Users, Replicator, and Users folders and remove any accounts from the folders for which permissions have not been granted.
Objective / Subjective	Objective

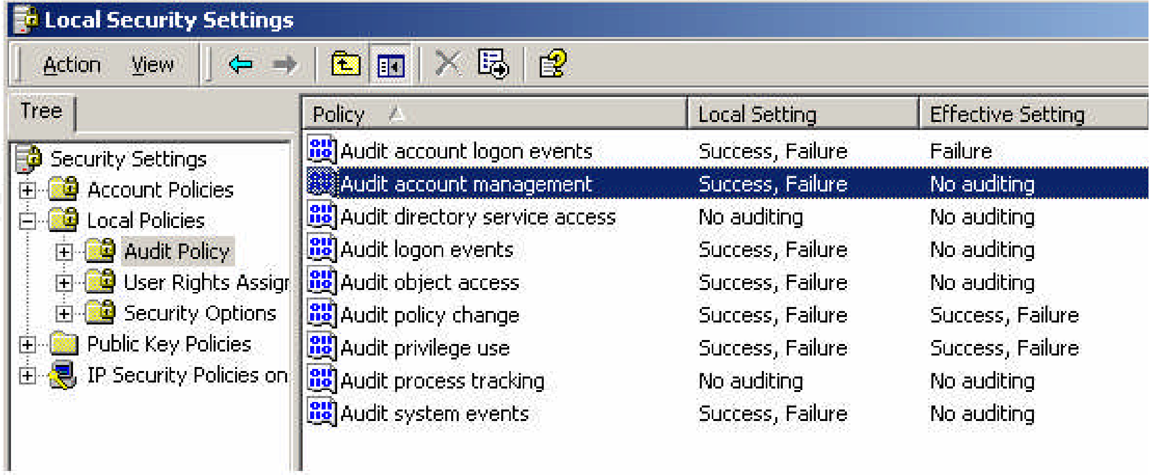
Checklist Item #5 – System Logon and Policy Auditing

<table>
<tr><td>Reference</td><td>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/maintain/monitor/logevnts.asp</td></tr>
<tr><td>Control Objective</td><td>Audit account logons, logon events, account management, object access, policy changes, and system events.</td></tr>
<tr><td>Risk</td><td>

- An attacker could remain unidentified as well as the inability to identify when a system policy change occurred if auditing is not enabled
- The probability is rated: High
- The impact is rated: High

</td></tr>
<tr><td>Compliance</td><td>In the Local Security Policy, Audit Policy for Audit Account Logon Events, Audit Account Management, Audit Logon Events, Audit Policy Change, Object Access, Policy Change and System Events are enabled and are set to log for both success and failure.</td></tr>
<tr><td>Testing</td><td>

- In the Control Panel open the Administrator Tools folder.
- In the Administrator Tools folder, click on Local Security Policy
- In the Local Security Policy Window, expand the Local Policies folder
- Open the Audit Policy folder
- The Local Setting in the preview pane displays “Success, Failure” for Audit Account Logon Events, Audit Account Management, Audit Logon Events, Audit Policy Change, Object Access, Policy Change and System Events



<table>
<tr><th>Policy</th><th>Local Setting</th><th>Effective Setting</th></tr>
<tr><td>Audit account logon events</td><td>Success, Failure</td><td>Failure</td></tr>
<tr><td>Audit account management</td><td>Success, Failure</td><td>No auditing</td></tr>
<tr><td>Audit directory service access</td><td>No auditing</td><td>No auditing</td></tr>
<tr><td>Audit logon events</td><td>Success, Failure</td><td>No auditing</td></tr>
<tr><td>Audit object access</td><td>Success, Failure</td><td>No auditing</td></tr>
<tr><td>Audit policy change</td><td>Success, Failure</td><td>Success, Failure</td></tr>
<tr><td>Audit privilege use</td><td>Success, Failure</td><td>Success, Failure</td></tr>
<tr><td>Audit process tracking</td><td>No auditing</td><td>No auditing</td></tr>
<tr><td>Audit system events</td><td>Success, Failure</td><td>No auditing</td></tr>
</table>

</td></tr>
<tr><td>Objective / Subjective</td><td>Objective</td></tr>
</table>

Checklist Item #6 – Verify Event Logs are Maintained and Reviewed Regularly

Reference	http://www.cert.org/security-improvement/practices/p092.html
Control Objective	To identify an attack or attempted attack on the server. Failed logins, and attempted changes to system files or data will give notice of attempted intentional system corruption
Risk	• By failing to review the security logs, an attacker could remain unidentified as well as the inability to identify when a system policy change occurred. • Probability is rated: Medium • Impact is rated: Medium
Compliance	Perform interview with System Administrators. Questions: • Are the log files being reviewed on a daily basis? • Are the log files being stored for longer then 1 week on the server? • Are the log files being archived for longer then 6 months
Testing	• Interview all systems administrators
Objective / Subjective	Subjective

Checklist Item #7 – Disable Any Unnecessary Services on the Server

Reference	• "Securing Windows 2000 Professional Using the Gold Standard Security Template" – SANS Press • Microsoft Baseline Security Analyzer
Control Objective	Verify that any unnecessary services not pertaining to the role of the AMCE application server are not installed or disabled
Risk	• By installing unnecessary services, you expand the avenues of approach to a hacker. Services such as IIS, RAS, RPC, Terminal Services, SQL Server all have security flaws that could allow a hacker access to the server. By disabling services that are not needed, you eliminate the need to patch future vulnerabilities in these services. • Probability is rated: High • Impact is rated: Medium
Compliance	Unnecessary services not installed or disabled on the ACME application server include: • Application Manager • Automatic Updates • ClipBook • Distributed Link Tracking • Fax Service

	• FTP • Indexing Service • IIS Admin Services • Internet Connection Sharing • Intersite Messaging • License Logging Service • Kerberos Key Distribution Center • Smart Card • Smart Card Helper • Telnet • Utility Manager • Any RAS Services
Testing	• Run Microsoft Baseline Security Analyzer • On the Security Report, open Additional System Information section, locate Services and • Click Services, then Results • Identify from the list, services that can be stopped or removed • Secondly, open the Control Panel and open the Administrator Tools Folder. • Open the Services folder and compare the list of running services on the server to the list defined in the Compliance section of this checklist.
Objective / Subjective	Objective

Checklist Item #8 – Verify Shared Folders on the Server

Reference	• Microsoft Baseline Security Analyzer • Personal Experience
Control Objective	To restrict access to the data that resides on the ACME Application Server
Risk	• Data on the server could become intentionally or unintentionally corrupted, overwritten, deleted, or inappropriately accessed. • Probability is rated: High • Impact is rated: Low
Compliance	Only authorized users have access to shares on the ACME applications server, to include Administrators and Application users.
Testing	• Run Microsoft Baseline Security Analyzer • On the Security Report, open Additional System Information section, locate Shares and Results • This will identify all shares on the server and who the folder is shared too.

	- Identify the contents of each shared folder and verify appropriate level access to each share. User data should be shared to the ACME users, and the Administrator folders should only provide access to the Administrator Group. No folder should be shared to "Everyone"
Objective / Subjective	Objective

Checklist Item #9 – Server Anti-Virus Practices

Reference	- XYZ Enterprises Anti-Virus Policy - http://www.nai.com/us/index.asp
Control Objective	Ensure that the anti-virus software is installed, up to date, and set to automatically update itself every day
Risk	- If the Anti-virus software is not installed or the signature files is not up to date a virus could infect the server making it unavailable as well as system corruption. - Probability is rated: Low - Impact is rated: High
Compliance	The server will run Network Associates Netshield 4.5 and will be configured to "AutoUpdate" on a daily basis.
Testing	- Click on the Start Menu, then Program Files, then Network Associates, then Netshield Console. - Click on Help, then About, this will give you the current version - Next click on Tools, then Automatic Updates from the Console Menu - The FTP Source radio button should be checked - The FTP Source should be set to ftp.nai.com/virusdefs/4.x - The Log Activity radio button should be checked - On the Menu Bar, click on File, then Properties - The properties window will appear an make sure the files to scan option is set to "All files" - Open the Activity Log to verify that the AutoUpdate feature is properly working and the most recent version is that found as the current version on www.nai.com
Objective / Subjective	Objective

Checklist Item #10 – Change Control Policy

Reference	- XYZ Enterprises Change Management Policy
Control Objective	To ensure that only authorized system changes are made

	after documentation, research, and thorough testing are made. The changes are to occur at a specific time when the system is deemed less critical and resources are available for additional repairs or unexpected failure.
Risk	• By allowing changes that are not documented or tested could leave the server in an unknown state. Multiple changes that are made at the same time could provide a more lengthy amount of down time to rollback the changes that occurred if they are non-compliant. • Probability is rated: Medium • Risk is rated: High
Compliance	All system changes and outages for maintenance are scheduled in advance, and are approved after being documented and tested for compliance. Emergency changes or repair is performed after submitting an emergency change notice and approved. In addition to scheduled and emergency changes, a rollback plan is also submitted for non-compliant changes to return to original system settings.
Testing	• Review XYZ Change Management Policy • Review recent changes that took place and review documentation, roll back plans, and compliance. • Interview System Administrators and Managers of Production Operations.
Objective / Subjective	Subjective

Checklist Item #11 – Patch Management Practices

Reference	• XYZ Enterprises Patch Management Policy • http://www.microsoft.com/security/security%5Fbulletins/ • ACME application technical support.
Control Objective	To ensure that compliant system changes are implemented by authorized administrators
Risk	• A security patch or service pack is implemented that is non-compliant with the current version of the application or the operating system. • Probability is rated: High • Impact is rated: High
Compliance	A security patch or system service pack is only implemented after the following steps have been met: • A security patch, service pack, or software upgrade is released by Microsoft or ACME • Recommendations are obtained from ACME technical support if the patch or service pack is compliant

	• Testing of the patch or service pack is performed on an offline system, in a research lab • Documentation of the testing is created and a rollback plan is established • Approval by the Change Management department
Testing	• Review XYZ Patch Management Policy • Review recent changes that took place and review documentation, roll back plans, and compliance. • Interview System Administrators and Managers of Production Operations
Objective / Subjective	Subjective

Checklist Item #12 – Backup and Restore Process

Reference	• XYZ Enterprises Backup and Restore Policy • http://www.labmice.net/Windows2000/Backup/default.htm
Control Objective	Ensure that proper backup policies are in place to archive application data.
Risk	• The integrity of the application data becomes compromised. If a known good backup were not available, the recovery of the system would not be possible. • Probability is rated: Medium • Impact is rated: High
Compliance	Complete system backups will be performed to tape daily, and tested on a bi-weekly basis.
Testing	• Click on Start, then Program Files, then Microsoft SQL Server, and then Enterprise Manager. • Expand Microsoft SQL Servers, Expand SQL Server Group, Expand ACME Database Server Name, Expand Management, and select Database Maintenance Plans. • In the right pane, double click on the backup plan for the ACME application. • On the General Tab, make sure the ACME Database is selected, as well as the Master and the MSDB database files • On the Complete Backup Tab, identify the location of where the backups are being saved. • Also on the Complete Backup Tab, ensure that a backup is being performed daily. • Go to the E:\Database Backups folder and ensure that the backups are being created. • Backups are also made to a tape, which are then stored offsite for redundant storage and disaster

	recover. Open BackupExec's Activity Manager and click on the activity tab. You will see all completed and failed jobs, start and end time, and byte count. • Now that the backups exist, check them to see if they will restore by clicking Restore Database from the Tools Menu Bar in the Enterprise Manager. • In the Restore Database window, select your database and what version, and click ok. This will start the restore.
Objective / Subjective	Objective

Checklist Item #13 – Disaster Recovery Plan

Reference	• XYZ Enterprises Disaster Recovery Plan • http://www.labmice.net/Windows2000/Backup/default.htm
Control Objective	Identify the contingency plan if the ACME Server becomes unavailable due to a complete hardware failure or loss.
Risk	• In the event of a disaster the ACME database would be key in identifying employees, guests, and non-authorized personnel inside the building prior to the disaster. It would also have alarms and events up to the time that the disaster occurred making the data important in identifying the source of an internal incident. Not having a contingency plan would prevent the restore of the data and system to it's current state. • Probability is rated: LOW • Impact is rated: HIGH
Compliance	In the event of a disaster to the building, the stand up of a new security system is not necessary although a contingency plan for protecting the building and area would be required. The current data and the previous tape backups would need to be recovered for use in identifying probable cause to the building by former employees and guests, so there will be an immediate need for a server to perform a data backup
Testing	• Obtain an off-site tape backup from the off-site data protection location. • At the off-site redundant data center, restore the tape acquired from off-site tape backups. • There is no accurate way of knowing that you will be able to recover the server or data that was on the server at the time of the disaster.
Objective / Subjective	Subjective

Checklist Item #14 – Vender Server and Application Access Policy

Reference	Personal Experience
Control Objective	To prevent the unauthorized changes to the server, workstation, or a person's access control card
Risk	• By giving the vender administrator access to the server and application, you are allowing the vender to possibly bypass the change management and patch management policies. Changes could be performed that XYZ Enterprises is not aware of that could lead to the integrity of the system or data. With VPN access the vender could possibly remotely connect to make system changes to intentionally make the system unavailable to force XYZ Enterprises to make a service call. • Probability is rated: Medium • Impact is rated: Critical
Compliance	The vender will not access the system without first notifying the system administrator. At no time will the vender be left alone with administrator access on the server or the application. The vender will not be able to log on locally to the server. The vender will not have VPN or dialup access to the XZY Enterprises network for remote access.
Testing	• Right-click on My Computer and select Manage from the list • Expand the System Tools folder • Expand the Local Users and Groups folder • View the group to make sure the Vender's user account is not here • Open ACME software and click on the Management Icon on the left side • Click on Classes • Open the Root Class • Ensure that Vender account is not here • Click on Users and Expand the Badges Column and the Query option should be the only option displayed
Objective / Subjective	Objective

Checklist Item #15 – Workstation Access Policy for Security Officers

Reference	• Personal Experience
Control Objective	Restrict the security officers using the ACME application to the most basic workstation privileges.
Risk	• Security officers typically have a minimal computer skill set and may inadvertently overwrite or delete a file, install a virus from an Internet download, or

	distract them from monitoring alarms if they have other additional computer resources such as the Internet or Games available
Compliance	Remove any unnecessary privileges and applications from the workstation
Testing	• Right-click on My Computer and select Manage from the list • Expand the System Tools folder • Expand the Local Users and Groups folder • Open the Users folder • Identify unauthorized local user accounts and remove those. • Open the Groups folder • Open each of the Administrators, Backup Operators, Guests, Power Users, Replicator, and Users folders and remove any accounts from the folders for which permissions have not been granted. • Removing Internet connectivity is a bit more difficult. The easiest way to remove it from some is to edit the security options in the C:\Program Files\Internet Explorer. Open My Computer and open the C: Drive, then open Program Files folder. Right click on Internet Explorer and select properties • When the Properties Window appears, click on the security tab and remove the group "Everyone" from the list and click ok. Now only administrators of the computer will be able to access Internet Explorer. The XYZ Enterprises computer image does not allow you to access the Internet through any other application (Outlook and Netscape) • Open the control panel and select Add/Remove Programs. When the Add/Remove box appears, select any program that does not pertain to the role of the workstation and remove it. (The XYZ Enterprises computer image does not have any additional applications loaded on here, so any that are here have been added and additional steps need to be taken to address how they were installed. The XYZ Enterprises policy for security officer computers also states that no security officer shall install any software or make any configuration changes to the workstation. Again, if any changes are made, additional steps need to be taken to find the source of the installation.)
Objective / Subjective	Objective

Checklist Item #16 – ACME Application Account Privileges

Reference	• Personal Experience of the ACME System Administrator and Security Officer Account Manager. • ACME users manual
Control Objective	Limit each ACME user to an associated group for the amount of access required to the application as necessary
Risk	• A user may have more access in the application then necessary, resulting in application changes that are incidental or intentional. • The probability is rated: High • The impact is rated: High
Compliance	All administrators are assigned to an Administrators Class with full control. The venders are assigned to a Vender Class where they can add/edit/ and remove hardware, but not modify badges. The Security Operations Center Class is able to modify badges, but not modify system hardware. The Lobby Officer Class is not able to modify any item, only view.
Testing	• Obtain a list of all Security Guards at the XYZ Enterprises corporate headquarters building with their assigned post. • Obtain a list of all Venders and administrators from the system administrator. • Open the ACME application • Click the Management Icon, then click Class. • Open, the Root Class, Vender Class, Lobby Officer Class, and the Security Operations Center Class and ensure the respective accounts are in the correct classes. • Now the User to Class is verified, click on the Programs Tab on the Edit Class Window. This will display all of the area's that the class has access to, along with the privilege of Add, Modify, Delete, or Query. Administrators should have the ability to Add, Modify, Delete, or Query on any area. The Venders should only be able to Add, Modify, Delete or Query on the Hardware specific items (Panels, door readers. Security Operations Class should be able to only Add, Modify, Delete, or Query on Badge related areas, and the Lobby Guard Class should only have Query on Badge related areas.
Objective / Subjective	Objective

Checklist Item #17 – Verify Authorized ACME Users

Reference	Personal Experience of the ACME System Administrator and Security Officer Account Manager Help Desk trouble ticket report for terminated employees
Control Objective	Limit the use of the ACME application to authorized and current users.
Risk	• An active account for a terminated or resigned security officer may still be activated on the XYZ Enterprises domain and on the ACME application. • Probability is rated: HIGH • Impact is rated: HIGH
Compliance	Only authorized and current users of the ACME will have an ACME user account.
Testing	• Obtain a list of all Security Guards at the XYZ Enterprises corporate headquarters building with their assigned post. • Obtain a list of all Venders and administrators from the system administrator. • Open the ACME application • Click the Management Icon, then click Users • Verify that the user accounts created within ACME are current and authorized from the administrator's and Account Manager's list. • Delete and non-authorized or non-current user account from ACME and place a trouble ticket with the help desk for the removal of the respective domain account. • To verify that terminated and resigned security officers domain accounts have also been deleted, obtain reports from the help desk in the name of the system ACME administrator who creates new users for the previous 6 months. • Obtain a list of terminated or resigned security officers from the Account Manager who have left XYZ Enterprises in the previous 6 months. • Compare the Help Desk report with that of the Account Manager to see if the ACME administrators are requesting the deletion of domain accounts for terminated or resigned security officers
Objective / Subjective	Objective

Checklist Item #18 – Verify Authorized ACME Workstations

Reference	• Personal Experience of the ACME System Administrator
Control Objective	Provide a 2nd layer of security by limiting the use of the

	ACME application to authorized workstations.
Risk	• Changes to the ACME application could be performed from an unauthorized access point. • Probability is rated: LOW • Impact is rated: High
Compliance	ACME application access will only be available on authorized workstations.
Testing	• Obtain a list of all authorized workstations from the System Administrator • Open the ACME application • Click the Management Icon, then click Workstations. • Verify that the workstation accounts created within ACME are on the administrator's authorized list. • Delete non-authorized or non-current workstation accounts from ACME application.
Objective / Subjective	Objective

Checklist Item #19 – Process of Assigning Clearance to a Controlled Area

Reference	• Personal Experience of the Security Officer in the Security Operations Center and System Administrator • XZY Security Policy for New or Modifying Badges
Control Objective	To limit access to secured areas
Risk	• An employee may have unauthorized access to a secured area, allowing physical access to the area and an unlimited amount of risks ranging from theft to property damage. • Probability is rated: HIGH • Impact is rated: HIGH
Compliance	Employees and Contractors will only be given access to areas approved by the manager responsible for the controlled area.
Testing	• Audit the process of obtaining clearance to a secured area by locating an employee with limited "Commons Area" access. • Have the employee go to the Security Operations Center without the necessary approval form for obtaining clearance a secured area. • Continuously ask the security officer to modify the badge to access the secured area, explaining the approving manager is out of the office and the employee needs access to the area. Secondly, open ACME, click reports, then expand the

	Badge Holder Reports option and select the Badge Holder Summary report. Select all users for each of the clearance codes and verify with the approving manager of each secured location that the list of employees and contractors are authorized. • Remove any unauthorized findings.
Objective / Subjective	Objective

Checklist Item #20 – Security Officer Response and Incident Handling Process

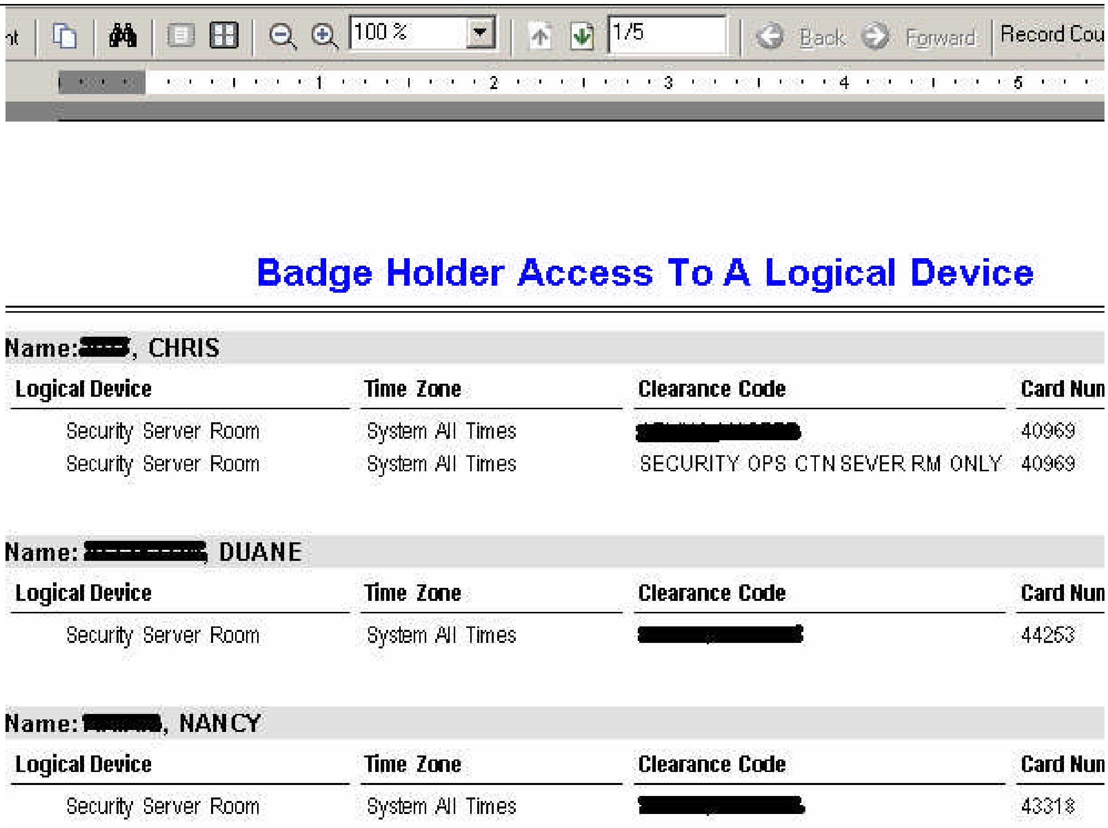
Reference	• Personal experience of a security officer. • Corporate Security's Incident Handling and Response Log Book • XYZ Enterprises Incident Handling and Response Policy
Control Objective	Ensure that all reported incidents and automated alarms are properly handled.
Risk	• An alarm goes unnoticed, or an incident is mishandled. The consequences for not responding to an incident are limitless. The consequences could be as small a door held open for a longer period then expected, to a life endangering situation. • The probability is rated: HIGH • The impact is rated: HIGH
Compliance	Security officers will remain vigilant and alert and monitor alarms and notified incidents with the utmost priority.
Testing	• Review the Corporate Security Incident Handling and Response Log Book to ensure past incidents have been logged and responded to properly. • Call in a situation to the Security Operations Center to review how the call is handled, if another officer was dispatched to the location in a timely manner and that the incident was handled properly. • Activate some of the panic button alarms throughout the senior management offices to see how quickly a call to the office is made, how quickly that an investigating security officer appears, and that the incident is handled according to the XYZ Enterprises Incident Handling and Response Policy
Objective / Subjective	Objective

Assignment Three – Audit Evidence

The following 10 items are believed to be the most valuable and critical in the system to audit. The impact of the exploited risk and the likeliness of the incident to happen are the factors for determining the list.

Audit #1 – Physical Security of the Server

Reference	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/5min/5min-203.asp
Control Objective	The ACME server must be properly secured in an environment with limited acces
Risk	• Physical damage to the server as well as the insertion of a bootable disk ir the CD-ROM or Floppy Drive may occur. A complete server failure could occur at the expense of unauthorized physical access to the server • The probability is rated: LOW • The is impact is rated: HIGH.
Compliance	• Physical access to the server will be restricted to the system administrator other approved support personnel by electronic access control. • The ability to add or delete access to the room where the server is stored be restricted to the system administrators.
Test Steps	• Review a copy of the clearance list for employees who can access the roo where the server is stored. • Review a list of people who can add others to the clearance list and review ensure that the system administrators are the only ones with this privilege. • Physically attempt alternate means of entry into the room. Raised floors, removable ceiling panels, and a “drywall only” wall are easy ways to bypas the access control devices and gain access to the secured room. • Ensure that the server cabinet is locked and the key is not available to anyone not on the approved access list.
Actions	• Open the ACME application, then click on the Reports Icon. • Select the “Badge Holder Access to a Logical device” report from the list. • Browse the list of logical devices and select “SECURITY SERVER ROOM” and click “Preview Report”. • The list shows 57 Employees who contain access to the room where the ACME access control server is located. This is far more then the two identified system administrators.



Badge Holder Access To A Logical Device

Name: [redacted], CHRIS

Logical Device	Time Zone	Clearance Code	Card Nun
Security Server Room	System All Times	[redacted]	40969
Security Server Room	System All Times	SECURITY OPS CTN SEVER RM ONLY	40969

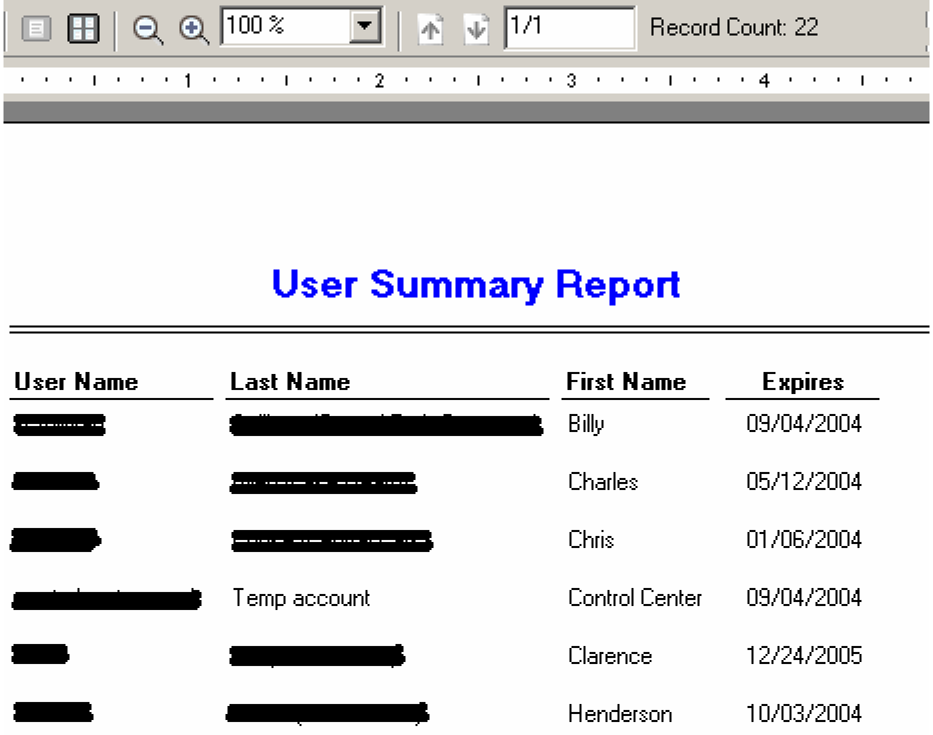
Name: [redacted], DUANE

Logical Device	Time Zone	Clearance Code	Card Nun
Security Server Room	System All Times	[redacted]	44253

Name: [redacted], NANCY

Logical Device	Time Zone	Clearance Code	Card Nun
Security Server Room	System All Times	[redacted]	43318

- Open the ACME application, then click on the Reports Icon.
- Expand the “Configuration Report” option, the choose “Class”.
- Browse the list of Classes and select “Root” and “Security Operations Cen and click “Preview Report”.
- The following report was obtained, which shows 22 users of the system, al which were authorized. One thing to point out is the discovery of a temp u account not assigned to someone, and used for a temporary guard.

<table>
<tr><td></td><td>


100 %

1/1

Record Count: 22

User Summary Report

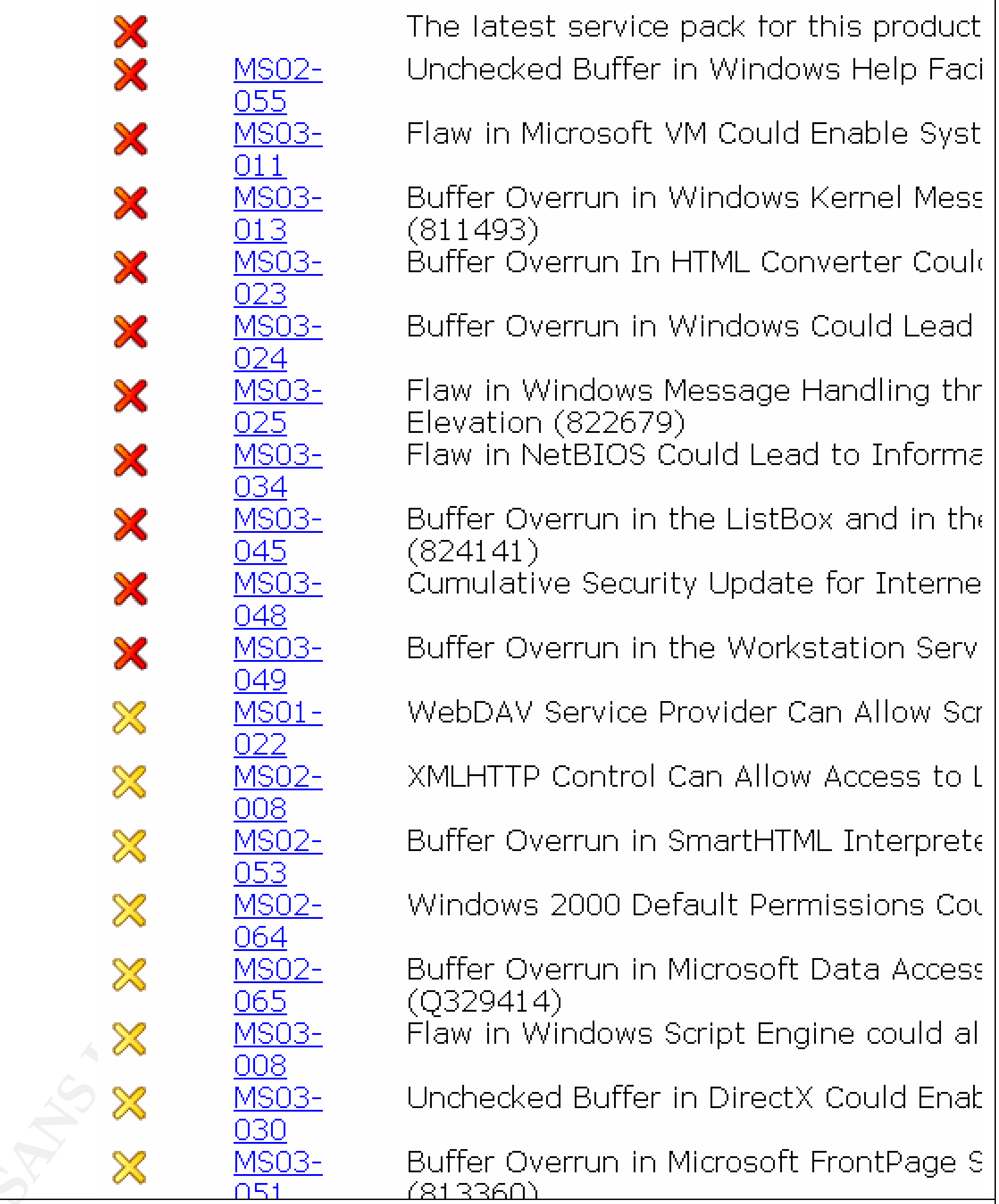
<table>
<tr><th>User Name</th><th>Last Name</th><th>First Name</th><th>Expires</th></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>Billy</td><td>09/04/2004</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>Charles</td><td>05/12/2004</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>Chris</td><td>01/06/2004</td></tr>
<tr><td>[redacted]</td><td>Temp account</td><td>Control Center</td><td>09/04/2004</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>Clarence</td><td>12/24/2005</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>Henderson</td><td>10/03/2004</td></tr>
</table>

- Physically attempted an alternate means of entry into the room. The floors are raised but entry into the room is prevented by the concrete floor suppo A small conduit is available only for passing cable and wire through and would not allow entry into the room. The ceiling has similar restrictive measures as the concrete support for the floor above prevents access through the ceiling. The walls are made out of wood with steel supports, making entry by cutting through an option, but very noisy. There is a secu officer within 10 feet of the room and the determination is made that any cutting would be heard by the security officer.
- Attempted to open the cabinet without a key, and was able to open the doo to obtain physical access to the server.
</td></tr>
<tr><td>Result</td><td>Failed – There are too many employees with access to this room that can open th door to the server room. Once inside the server room, there is no restrictions currently in place to stop someone from opening the server cabinet to shut down insert a disk into the server.</td></tr>
</table>

Audit #2 – Service Packs and Hotfixes

Reference	Microsoft Baseline Security Analyzer http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=e987ab2f-3c97-4fdc-aa7b-21992ff9af7a
Control Objective	Correct published vulnerabilities in the Microsoft Windows operating system to minimize the risk of a denial of service/operation or system compromise from a virus or Trojan horse.
Risk	• Each service pack or hotfix corrects a publicly published vulnerability, of which many have malicious code to exploit the vulnerability. Without applying the patches the server is left in an unsecured state.

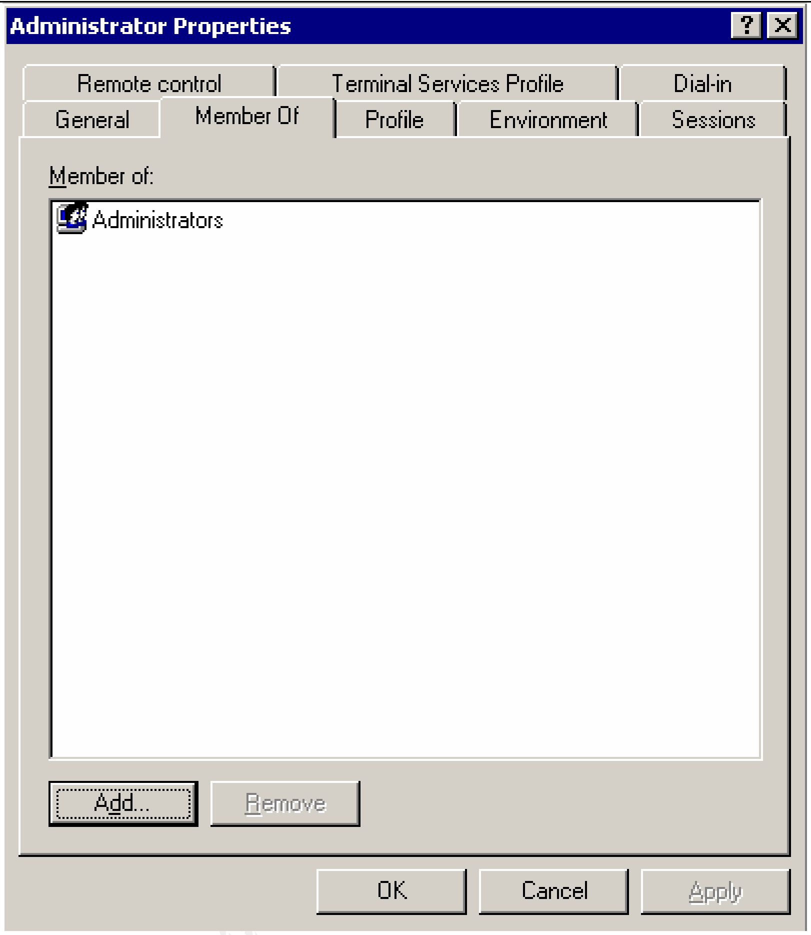
	• The probability is rated: High • The impact is rated: High
Compliance	All security patches or updates that apply to this system are installed
Test Steps	• Download the Microsoft Baseline Security Analyzer from http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=e987ab2f-3c97-4fdc-aa7b-21992ff9af7a • Complete the installation of the MBSA tool and open the application. • Type the IP address of the server, select all of the options and click “Start Scan” • Scroll down the report until you see “Windows Scan Results” and the “Windows Hotfixes” Issue. Here you will see the number of missing or unconfirmed hotfixes. • Click on “Result Details” to search the identified critical updates for this server. Because this Server is running Microsoft Windows 2000 Server SP3 and MS SQL Server 2000 SP3, the only required security updates are: o MS03-026 o MS03-033 o MS03-039 o MS03-041 o MS03-042 o MS03-043 o MS03-044
Actions	• Logged into a Windows 2000 Workstation as an administrator account. • Completed the installation of the MBSA tool and opened the application. • Entered the IP address of the server, and selected all of the options began the scan of the ACME server • Opened the scan report and located the “Windows Scan Results”. The MBSA identified 17 missing hotfixes and updates • Click on “Result Details” to search the identified critical updates for this server. Reviewed the list to see if any of the following updates are missing: o MS03-026 o MS03-033 o MS03-039 o MS03-041 o MS03-042 o MS03-043 o MS03-044

	 ❌ The latest service pack for this product ❌ MS02-055 Unchecked Buffer in Windows Help Faci ❌ MS03-011 Flaw in Microsoft VM Could Enable Syst ❌ MS03-013 Buffer Overrun in Windows Kernel Mess (811493) ❌ MS03-023 Buffer Overrun In HTML Converter Coul ❌ MS03-024 Buffer Overrun in Windows Could Lead ❌ MS03-025 Flaw in Windows Message Handling thr Elevation (822679) ❌ MS03-034 Flaw in NetBIOS Could Lead to Informa ❌ MS03-045 Buffer Overrun in the ListBox and in the (824141) ❌ MS03-048 Cumulative Security Update for Interne ❌ MS03-049 Buffer Overrun in the Workstation Serv ✗ MS01-022 WebDAV Service Provider Can Allow Scr ✗ MS02-008 XMLHTTP Control Can Allow Access to L ✗ MS02-053 Buffer Overrun in SmartHTML Interprete ✗ MS02-064 Windows 2000 Default Permissions Cou ✗ MS02-065 Buffer Overrun in Microsoft Data Access (Q329414) ✗ MS03-008 Flaw in Windows Script Engine could al ✗ MS03-030 Unchecked Buffer in DirectX Could Enab ✗ MS03-051 Buffer Overrun in Microsoft FrontPage S (813360)
Result	Passed – This report does not identify any missing hotfixes or security updates pertaining directly to the role of the server

Audit #3 – Rename the Server Administrator Account

Reference	• XYZ Enterprises server password policy • Mastering Windows 2000 Server • http://support.microsoft.com/default.aspx?scid=kb;en-us;320053&Product=win2000
Control Objective	Elevate the difficulty it would take for a hacker to acquire the administrator username and password by renaming it to a name appearing as a general user account.

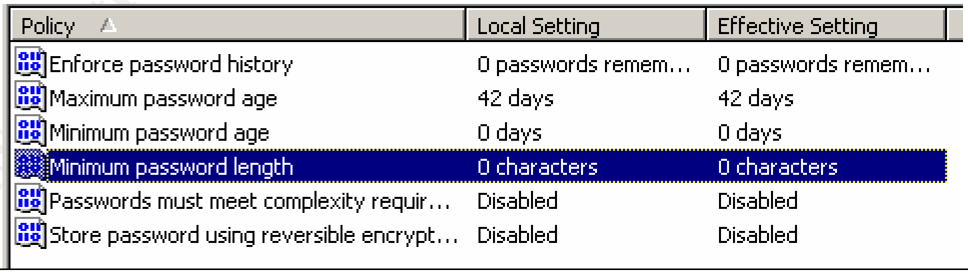
Risk	• The Windows 2000 Server Administrator account has a default name of “administrator”. Since this account can not be locked out, someone could attempt to guess the password with brute force as many times as they wish without ever getting locked out. Leaving the name set to its default settings makes it much easier to locate a user account with administrator privileges. • The probability is rated: LOW • The impact is rated: HIGH
Compliance	The administrator account is renamed from its default name
Test Steps	• Right-click on My Computer and select Manage from the list • Expand the System Tools folder • Expand the Local Users and Groups folder • Open the Users folder • Browse the list for a user named Administrator • If an account is found named “Administrator”, double click the account and select the “Member of” tab. • Look at the “Member of” tab to identify the groups that the account belongs to.
Actions	• Opened the Users folder from the “Computer Management” tool • Reviewed the list of user accounts and identified an account named “Administrator” • Opened the “Administrator” account and found that it does belong to the “Administators” group.



Member of:

Administrators

Note: In the Local Security Policy, enforcing strong passwords or requiring a minimum length are not enabled. The password on the administrator account is also set to “never expires”.



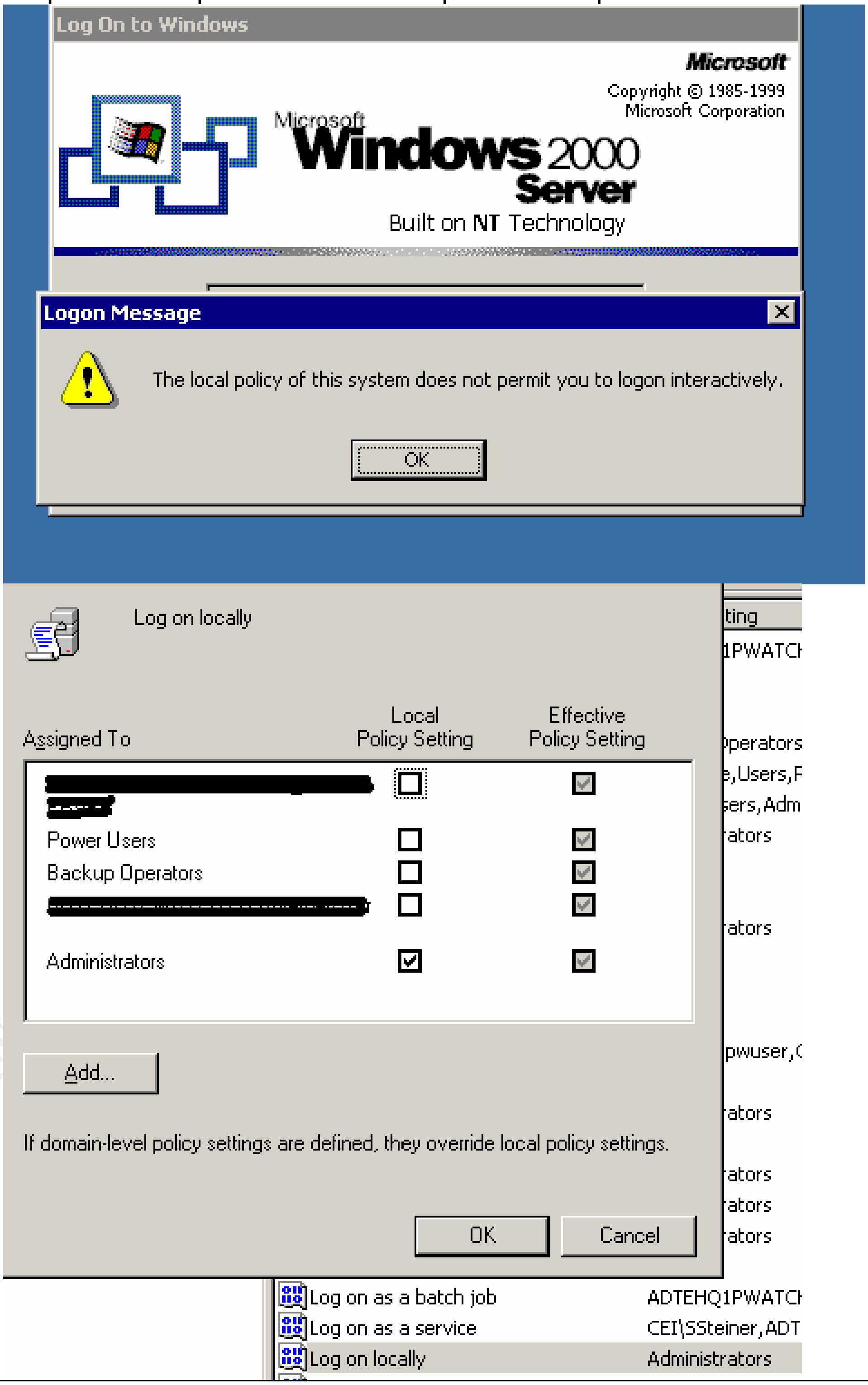
Policy	Local Setting	Effective Setting
Enforce password history	0 passwords remem...	0 passwords remem...
Maximum password age	42 days	42 days
Minimum password age	0 days	0 days
Minimum password length	0 characters	0 characters
Passwords must meet complexity requir...	Disabled	Disabled
Store password using reversible encrypt...	Disabled	Disabled

Result	Failed – The administrator account has not been renamed, leaving it more easily available to brute force or guess the password.

Audit #4 – Server User Accounts and Group Settings

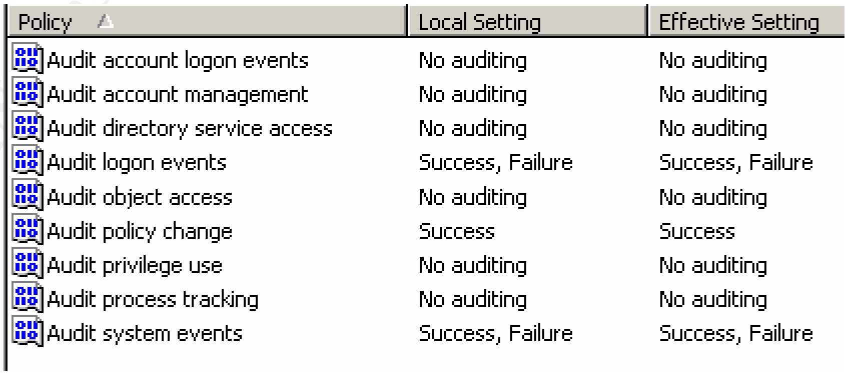
Reference	• XYZ Enterprises User Account and Password Policy • Mastering Windows 2000 Server • http://windowsecurity.com/articles/Passwords_Improve_Windows_Security_Part1.html
Control Objective	Identify non-authorized local user accounts on the server, as well as members of the administrator and users group that do not have a need to log on to the

	server
Risk	• Non-authorized local accounts or elevated privileges on the server could allow accidental or intended loss of data or system corruption. • The probability is rated: LOW • The impact is rated: HIGH
Compliance	• Local user accounts and group privileges are approved by the system administrator and all passwords meet the requirements specified in the XYZ User Account And Password Policy.
Test Steps	• Right-click on My Computer and select Manage from the list • Expand the System Tools folder • Expand the Local Users and Groups folder • Open the Users folder • Identify unauthorized local user accounts and remove those. • Open the Groups folder • Open each of the Administrators, Backup Operators, Guests, Power Users, Replicator, and Users folders and identify any accounts from the folders for which permissions have not been granted. • In the MBSA Scan results, locate the “Administrators” issues and click on “Result Details”. • Identify and validate all administrators of the computer. • Identify a user assigned to the Users group and see if they can log on at the console to access the server
Actions	• Logged on to the server with an administrator account • Right-clicked on “My Computer” and then selected “Manage” from the list. • Expanded the “System Tools” folder, then expanded the Local Users and Groups folder, then selected the “Users” folder. (Note: To protect the corporation, the screen shot of the local users will not be published) • Identified TWO local user accounts and both are verified as authorized users • Clicked on the “Groups” folder to display the Groups list. In the “Users” the only users identified was a domain group named “XYZInc\ACMEUsers” which has been verified as the authorized list of ACME application users. The application uses NT authentication to the server to allow the user to log on to the application. A separate audit of this domain group will be performed later in the checklist items (Checklist Item 18). The “Backup Operators”, “Guests”, “Power Users”, and “Replicator” groups contained no users. The Administrator Group has 5 accounts added to the Group. This list includes both administrators, the local service account for ACME, as well as the “XYZInc\Domain Admin” and “XYZInc\ACMEAdministrators” Group. A separate audit of these domain groups will be performed later in the checklist items (Checklist Item 18). • **Stimulus/Response** - Obtained the username and password of a security officer assigned to the ACME server “Users” group. Because

	the Local Security Policy is set to not allow any user to log on locally except the “Administrators” group, the action was not permitted. This provided expected results and passed this portion of the audit step.  Log On to Windows Microsoft Copyright © 1985-1999 Microsoft Corporation Microsoft Windows 2000 Server Built on NT Technology Logon Message The local policy of this system does not permit you to logon interactively. OK Log on locally Assigned To — Local Policy Setting — Effective Policy Setting [redacted] □ ☑ Power Users □ ☑ Backup Operators □ ☑ [redacted] □ ☑ Administrators ☑ ☑ Add... If domain-level policy settings are defined, they override local policy settings. OK Cancel Log on as a batch job ADTEHQ1PWATCH Log on as a service CEI\SSteiner,ADT Log on locally Administrators
Result	Failed – There were no unidentified local accounts, however, the Administrator group contains XYZ Enterprises employees with privileges that do not belong.

	The “XYZInc\Domain Administrators” Group should be removed as well as any individual accounts. All employees that need to belong to the Administrator Group should be included in the “XYZinc\ACMEAdministrators” group.

Audit #5 – System Logon and Policy Auditing

<table>
<tr><td>Reference</td><td>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserv/maintain/monitor/logevnts.asp</td></tr>
<tr><td>Control Objective</td><td>Audit account logons, logon events, account management, object access, policy changes, and system events.</td></tr>
<tr><td>Risk</td><td>• An attacker could remain unidentified as well as the inability to identify when a system policy change occurred if auditing is not enabled
• The probability is rated: High
• The impact is rated: High</td></tr>
<tr><td>Compliance</td><td>• In the Local Security Policy, Audit Policy for Audit Account Logon Events, Audit Account Management, Audit Logon Events, Audit Policy Change, Object Access, Policy Change and System Events are enabled and are set to log for both success and failure.</td></tr>
<tr><td>Test Steps</td><td>• In the Control Panel open the Administrator Tools folder.
• In the Administrator Tools folder, click on Local Security Policy
• In the Local Security Policy Window, expand the Local Policies folder
• Open the Audit Policy folder
• The Local Setting in the preview pane displays “Success, Failure” for Audit Account Logon Events, Audit Account Management, Audit Logon Events, Audit Policy Change, Object Access, Policy Change and System Events</td></tr>
<tr><td>Actions</td><td>• Opened the Local Security Policy Settings through the Control panel, expanded the Local Policies folder and selected opened the Audit Policy folder.

<table>
<tr><th>Policy</th><th>Local Setting</th><th>Effective Setting</th></tr>
<tr><td>Audit account logon events</td><td>No auditing</td><td>No auditing</td></tr>
<tr><td>Audit account management</td><td>No auditing</td><td>No auditing</td></tr>
<tr><td>Audit directory service access</td><td>No auditing</td><td>No auditing</td></tr>
<tr><td>Audit logon events</td><td>Success, Failure</td><td>Success, Failure</td></tr>
<tr><td>Audit object access</td><td>No auditing</td><td>No auditing</td></tr>
<tr><td>Audit policy change</td><td>Success</td><td>Success</td></tr>
<tr><td>Audit privilege use</td><td>No auditing</td><td>No auditing</td></tr>
<tr><td>Audit process tracking</td><td>No auditing</td><td>No auditing</td></tr>
<tr><td>Audit system events</td><td>Success, Failure</td><td>Success, Failure</td></tr>
</table>
• From the summary window, it is easy to recognize the events that have any auditing enabled. It is then determined that only the Logon and System Events Policy’s are being correctly audited.
• Logged off of the server.</td></tr>
</table>

Stimulus/Response

Action: Attempted to log on locally to the server as the vender account with the incorrect password.

Response: Received error that the password or username is invalid.

Action: Attempted to log on locally to the server as the vender account with the correct password.

Response: Received error that the Local Security Policy does not allow this account to log on to the box.

Action: Attempted to log on locally to the server as an administrator account with the incorrect password.

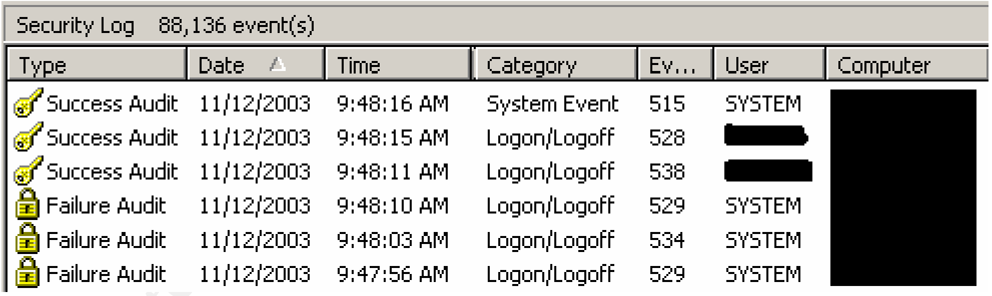
Response: Received error that the password or username is invalid.

Action: Attempted to log on locally to the server as an administrator account with the correct password.

Response: Received authentication.

Notes:

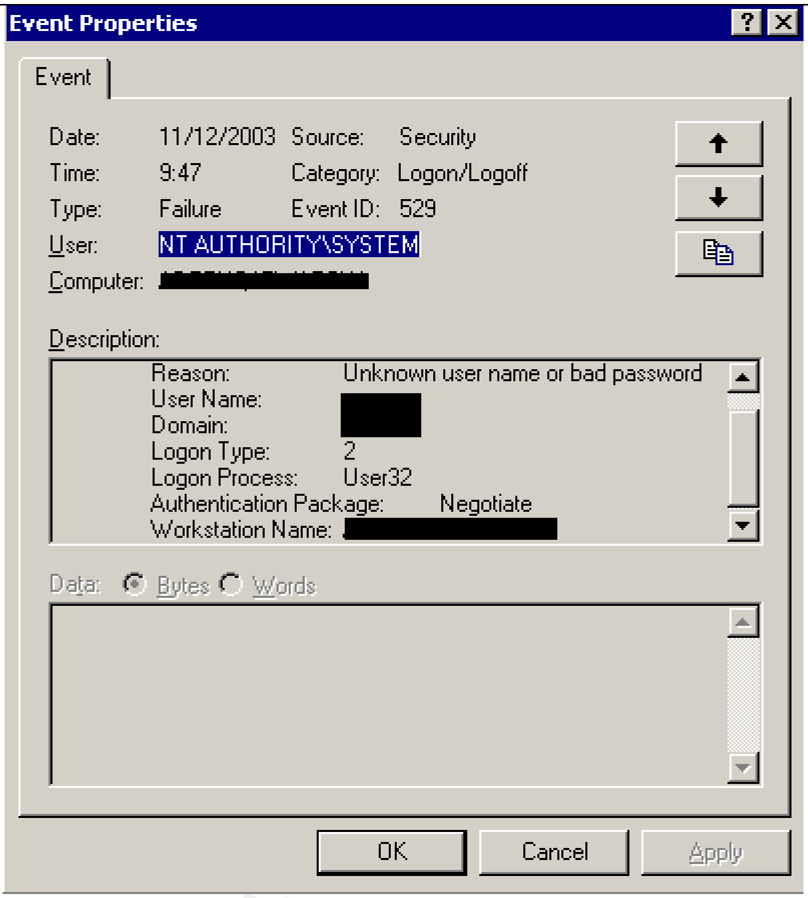
- Opened the Event Viewer through the Control Panel and Clicked on the Security Log.
- Quickly identified the process of incorrectly and correctly logging in to the server as they were they first 4 events in the log

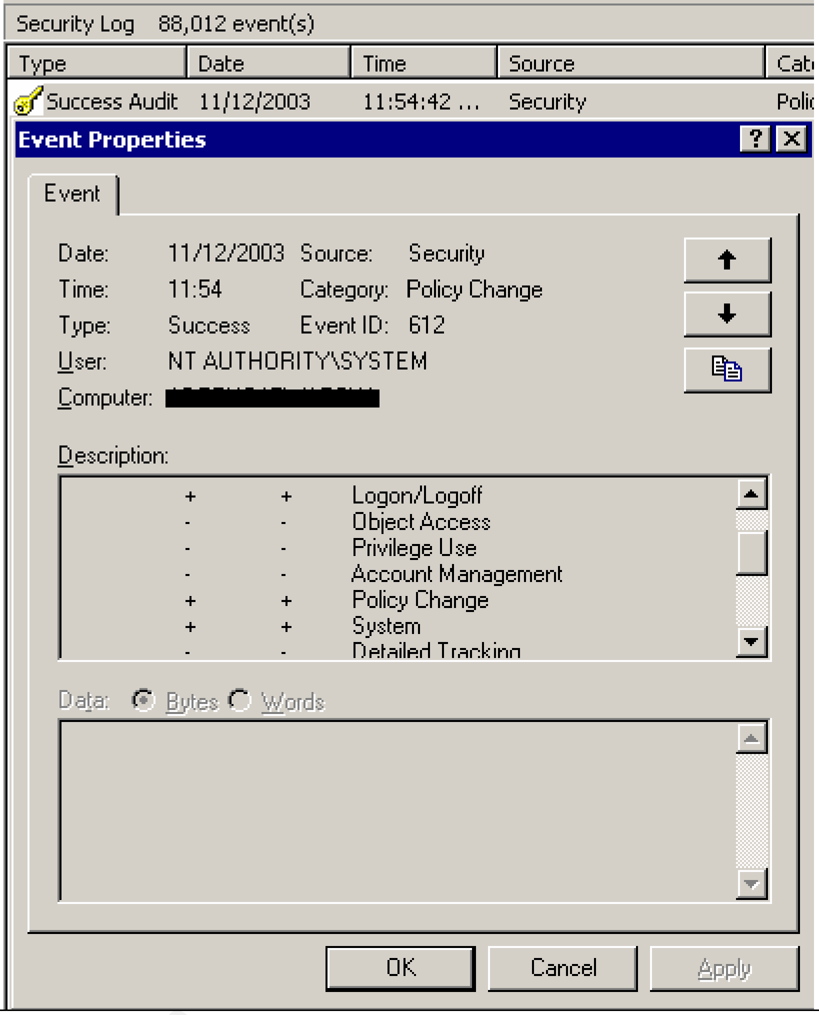


Security Log 88,136 event(s)

Type	Date	Time	Category	Ev...	User	Computer
Success Audit	11/12/2003	9:48:16 AM	System Event	515	SYSTEM	[redacted]
Success Audit	11/12/2003	9:48:15 AM	Logon/Logoff	528	[redacted]	[redacted]
Success Audit	11/12/2003	9:48:11 AM	Logon/Logoff	538	[redacted]	[redacted]
Failure Audit	11/12/2003	9:48:10 AM	Logon/Logoff	529	SYSTEM	[redacted]
Failure Audit	11/12/2003	9:48:03 AM	Logon/Logoff	534	SYSTEM	[redacted]
Failure Audit	11/12/2003	9:47:56 AM	Logon/Logoff	529	SYSTEM	[redacted]

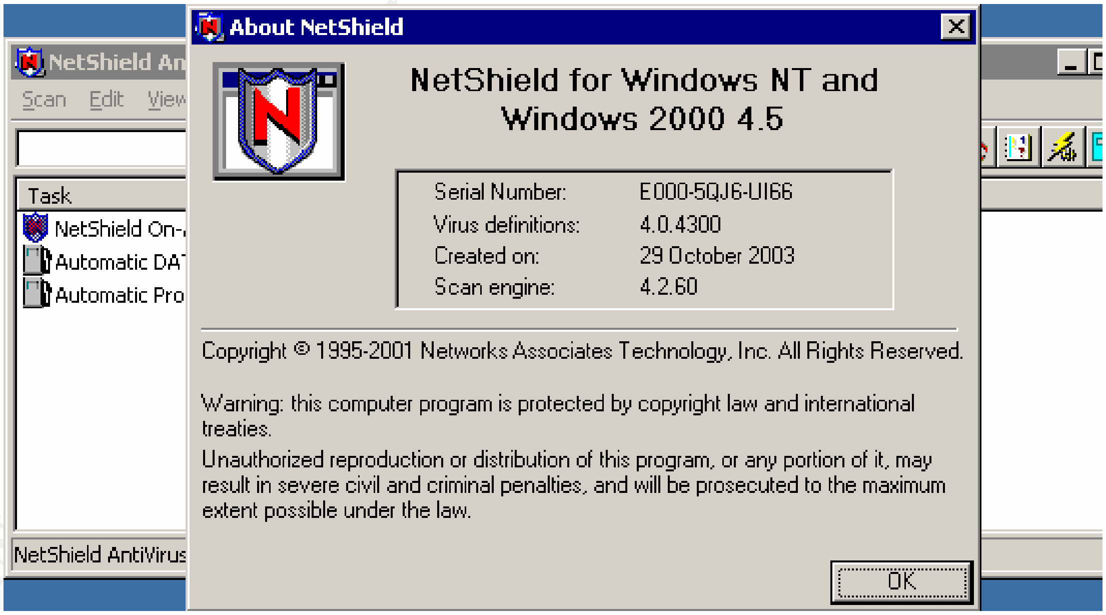
- After double clicking on each of the selected events, it is determined that the local security policy for logging in set correctly, as well as the audit policy for successful and failed logins.

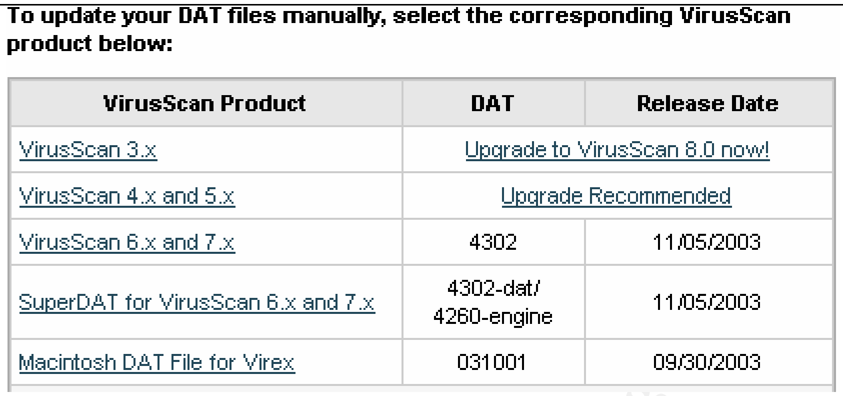
		 Event Properties Event Date: 11/12/2003 Source: Security Time: 9:47 Category: Logon/Logoff Type: Failure Event ID: 529 User: NT AUTHORITY\SYSTEM Computer: [redacted] Description: Reason: Unknown user name or bad password User Name: [redacted] Domain: Logon Type: 2 Logon Process: User32 Authentication Package: Negotiate Workstation Name: [redacted] Data: ● Bytes ○ Words OK Cancel Apply **Action:** Open the Local Security Policy Setting window and change the settings on the Audit Policy Change to include failed attempts. **Response:** After opening the Security Event Log, an event was created for the changed security policy.

	 Security Log 88,012 event(s) Type Date Time Source Cat Success Audit 11/12/2003 11:54:42 ... Security Polic Event Properties Event Date: 11/12/2003 Source: Security Time: 11:54 Category: Policy Change Type: Success Event ID: 612 User: NT AUTHORITY\SYSTEM Computer: [redacted] Description: + + Logon/Logoff - - Object Access - - Privilege Use - - Account Management + + Policy Change + + System - - Detailed Tracking Data: ● Bytes ○ Words OK Cancel Apply
Result	Failed – The local security policy of this server does not meet the established requirements in the XYZ Enterprises Server Security Policy for auditing.

Audit #6 – Server Anti-Virus Practices

Reference	• XYZ Enterprises Anti-Virus Policy • http://www.nai.com/us/index.asp
Control Objective	Ensure that the anti-virus software is installed, up to date, and set to automaticall update itself every day
Risk	• If the Anti-virus software is not installed or the signature files is not up to da a virus could infect the server making it unavailable as well as system corruption. • Probability is rated: Low • Impact is rated: High
Compliance	The server will run Network Associates Netshield 4.5 and will be configured to "AutoUpdate" on a daily basis.
Test Steps	• Click on the Start Menu, then Program Files, then Network Associates, the Netshield Console.

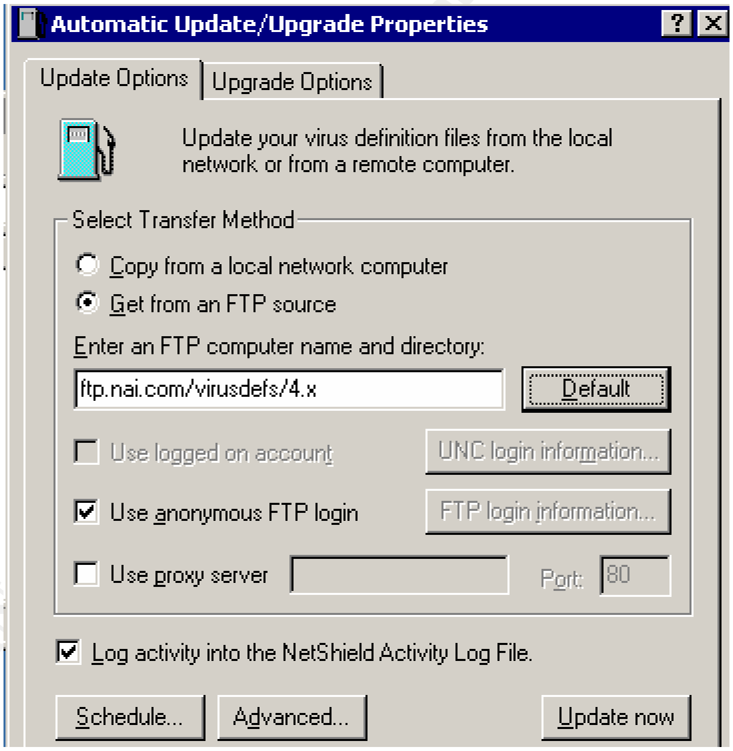
	• Click on Help, then About, this will give you the current version • Next click on Tools, then Automatic Updates from the Console Menu • The FTP Source radio button should be checked • The FTP Source should be set to ftp.nai.com/virusdefs/4.x • The Log Activity radio button should be checked • Next, click on the "Schedule" button and verify that the update is set to download daily, then close the window to return to the Console. • On the Menu Bar, click on File, then Properties • The properties window will appear an make sure the files to scan option is to "All files" • Open the Activity Log to verify that the AutoUpdate feature is properly worl and the most recent version is that found as the current version on www.nai.com
Actions	• Opened the Netshield Console from the Start Menu to start the application This verifies that Anti-virus is installed on the server. • Selected the "About" from the Help Menu option, and compard the version (Virus Definition 4.0.4300) with the most current version offered on www.mcaffee.com website.  About NetShield NetShield for Windows NT and Windows 2000 4.5 Serial Number: E000-5QJ6-UI66 Virus definitions: 4.0.4300 Created on: 29 October 2003 Scan engine: 4.2.60 Copyright © 1995-2001 Networks Associates Technology, Inc. All Rights Reserved. Warning: this computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law. NetShield An Scan Edit View Task NetShield On- Automatic DA Automatic Pro NetShield AntiVirus OK • Opened the page: http://download.mcafee.com/updates/updates.asp and located tl most recent Signiture files. The most recent update is 4302, released Nov so the Anti-Virus has failed automatically update for 7 days.



To update your DAT files manually, select the corresponding VirusScan product below:

VirusScan Product	DAT	Release Date
VirusScan 3.x	Upgrade to VirusScan 8.0 now!	
VirusScan 4.x and 5.x	Upgrade Recommended	
VirusScan 6.x and 7.x	4302	11/05/2003
SuperDAT for VirusScan 6.x and 7.x	4302-dat/ 4260-engine	11/05/2003
Macintosh DAT File for Virex	031001	09/30/2003

- Returned to the Netshield Console, and opened the properties window for Automatic DAT Update.
- The FTP Source radio button is checked
- The FTP Source should is set to ftp.nai.com/virusdefs/4.x
- The Log Activity radio button is checked



Automatic Update/Upgrade Properties

Update Options | Upgrade Options

Update your virus definition files from the local network or from a remote computer.

Select Transfer Method

○ Copy from a local network computer

● Get from an FTP source

Enter an FTP computer name and directory: ftp.nai.com/virusdefs/4.x

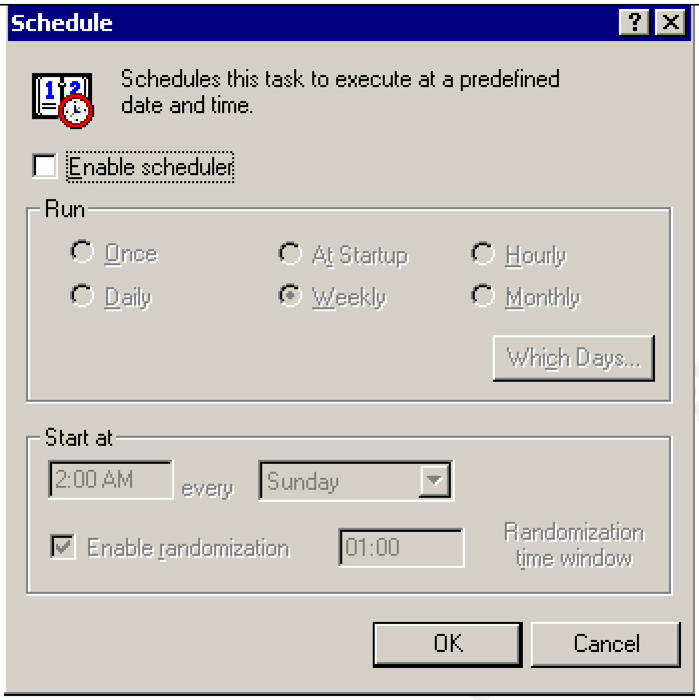
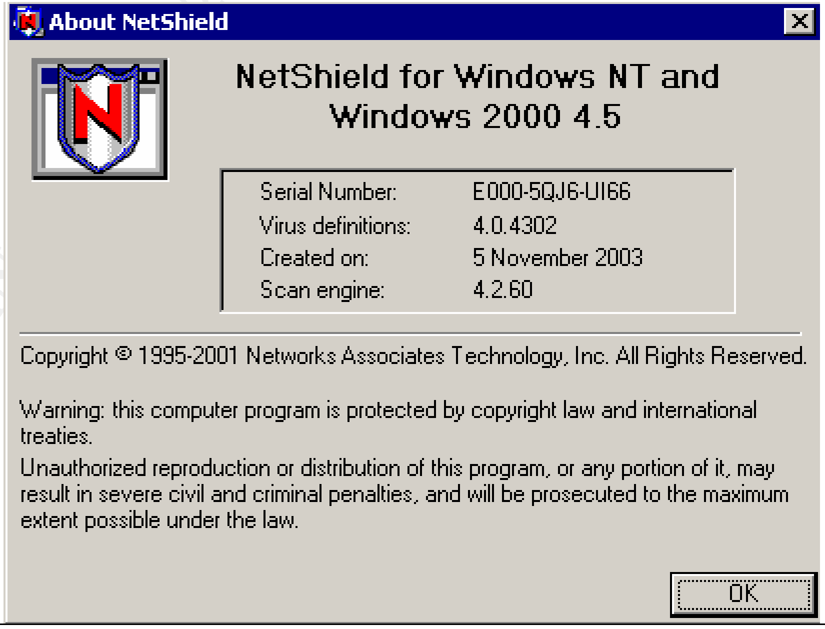
□ Use logged on account

☑ Use anonymous FTP login

□ Use proxy server Port: 80

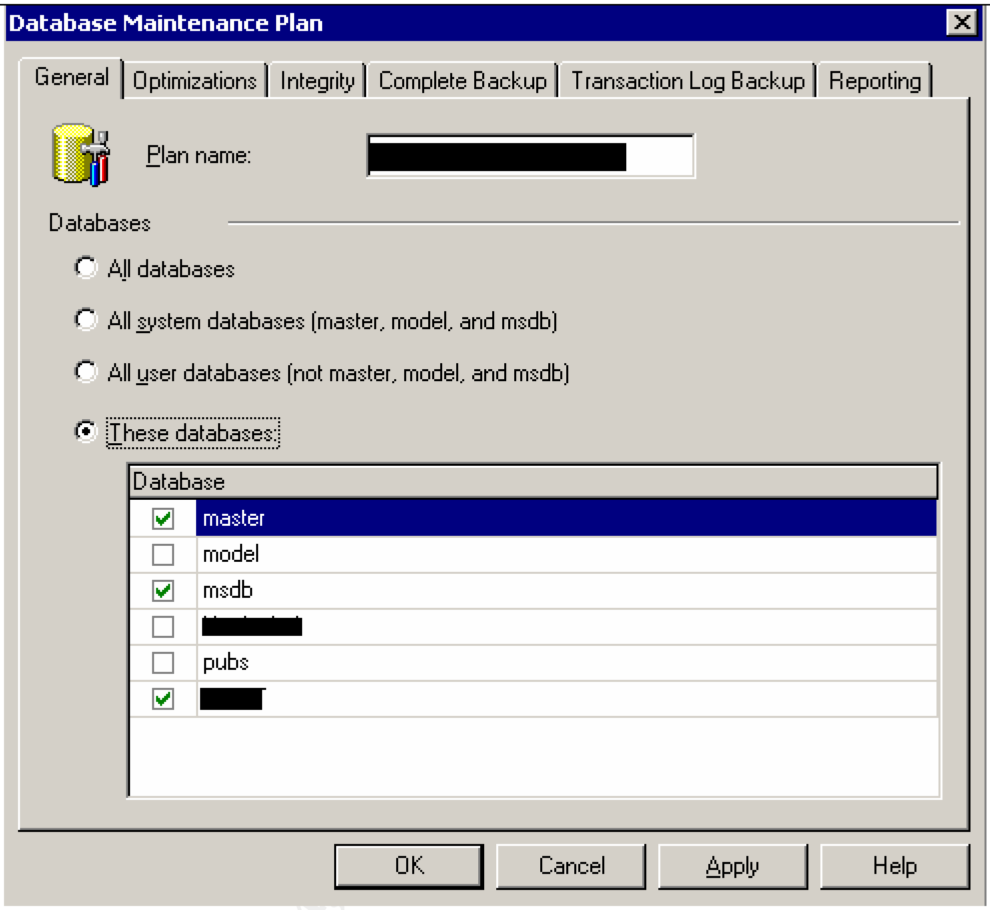
☑ Log activity into the NetShield Activity Log File.

- Clicked the "Schedule" button and discovered there is no download schedu set. This means that the anti-virus signature file is only getting updated wh an administrator logs on and the logon script associated to the script is executed.

	 **Schedule** Schedules this task to execute at a predefined date and time. □ Enable scheduler Run ○ Once ○ At Startup ○ Hourly ○ Daily ● Weekly ○ Monthly Which Days... Start at 2:00 AM every Sunday ☑ Enable randomization 01:00 Randomization time window OK Cancel **Stimulus/Response:** **Action –** Returned to the Properties and clicked the “Update Now” button. **Response –** The Update succeeded, meaning the properties are properly configured, but the schedule needs to be enabled.  **About NetShield** NetShield for Windows NT and Windows 2000 4.5 Serial Number: E000-5QJ6-UI66 Virus definitions: 4.0.4302 Created on: 5 November 2003 Scan engine: 4.2.60 Copyright © 1995-2001 Networks Associates Technology, Inc. All Rights Reserved. Warning: this computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law. OK
Result	Failed – The anti-virus software is installed and receives periodic updates when a administrator logs into the server from the logon script, but the anti-virus program needs to be automatically configured to receive automatic updates daily.

Audit #7 – Backup and Restore Process

Reference	• XYZ Enterprises Backup and Restore Policy • http://www.labmice.net/Windows2000/Backup/default.htm
Control Objective	Ensure that proper backup policies are in place to archive application data.
Risk	• The integrity of the application data becomes compromised. If a known good backup were not available, the recovery of the system would not be possible. • Probability is rated: Medium • Impact is rated: High
Compliance	Complete system backups will be performed to tape daily, and tested on a bi-weekly basis.
Test Steps	• Click on Start, then Program Files, then Microsoft SQL Server, and then Enterprise Manager. • Expand Microsoft SQL Servers, Expand SQL Server Group, Expand ACME Database Server Name, Expand Management, and select Database Maintenance Plans. • In the right pane, double click on the backup plan for the ACME application. • On the General Tab, make sure the ACME Database is selected, as well as the Master and the MSDB database files • On the Complete Backup Tab, identify the location of where the backups are being saved. • Also on the Complete Backup Tab, ensure that a backup is being performed daily. • Go to identified folder in the previous step and ensure that the backups are being created. • Backups are also made to a tape, which are then stored offsite for redundant storage and disaster recover. Open BackupExec's Activity Manager and click on the activity tab. You will see all completed and failed jobs, start and end time, and byte count. • Now that the backups are confirmed to exist, check them to see if they will restore by clicking Restore Database from the Tools Menu Bar in the Enterprise Manager. • In the Restore Database window, select your database and what version, and click ok. This will start the restore.
Actions	• Opened the Microsoft SQL Server Enterprise Manager, then located the Database Maintenance Plans from within the ACME Database. • On the General Tab, verified that the ACME Database is selected, as well as the Master and the MSDB database files.



Plan name: [redacted]

Databases

○ All databases

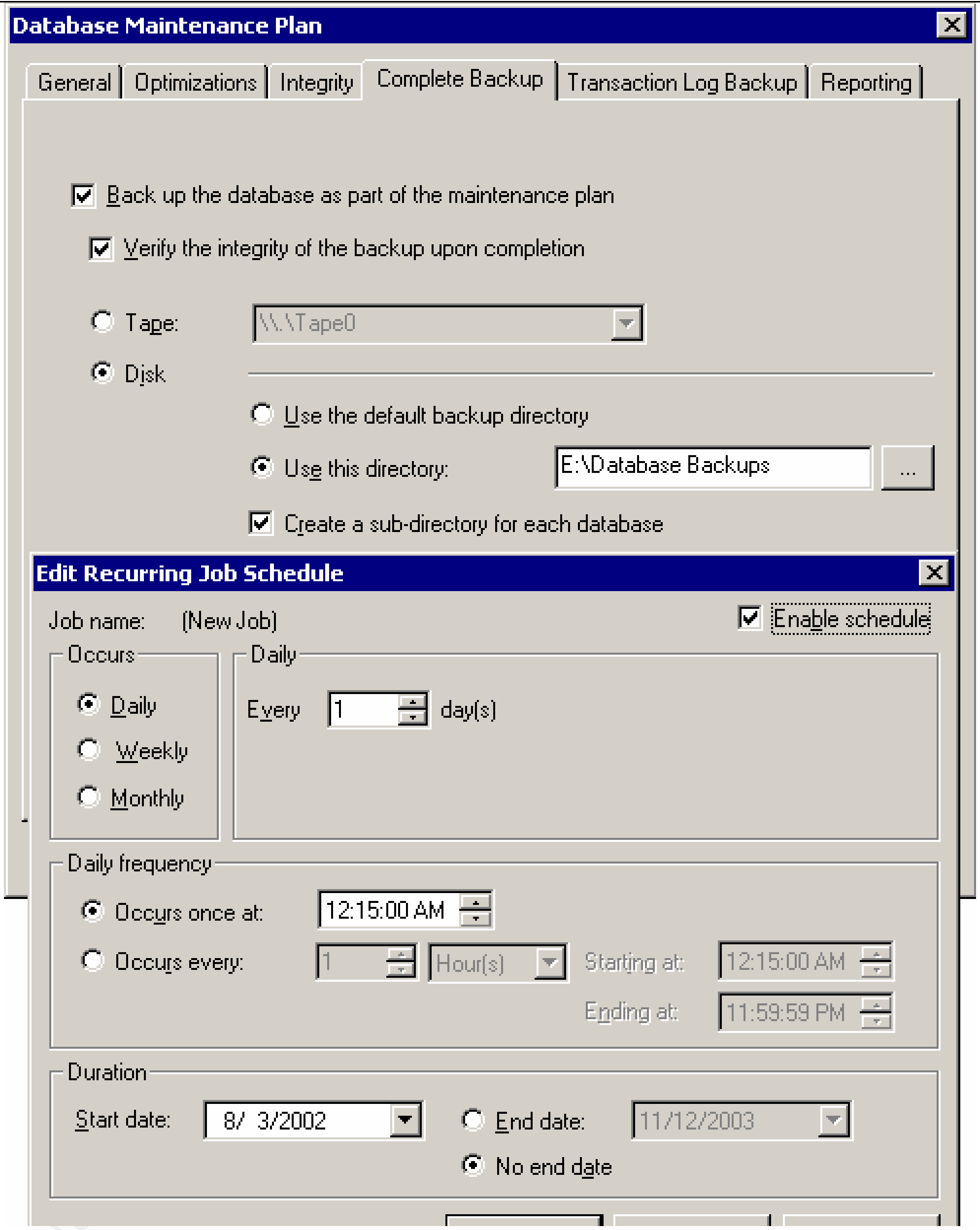
○ All system databases (master, model, and msdb)

○ All user databases (not master, model, and msdb)

● These databases:

	Database
☑	master
□	model
☑	msdb
□	[redacted]
□	pubs
☑	[redacted]

- From the Complete Backup tab, identified that the backups are being stored to disk at E:\Database Backups.
- Opened up the schedule properties and verified that the backups are scheduled daily.



Database Maintenance Plan

☑ Back up the database as part of the maintenance plan

☑ Verify the integrity of the backup upon completion

○ Tape: \\.\Tape0

● Disk

○ Use the default backup directory

● Use this directory: E:\Database Backups

☑ Create a sub-directory for each database

Edit Recurring Job Schedule

Job name: (New Job)

☑ Enable schedule

Occurs: ● Daily ○ Weekly ○ Monthly

Daily: Every 1 day(s)

Daily frequency

● Occurs once at: 12:15:00 AM

○ Occurs every: 1 Hour(s) Starting at: 12:15:00 AM Ending at: 11:59:59 PM

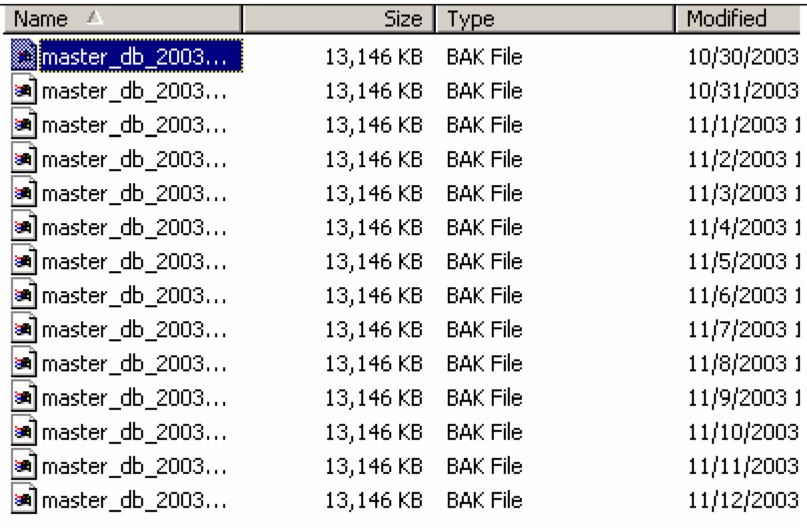
Duration

Start date: 8/ 3/2002

○ End date: 11/12/2003

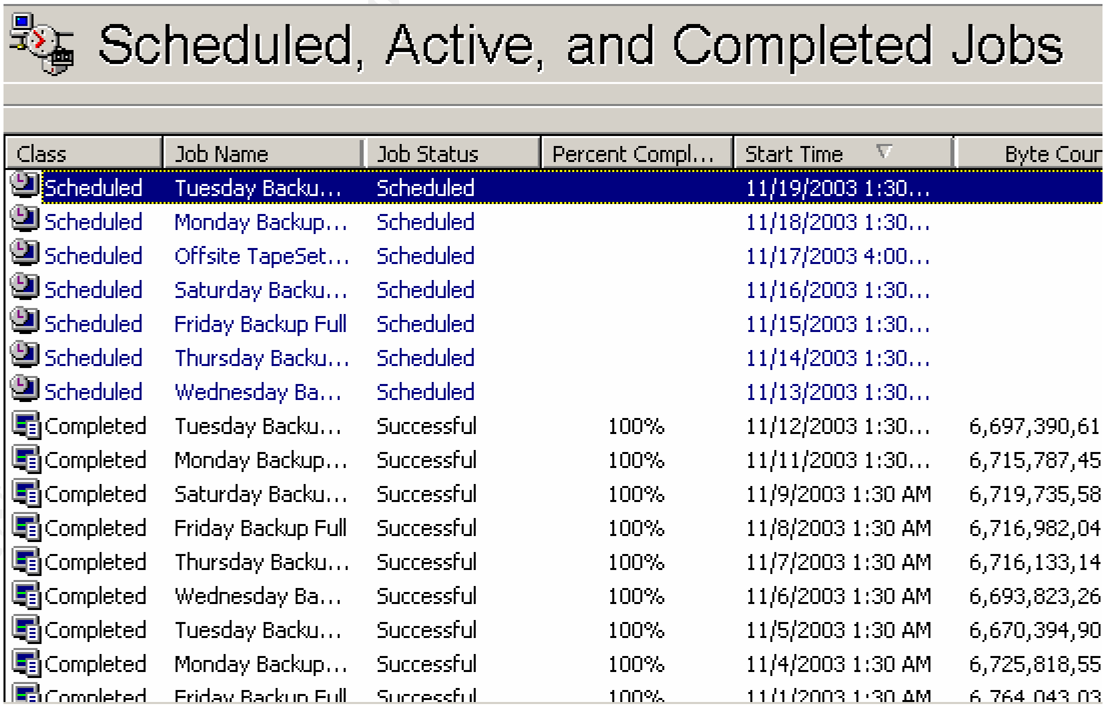
● No end date

- In Windows Explorer, browsed to the E:\Database Backups and verified that it is writing backups to this folder and is keeping files for 14 days, with today as the most current.



Name	Size	Type	Modified
master_db_2003…	13,146 KB	BAK File	10/30/2003
master_db_2003…	13,146 KB	BAK File	10/31/2003
master_db_2003…	13,146 KB	BAK File	11/1/2003 1
master_db_2003…	13,146 KB	BAK File	11/2/2003 1
master_db_2003…	13,146 KB	BAK File	11/3/2003 1
master_db_2003…	13,146 KB	BAK File	11/4/2003 1
master_db_2003…	13,146 KB	BAK File	11/5/2003 1
master_db_2003…	13,146 KB	BAK File	11/6/2003 1
master_db_2003…	13,146 KB	BAK File	11/7/2003 1
master_db_2003…	13,146 KB	BAK File	11/8/2003 1
master_db_2003…	13,146 KB	BAK File	11/9/2003 1
master_db_2003…	13,146 KB	BAK File	11/10/2003
master_db_2003…	13,146 KB	BAK File	11/11/2003
master_db_2003…	13,146 KB	BAK File	11/12/2003

- Now that the backups are being written to disk, we also verify them being written to tape in the main data center. Opened BackupExec's Activity Manager and selected the activity tab. Here, we are able to see that a daily backup plan is in place to write to tape on a daily basis.

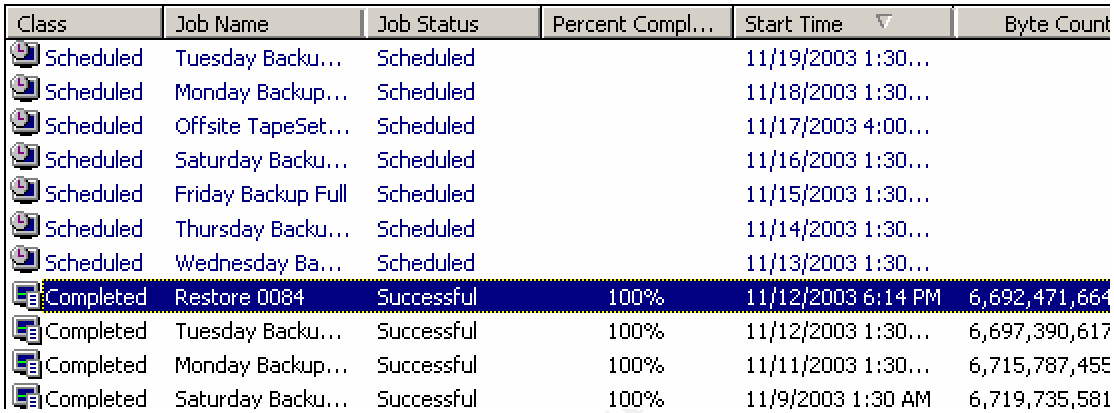


Scheduled, Active, and Completed Jobs

Class	Job Name	Job Status	Percent Compl…	Start Time	Byte Cour
Scheduled	Tuesday Backu…	Scheduled		11/19/2003 1:30…	
Scheduled	Monday Backup…	Scheduled		11/18/2003 1:30…	
Scheduled	Offsite TapeSet…	Scheduled		11/17/2003 4:00…	
Scheduled	Saturday Backu…	Scheduled		11/16/2003 1:30…	
Scheduled	Friday Backup Full	Scheduled		11/15/2003 1:30…	
Scheduled	Thursday Backu…	Scheduled		11/14/2003 1:30…	
Scheduled	Wednesday Ba…	Scheduled		11/13/2003 1:30…	
Completed	Tuesday Backu…	Successful	100%	11/12/2003 1:30…	6,697,390,61
Completed	Monday Backup…	Successful	100%	11/11/2003 1:30…	6,715,787,45
Completed	Saturday Backu…	Successful	100%	11/9/2003 1:30 AM	6,719,735,58
Completed	Friday Backup Full	Successful	100%	11/8/2003 1:30 AM	6,716,982,04
Completed	Thursday Backu…	Successful	100%	11/7/2003 1:30 AM	6,716,133,14
Completed	Wednesday Ba…	Successful	100%	11/6/2003 1:30 AM	6,693,823,26
Completed	Tuesday Backu…	Successful	100%	11/5/2003 1:30 AM	6,670,394,90
Completed	Monday Backup…	Successful	100%	11/4/2003 1:30 AM	6,725,818,55
Completed	Friday Backup Full	Successful	100%	11/1/2003 1:30 AM	6,764,043,03

<u>Stimulus/Response:</u>
Action - Now that the backups are confirmed to be successfully written to disk and tape, we will first begin a restore from tape, by clicking the Restore button on the Backup Exec tool bar. The most recent tape backup was selected to be restored to a folder named "E:\Restore\Database Backups".
Response - The restore from tape to disk was successful, indicated by the

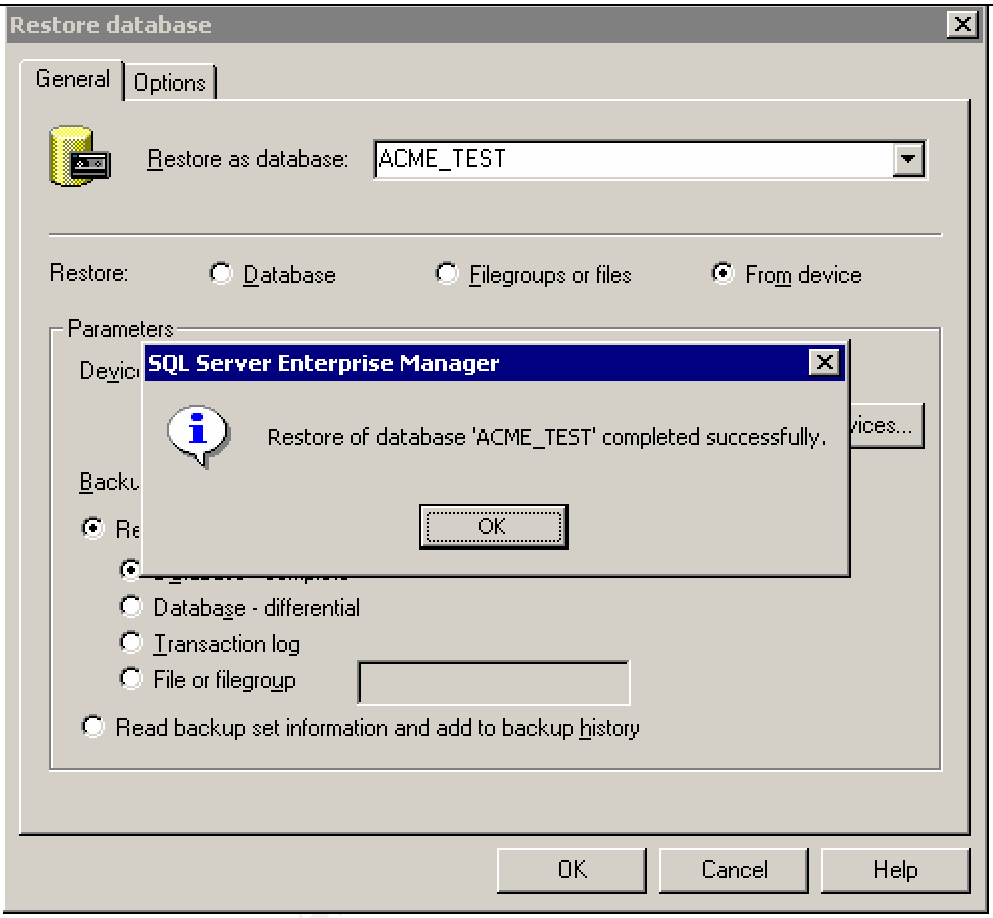
screen shot below.



Class	Job Name	Job Status	Percent Compl...	Start Time	Byte Count
Scheduled	Tuesday Backu...	Scheduled		11/19/2003 1:30...	
Scheduled	Monday Backup...	Scheduled		11/18/2003 1:30...	
Scheduled	Offsite TapeSet...	Scheduled		11/17/2003 4:00...	
Scheduled	Saturday Backu...	Scheduled		11/16/2003 1:30...	
Scheduled	Friday Backup Full	Scheduled		11/15/2003 1:30...	
Scheduled	Thursday Backu...	Scheduled		11/14/2003 1:30...	
Scheduled	Wednesday Ba...	Scheduled		11/13/2003 1:30...	
Completed	Restore 0084	Successful	100%	11/12/2003 6:14 PM	6,692,471,664
Completed	Tuesday Backu...	Successful	100%	11/12/2003 1:30...	6,697,390,617
Completed	Monday Backup...	Successful	100%	11/11/2003 1:30...	6,715,787,455
Completed	Saturday Backu...	Successful	100%	11/9/2003 1:30 AM	6,719,735,581

- Now that the database backup file has been written from the tape, we mus now ensure that it is a known good backup of the database. Re-open Enterprise Manager and Select the ACME Database, then click Tools and Restore from the menu bar.
- We are performing a test restore of all three backups (note that all restores are not being restored to the actual database, but a development server set up to test the backups.

Action – In the Enterprise Manager, the selected the database item, then selected Restore database from the toolbar. Set the name of the database to “ACME_TEST”, and set the data files to point to the “E:\Restore\Database Backups\ACME_TEST.bak” file which was created from the tape restore.
Response - The restore completed successfully



Restore as database: ACME_TEST

Restore: ○ Database ○ Filegroups or files ● From device

● Re

○ Database - differential

○ Transaction log

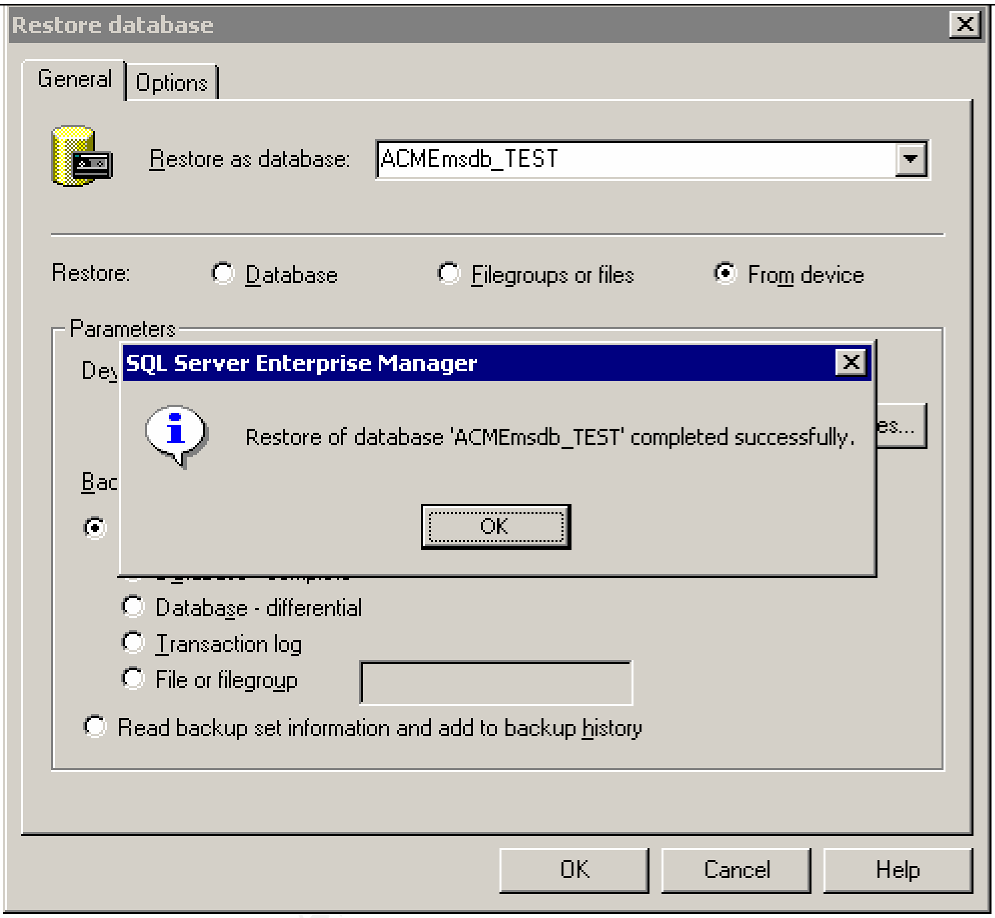
○ File or filegroup

○ Read backup set information and add to backup history

SQL Server Enterprise Manager

Restore of database 'ACME_TEST' completed successfully.

Action - In the Enterprise Manager, the selected the database item, then selecte Restore database from the toolbar. Set the name of the database to "ACMEmsdb_TEST", and set the data files to point to the "E:\Restore\Database Backups\ACMEmsdb_TEST.bak" file which was created from the tape restore.
Response – The restore completed successfully



Restore as database: ACMEmsdb_TEST

Restore: ○ Database ○ Filegroups or files ● From device

Parameters

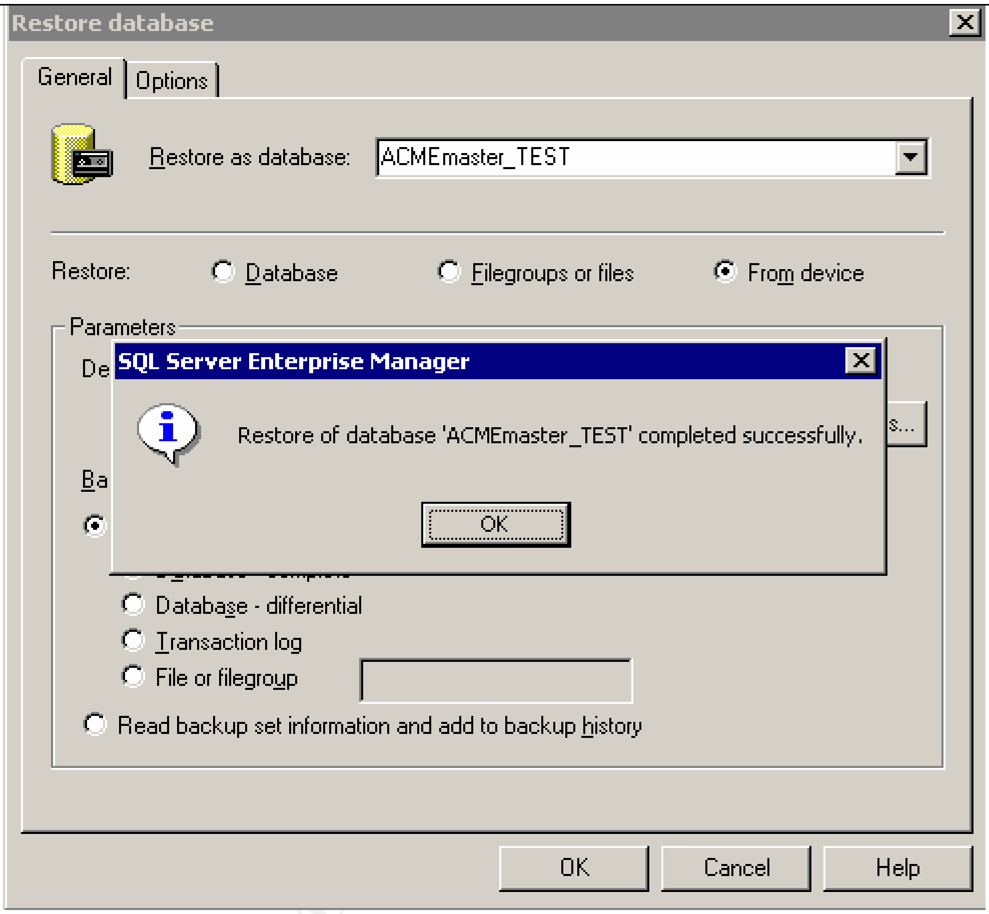
SQL Server Enterprise Manager

Restore of database 'ACMEmsdb_TEST' completed successfully.

OK

○ Database - differential
○ Transaction log
○ File or filegroup
○ Read backup set information and add to backup history

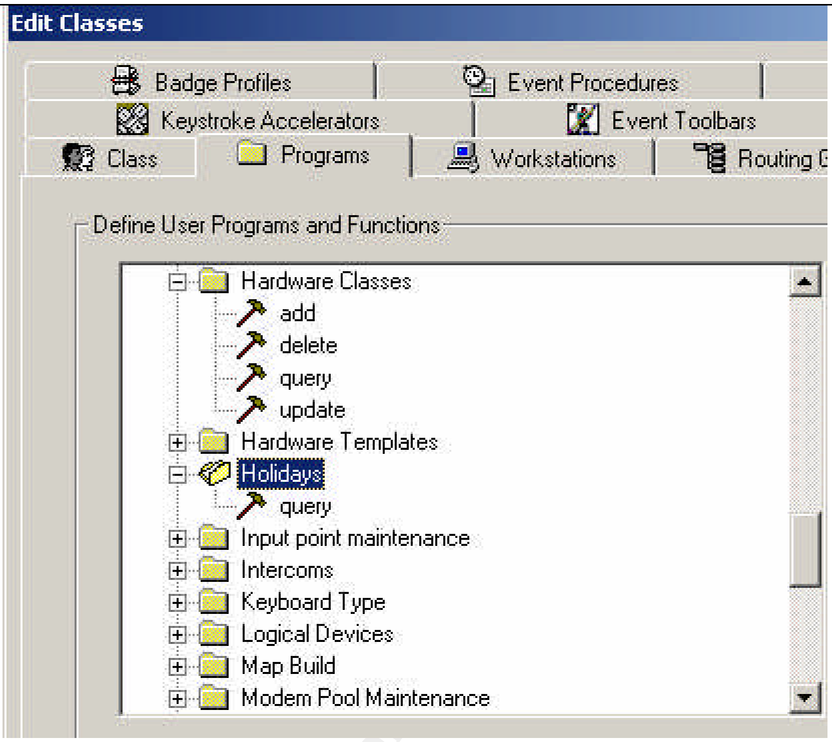
Action - In the Enterprise Manager, the selected the database item, then selecte Restore database from the toolbar. Set the name of the database to "ACMEmaster_TEST", and set the data files to point to the "E:\Restore\Database Backups\ACMEmaster_TEST.bak" file which was created from the tape restore..
Response - The restore completed successfully

	 Restore database Restore as database: ACMEmaster_TEST Restore: ○ Database ○ Filegroups or files ● From device Parameters SQL Server Enterprise Manager Restore of database 'ACMEmaster_TEST' completed successfully. ○ Database - differential ○ Transaction log ○ File or filegroup ○ Read backup set information and add to backup history General Options De Ba s... OK OK Cancel Help • Successfully restored all three backups to the development environment. Opened the application and verified the connectivity and the data, which has succeeded. The application opens and is able to browse the folders that contain data and settings, which are verified.
Result	Passed – Successful measures have been taken to archive and restore data fron the ACME server in accordance with the XYZ Enterprises Backup and Restore Policy. Data was successfully written to disk, to tape, from tape to disk to give a redundant means of archiving data. To complete the test, a successful restore of that data completed, as well as the successful connection from the application.

Audit #8 – ACME Application Privileges Check

Reference	• Personal Experience of the ACME System Administrator and Security Officer Account Manager. • ACME users manual
Control Objective	Limit each ACME user to an associated group for the amount of access required to the application as necessary
Risk	• A user may have more access in the application then necessary, resulting in application changes that are incidental or intentional. • The probability is rated: High

	- The impact is rated: High
Compliance	All administrators are assigned to an Administrators Class with full control. The venders are assigned to a Vender Class where they can add/edit/ and remove hardware, but not modify badges. The Security Operations Center Class is able to modify badges, but not modify system hardware. The Lobby Officer Class is not able to modify any item, only view badge holder information.
Test Steps	- Obtain a list of all Security Guards at the XYZ Enterprises corporate headquarters building with their assigned post from the security officers Account Manager. - Obtain a list of all Venders and administrators from the system administrator. - Open the ACME application - Click the Management Icon, then click Class. - Open, the Root Class, Vender Class, Lobby Officer Class, and the Security Operations Center Class and ensure the respective accounts are in the correct classes. - Now the “User” to “Class” is verified, click on the Programs Tab on the Edit Class Window. This will display all of the area’s that the class has access to, along with the privilege of Add, Modify, Delete, or Query. Administrators should have the ability to Add, Modify, Delete, or Query on any area. The Venders should only be able to Add, Modify, Delete or Query on the Hardware specific items (Panels, door readers. Security Operations Class should be able to only Add, Modify, Delete, or Query on Badge related areas, and the Lobby Guard Class should only have Query on Badge related areas.
Actions	- Received a list of all security officers from the Account Manager - Received the list of administrators and approved vender’s and the class they are assigned - Opened ACME client and opened the “Class” page. Here I discovered 4 classes, Root, SOC Guards, Lobby Guards, and Venders - Opened each class and verified the amount of access. In the Administrators Class, the 2 system administrators were the only users assigned and they had full system privileges. - The Vender Class had privileges to view everything, but could only add, modify, or delete items within the hardware tree.



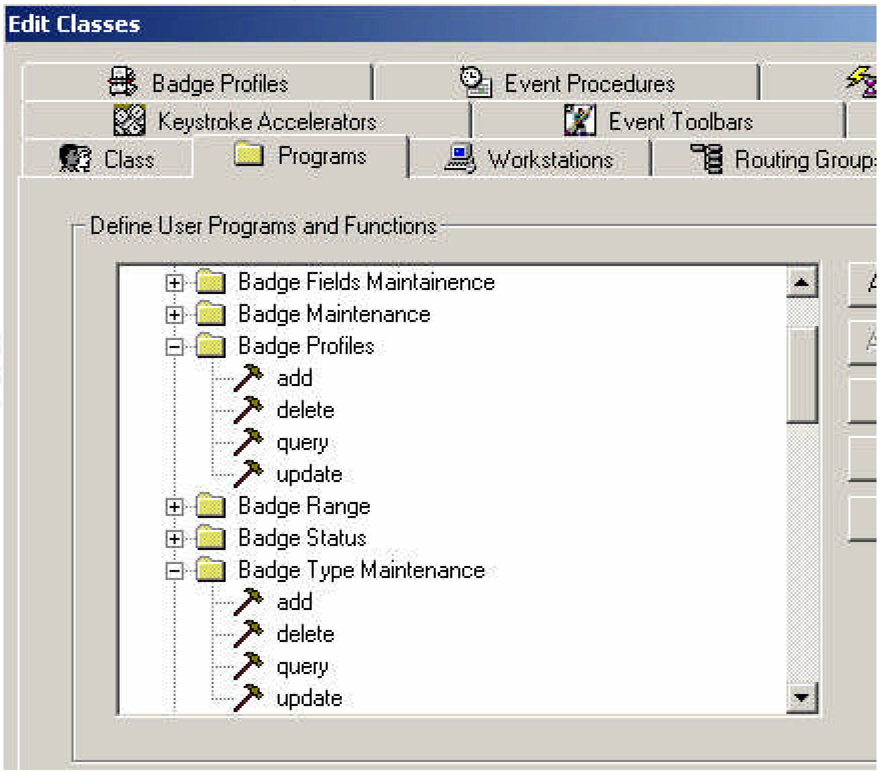
Edit Classes

Badge Profiles | Event Procedures
Keystroke Accelerators | Event Toolbars
Class | Programs | Workstations | Routing G

Define User Programs and Functions

```
⊟ Hardware Classes
    add
    delete
    query
    update
⊞ Hardware Templates
⊟ Holidays
    query
⊞ Input point maintenance
⊞ Intercoms
⊞ Keyboard Type
⊞ Logical Devices
⊞ Map Build
⊞ Modem Pool Maintenance
```

- The “SOC Guard” Class was able to view everything, but only able to add, delete, or modify a badge.



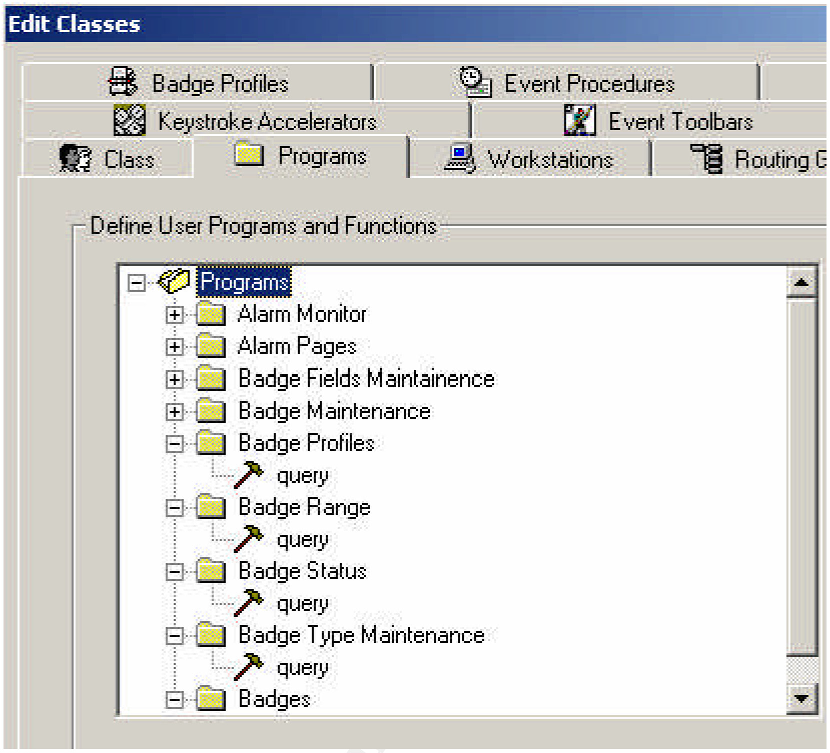
Edit Classes

Badge Profiles | Event Procedures
Keystroke Accelerators | Event Toolbars
Class | Programs | Workstations | Routing Group

Define User Programs and Functions

```
⊞ Badge Fields Maintainence
⊞ Badge Maintenance
⊟ Badge Profiles
    add
    delete
    query
    update
⊞ Badge Range
⊞ Badge Status
⊟ Badge Type Maintenance
    add
    delete
    query
    update
```

- The Lobby Guard Class was only able to view the badge information and none of the hardware items.



Edit Classes

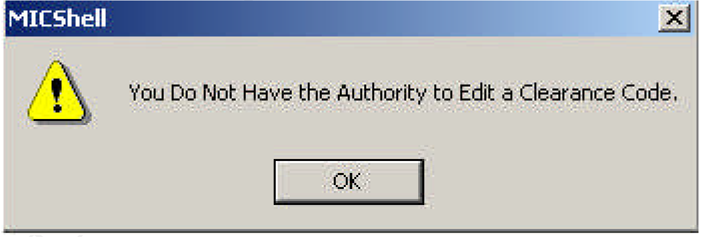
Define User Programs and Functions

- Programs
  - Alarm Monitor
  - Alarm Pages
  - Badge Fields Maintainence
  - Badge Maintenance
  - Badge Profiles
    - query
  - Badge Range
    - query
  - Badge Status
    - query
  - Badge Type Maintenance
    - query
  - Badges

Stimulus/Resonse:

Action – Logged in to a client workstation as the vender account and attempted to modify a badge clearance code.

Response - Received a denied access message.

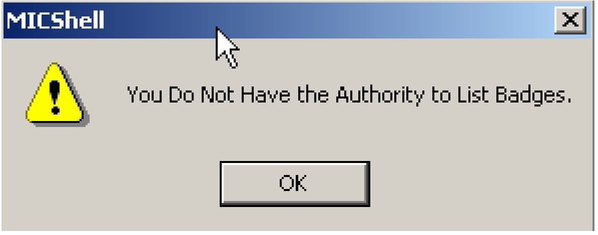


MICShell

You Do Not Have the Authority to Edit a Clearance Code.

Action – Again with the vender account, attempted to modify a badge profile

Response – Received a denied access message.

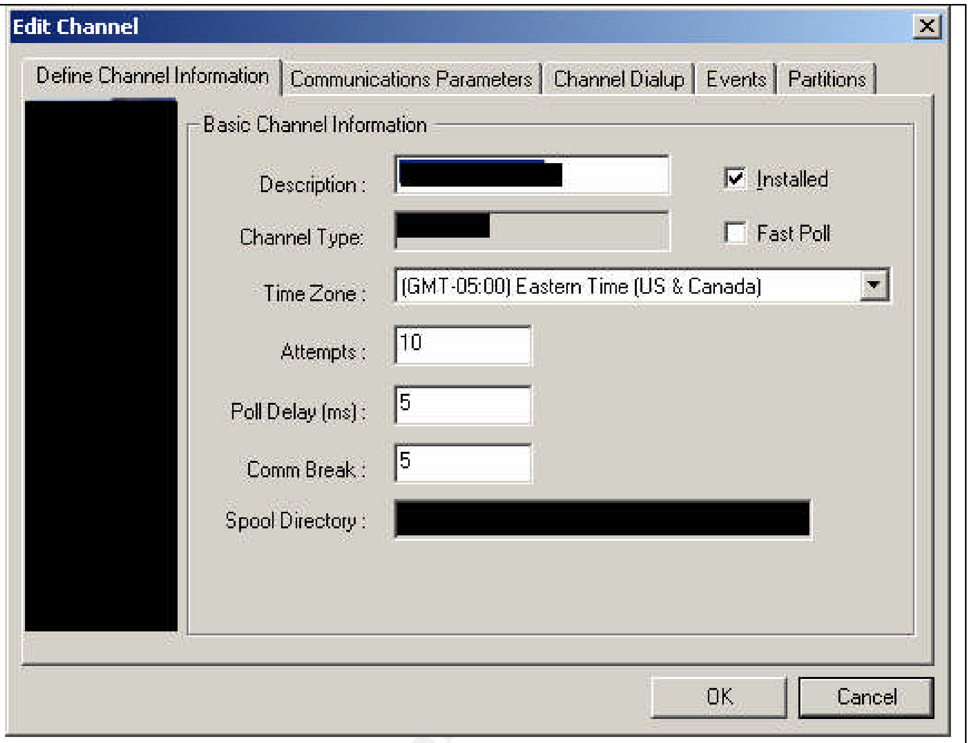


MICShell

You Do Not Have the Authority to List Badges.

Action – Logged in to a client workstation as the vender account and attempted to modify a site panel in the hardware tree.

Response - Received access



Edit Channel

[redacted]

Basic Channel Information

Description : [redacted]

☑ Installed

Channel Type: [redacted]

□ Fast Poll

Time Zone : (GMT-05:00) Eastern Time (US & Canada)

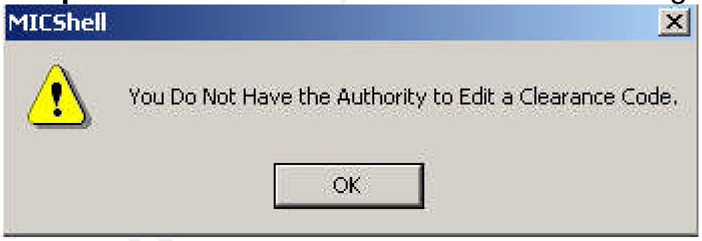
Attempts : 10

Poll Delay (ms) : 5

Comm Break : 5

Spool Directory : [redacted]

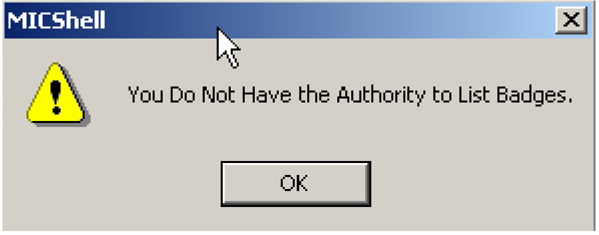
Action – Logged in to a client workstation as a lobby security officer and attempted to modify a badge clearance code.
Response - Received a denied access message.



MICShell

You Do Not Have the Authority to Edit a Clearance Code.

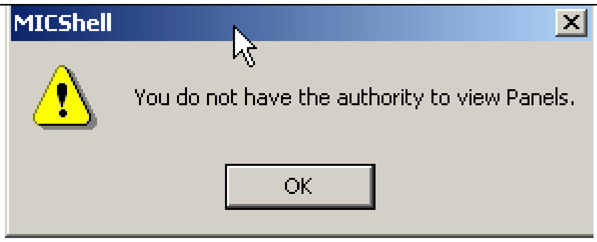
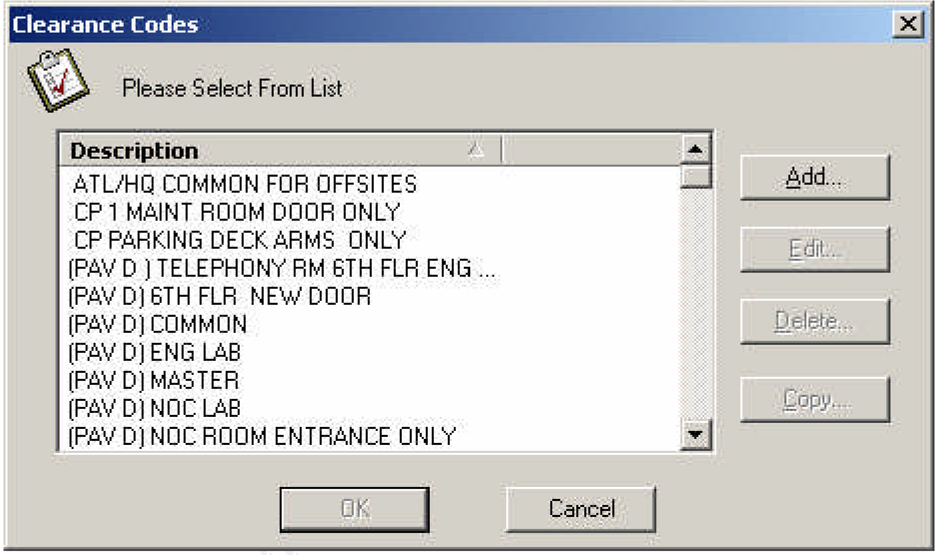
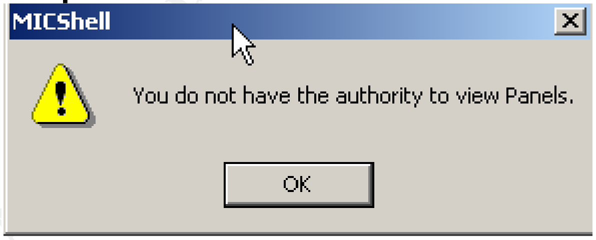
Action – Again with the lobby officer account, attempted to modify a badge profile
Response – Received a denied access message.



MICShell

You Do Not Have the Authority to List Badges.

Action – Again with the lobby officer account, attempted to modify the hardware class.
Response – Received a denied access message.

	 You do not have the authority to view Panels. **Action –** Logged in to a client workstation as the SOC officer account and attempted to modify a badge clearance code. **Response -** Received access  Clearance Codes Description Add... Edit... Delete... Copy... OK Cancel Please Select From List ATL/HQ COMMON FOR OFFSITES CP 1 MAINT ROOM DOOR ONLY CP PARKING DECK ARMS ONLY (PAV D) TELEPHONY RM 6TH FLR ENG ... (PAV D) 6TH FLR NEW DOOR (PAV D) COMMON (PAV D) ENG LAB (PAV D) MASTER (PAV D) NOC LAB (PAV D) NOC ROOM ENTRANCE ONLY **Action –** Again with the SOC officer account, attempted to modify the hardware class. **Response –** Received a denied access message.  You do not have the authority to view Panels.
Result	Passed – Every user belonged to the class for the required position. Only one vender was identified and was correctly assigned to the Vender class. Only two administrators were identified, and the lobby guards and SOC guards were placed in the correct classes. No class settings were identified that gave users elevated privileges.

Audit #9 – Process of Assigning Clearance to a Controlled Area

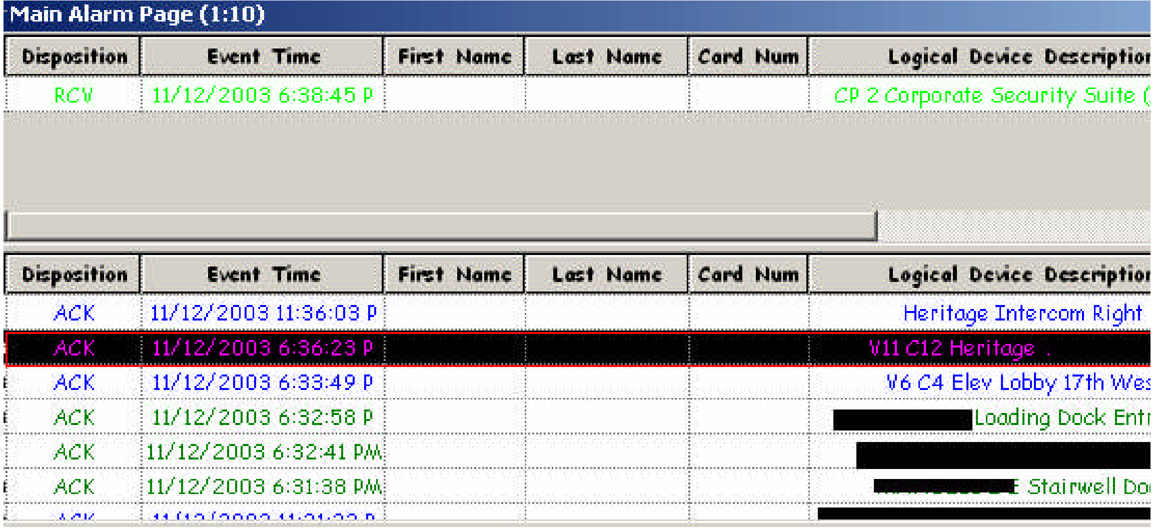
Reference	• Personal Experience of the Security Officer in the Security Operations Center and System Administrator

	• XZY Security Policy for New or Modifying Badges
Control Objective	To limit access to secured areas
Risk	• An employee may have unauthorized access to a secured area, allowing physical access to the area and an unlimited amount of risks ranging from theft to property damage. • Probability is rated: HIGH • Impact is rated: HIGH
Compliance	Employees and Contractors will only be given access to areas approved by the manager responsible for the controlled area.
Test Steps	• Open ACME, click reports, then expand the Badge Holder Reports option and select the Badgeholder Summary report. Select all users for each of the clearance codes and verify with the approving manager of each secured location that the list of employees and contractors are authorized. • Attempt to gain clearance to a secured area by locating an employee with limited "Commons Area" access and asking the officer at Security Operations Center for obtaining clearance to the data center without the necessary approval forms or escorted employee. • Continuously ask the security officer to modify the badge to access the secured area, explaining the approving manager is out of the office and the employee needs access to the area. • Open ACME, click reports, then expand the Badge Holder Reports option and select the Badgeholder Summary report. Select all users for each of the clearance codes and verify with the approving manager of each secured location that the list of employees and contractors are authorized.
Actions	• Opened the ACME reporting module and selected the Badgeholder Summary report. • Performed a report for the data center access list and reviewed it with the data center manager. Out of 53 employees and contractors, 7 were found on the list with unauthorized access • Performed a report for the Corporate Security suite access list and reviewed it with the Corporate Security manager. Out of 19 employees and contractors, there were no findings of employees or contractors with unauthorized access. • Performed a report for the financials room access list and reviewed it with the data center manager. Out of 14 employees and contractors, 2 were found on the list with unauthorized access. Both employees were inter-department transfers who no longer need access.

	- Performed a report for the Master access list and reviewed it with the Corporate Security manager. Out of 48 employees and contractors, 9 were found on the list with unauthorized access - Performed a report for the Security Room data center access list and reviewed it with the System Administrator. Out of 53 employees and contractors, 48 were found on the list with unauthorized access. - Since I am a contractor with limited "Commons Only" access, and the officers inside the SOC do not know me or what I am doing at the building, I was the subject of this test. **Stimulus/Response** **Action -** I approached the officer at the SOC and explained that I needed in to the data center for a routine check of the automated monitoring equipment and that my supervisor was supposed to be here with me to get me access but he hasn't arrived and is unreachable. **Response –** The officer asked me if I had a filled out authorization form and explained that I would need one to access the data center. **Action –** I explained I did not have one and needed access to test the monitoring equipment, and that my manager and the data center manager were both unreachable. **Response –** The officer again denied my request and told me I would have to come back or be escorted by an employee with appropriate access, and asked if there was another employee to call
Result	Passed – The procedures in place for providing access to secured areas was successful, but there is no audit process in place for reviewing the clearance currently assigned to employees and contractors.

Audit #10 – Security Officer Response and Incident Handling

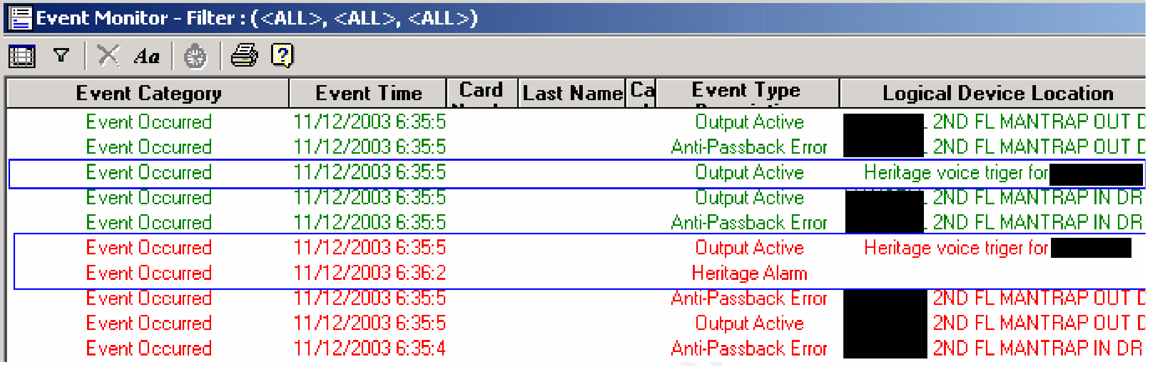
Reference	- Personal experience of a security officer. - Corporate Security's Incident Handling and Response Log Book - XYZ Enterprises Incident Handling and Response Policy
Control Objective	Ensure that all reported incidents and automated alarms are properly handled.
Risk	- An alarm goes unnoticed, or an incident is mishandled. The consequences for not responding to an incident are limitless. The consequences could be as small a door held open for a longer period then expected, to a life endangering situation. - The probability is rated: HIGH - The impact is rated: HIGH
Compliance	- Security officers will remain vigilant and alert and monitor alarms and notified incidents with the utmost priority.

Test Steps	• Review the Corporate Security Incident Handling and Response Log Book to ensure past incidents have been logged and responded to properly. • Call in a situation to the Security Operations Center to review how the call is handled, if another officer was dispatched to the location in a timely manner and that the incident was handled properly. • Activate some of the panic button alarms throughout the senior management offices to see how quickly a call to the office is made, how quickly that an investigating security officer appears, and that the incident is handled according to the XYZ Enterprises Incident Handling and Response Policy
Actions	• Reviewed the Corporate Security Incident Response and Handling Lob book. Incidents and alarms are being thoroughly documented in a log book, with dates, officers names, very detailed descriptions of the incident and minute by minute logged entries of the officers taken steps or change of status to the incident. • Notified Corporate Security and asked a manager to set off an alarm in the museum to view the security officers actions. To not tip off the security officer at the Operations Center, his actions were viewed remotely by a camera that has a remote access client. • The manager of Corporate Security set off an alarm in the museum by attempting to access a secured item. He tripped a motion beam that invisibly protects a valuable item to the company. By doing this, a visual alarm was sent to the Operations Center as well as an event logged to the Event Viewer/Log File. 

Main Alarm Page (1:10)

Disposition	Event Time	First Name	Last Name	Card Num	Logical Device Descriptio
RCV	11/12/2003 6:38:45 P				CP 2 Corporate Security Suite (

Disposition	Event Time	First Name	Last Name	Card Num	Logical Device Descriptio
ACK	11/12/2003 11:36:03 P				Heritage Intercom Right
ACK	11/12/2003 6:36:23 P				V11 C12 Heritage .
ACK	11/12/2003 6:33:49 P				V6 C4 Elev Lobby 17th Wes
ACK	11/12/2003 6:32:58 P				[redacted] Loading Dock Entr
ACK	11/12/2003 6:32:41 PM				[redacted]
ACK	11/12/2003 6:31:38 PM				[redacted] E Stairwell Do
[illegible]	[illegible]				[redacted]

<table>
<tr>
<td></td>
<td>

Event Monitor - Filter : (<ALL>, <ALL>, <ALL>)
<table>
<tr><th>Event Category</th><th>Event Time</th><th>Card</th><th>Last Name</th><th>Ca</th><th>Event Type</th><th>Logical Device Location</th></tr>
<tr><td>Event Occurred</td><td>11/12/2003 6:35:5</td><td></td><td></td><td></td><td>Output Active</td><td>[redacted] 2ND FL MANTRAP OUT D</td></tr>
<tr><td>Event Occurred</td><td>11/12/2003 6:35:5</td><td></td><td></td><td></td><td>Anti-Passback Error</td><td>[redacted] 2ND FL MANTRAP OUT D</td></tr>
<tr><td>Event Occurred</td><td>11/12/2003 6:35:5</td><td></td><td></td><td></td><td>Output Active</td><td>Heritage voice triger for [redacted]</td></tr>
<tr><td>Event Occurred</td><td>11/12/2003 6:35:5</td><td></td><td></td><td></td><td>Output Active</td><td>[redacted] 2ND FL MANTRAP IN DR</td></tr>
<tr><td>Event Occurred</td><td>11/12/2003 6:35:5</td><td></td><td></td><td></td><td>Anti-Passback Error</td><td>[redacted] 2ND FL MANTRAP IN DR</td></tr>
<tr><td>Event Occurred</td><td>11/12/2003 6:35:5</td><td></td><td></td><td></td><td>Output Active</td><td>Heritage voice triger for [redacted]</td></tr>
<tr><td>Event Occurred</td><td>11/12/2003 6:36:2</td><td></td><td></td><td></td><td>Heritage Alarm</td><td></td></tr>
<tr><td>Event Occurred</td><td>11/12/2003 6:35:5</td><td></td><td></td><td></td><td>Anti-Passback Error</td><td>[redacted] 2ND FL MANTRAP OUT D</td></tr>
<tr><td>Event Occurred</td><td>11/12/2003 6:35:5</td><td></td><td></td><td></td><td>Output Active</td><td>[redacted] 2ND FL MANTRAP OUT D</td></tr>
<tr><td>Event Occurred</td><td>11/12/2003 6:35:4</td><td></td><td></td><td></td><td>Anti-Passback Error</td><td>[redacted] 2ND FL MANTRAP IN DR</td></tr>
</table>
<ul>
<li>Immediately after tripping the alarm, the manager heard audible instructions inside the museum “You are too close to the secured area, please step back. Security has been notified”</li>
<li>Within 8 seconds of the alarm sounding at the control center, the officer responded to the alarm, and made visual confirmation as in this case, there is an observation camera that covers this area. The officer inside the Operations Center dispatched his supervisor via radio to the scene. The Operations Center officer continued to monitor the manager via video, and the Security Supervisor reached the museum in under 2 minutes.</li>
<li>Interviewed the security officer at the Operations Center and he informed me that had the manager removed items from the museum, radio contact to the front desk would have been made to stop the manager at the front lobby and not allow him to exit.</li>
</ul>
</td>
</tr>
<tr>
<td>Result</td>
<td>Passed – The procedures that the security officer at the Operations Center followed were above the expected time allowance set by Corporate Security Policy. The security officer responded to the alarms immediately and dispatched a 2nd officer to the scene as dictated by the XYZ Enterprises Incident Handling and Response Policy</td>
</tr>
</table>

Residual Risk

XYZ has implemented a very effective perimeter for access into the building with multiple layers of security identification prior to being permitted access into the building, but once you have obtained an access card and have entered the building, there are no checks or audits that are performed to ensure you have the appropriate level access. The security system is well designed and implemented, but the determination can be made from this audit that not enough emphasis has been placed on doing routine checks of the access levels, clearance code lists, authorized users, and the policies and procedures that are in place.

While not every risk can be eliminated, many of the holes discovered in the results of this audit can be filled. A checklist should be performed routinely on the access levels of active and non-active employees and contractors. These lists should be reviewed with management of the respective areas on a regular basis to prevent thefts, physical destruction of company property, or harm to an employee.

Residual Risk #1 – Reviewing the Access to Secured Areas

Control Objective	To maintain a secured enterprise with emphasis on the access control system
Residual Risk	System privilege checks as well as access list reviews being conducted to identify access cards with elevated privileges to a secured area
Recommendations	Establish a monthly review session with the managers of each secure area to identify employees or contractors who have been inadvertently granted access to a secured area, or an employee or contractor who has left the company that still has a valid card. Cards for employees should also be set to expire in 1 year. Currently there is no standard on expiration dates for employees or contractors. This risk can not be completely eliminated due to system limitations. A security officer could always assign themselves unauthorized access to a secured area. Contact with the ACME development team should be notified of this for future product enhancements.
Estimated Costs	$0 - The task of printing out the access reports and delivering them to the managers is a duty defined in the system administrators requirements, it is not being implemented. Performing this recommendation will not come as a further expense to the company.

Residual Risk #2 – Validating Authorized ACME Users

Control Objective	To maintain reliance and integrity of the ACME application.

Residual Risk	A terminated security officer could continue to log on to the domain and ACME after termination
Recommendations	Upon termination or the resignation of a security officer, the system administrators need to know prior to or immediately following the security officer leaving the company.
Estimated Costs	$0 – The terminated security officer could gain access to a computer at an off-site office that may not know they no longer work for the company. They could then gather information from the Global Address Book in Outlook, and personal information on employee's through ACME. The retrieval of archived video from the digital video recorders is also possible, possibly leading a security officer to gather the pictures and home and office information of employees of the company.

Residual Risk #3 – Reviewing the Termination or Resignation Process of Employees.

Control Objective	To remove access from an employee or contractor's access control card immediately upon termination or resignation.
Residual Risk	An employee can gain access to the building after leaving the company.
Recommendations	A notification system needs to be implemented and the managers in the company need to be briefed on the policy and held accountable for access control cards of employees that have been terminated or resigned.
Estimated Costs	$0-$2,000,000 – The cost is based on the level of physical damage that a returning employee could cause to the building or another employee.

Residual Risk #4 – Administrators on the ACME Server

Control Objective	To maintain the reliability and integrity of the ACME server, the Administrators on the server should be limited to only the system administrators.
Residual Risk	A system outage could occur if inappropriate or unauthorized change are made. If the system administrators are the only Administrators of the ACME server, the Patch management system can be better administered.
Recommendations	Remove everyone except the System Administrators and members of the Server Group identified as backups. Also, enforcing strong passwords and setting a password expiration policy should take place for administrator accounts.
Estimated Costs	$0-$1500 – If changes are made it may be necessary to bring in vender maintenance contractors to assist in the restore of the system. Labor rates for 2 contractors for 1

	day at $85/hour

Residual Risk #5 – Anti-virus and patch management

Control Objective	To reduce the exposure of vulnerabilities to the ACME server from Viruses, worms, and Trojan horses.
Residual Risk	A DoS attack, or malicious code is executed against the ACME server, causing a complete system failure.
Recommendations	Implement a corporate security policy to evaluate and analyze the released security updates and patches. Currently, each department is left on their own for deciding if updates and service packs get installed on their servers/workstations. Define a corporate policy that will eliminate this and will provide administrators with just the specific tasks of implementing the updates.
Estimated Costs	$0-$150,000 – Salary of 1-2 information security engineers.

Is the System Auditable?

The XYZ Enterprises access control system has been determined auditable by breaking it down from a system wide audit, to an combination of individual audits. Performing checks and routine procedures by the system administrators is very difficult, due to the complexity of the system, and time restraints from supporting other applications.

Many of the objectives defined in the checklist of the audit have been achieved. Policies and procedures of obtaining clearance to a secure area seem to be enforced properly, but no management or maintenance of the actual application is being performed. It is a similar situation with the maintenance of the server, it is though the large items such as backups and restores, patches and service pack updates, and managing of user accounts are taking place, but other things like the security policy and anti-virus are taken for granted and not being reviewed.

Assignment Four – The Audit Report

Executive Summary

During the past two weeks, a complete audit of XYZ Enterprise's electronic access control system has been conducted. The purpose of this audit was to identify risks and vulnerabilities associated with the server, client workstations, the ACME application, as well as the policies and procedures which govern the security officers on their day-to-day operations.

In this report, you will discover key findings which support strong policies and procedures for the security officers in responding to events, incidents, and alarms. Effective policies and practices are also in order for the issuing of the minimal required clearance to an employee or contractor. Technology findings will show the IT department has established maintenance plans to properly update the ACME server with security updates and service packs. Patch management and change management are effectively being carried out to optimize system performance and to provide documentation of system changes. A thorough backup and restore process, as well as effective disaster recovery plans are also in place.

Physical security and server updates seem to draw the most attention and concerns as those areas are well maintained. The areas of the application maintenance and changing system policies do not appear to be happening. Clearance code lists are not being reviewed, nor is there an effective termination notification policy in place. Two years ago when the access control server was implemented, it was done so with the current security policies and settings, but now that those policies have changed, the server has not been updated. The local security policy, as well as the auto-update features that perform anti-virus updates are not being reviewed or updated by the system administrators. It was discovered that an information security team does not exist at XYZ Enterprises, and that security update evaluations are the responsibility of the owners of the system. Improving in these areas would increase the overall goals and success of the access control system, which is 100% reliability.

Audit Findings

Audit Finding #1 – Access to Secured Areas

Reference: Audit steps #1, #16, and #19
Background/Risk: A policy to review badge holder's access on a periodic basis is not established. Currently, there are no checks performed on the clearance code list to make sure the correct doors are assigned to appropriate clearance code lists. An employee with elevated access privileges could cause destruction to the building or in the case of the server rooms, cause in interruption of service by physical or logical damage to the systems. This is a critical step as XYZ Enterprises relies on these systems to provide access to the revenue generating website www.HouseHoldRealty.com.
Recommendation: Doors for the data centers, financial rooms, and the security operations centers should not be included in any of the clearance codes and manually added to a badge holder's access list. These special access doors should need to be identified and have the access lists reviewed on a periodic basis with the managers responsible for the secured area. Another way to promote additional security to these areas is the installation of biometrics devices to add another layer of depth.
Cost: The integration of biometrics finger print readers could be implemented for under $3000 for the four highly secured areas of the Security Operations Center, data center, financials room, and the security server room. Reviewing the clearance codes for employees with elevated access will not serve as any added expense to the company
Compensating Controls: Create and enforce the monthly review of all access control clearance code lists.

Audit Finding #2 – Badge Deactivation

Reference: Audit step #19
Background/Risk: A policy to remove badge holder's access upon termination or resignation is not in place. Currently, the security group is only notified of terminated employees inside the building by the HR department from a monthly email. There may not be any notification of contractors and employees not located in the building as they are not administered by the internal HR department and rely on chance to be notified of a contractor or vender termination. The employee may be able to re-enter the building by telling the security officer that they lost their badge and be reissued a new one, or by using their card if it was not turned in upon loss of employment. By not immediately deactivating the badge of a person who is no longer employed with XYZ Enterprises, limitless property damage, theft, or employee confrontation is can occur.
Recommendation: Implement and enforce a policy with managers of the company that immediately upon the termination or resignation of an employee or contractor that works in their department that security is notified within 24 hours of departure from the company.
Cost: Implementing this policy will not serve as any added expense to the

company
Compensating Controls: To add other layers of security, implement an automated Visitor Management System that would enforce all visitors to sign in electronically at the front security desk. Former employees could then be added to a banned list to prevent access under different identities. A VMS could be implemented for $25,000-50,000 depending on the objective of the system. Biometric readers could also be installed throughout the building to prevent a lost or stolen card to be used without the person it is assigned to. As stated in "Audit Findings #1", a biometric system could be installed on business critical doors for approximately $3000 including the hardware and labor costs.

Audit Finding #3 – ACME Server and Application Administrators

Reference: Audit steps #3, #6, #7, #15, #17
Background/Risk: The server and application administrators are not fully implementing the XYZ Enterprises Security Policies for the server and application settings. By not following the procedures outlined in the Security Policies, the server is not configured to resist or detect an attack from a hacker. If the attack did occur, the Security Log files are not being reviewed or archived, in fact, the log file is overwritten in less then 48 hours.
Recommendation: Conduct a review of the XYZ Enterprises Security Policy for the ACME server and update the server configurations accordingly. A monthly review of the Server Security Policy or when published changes to the policy occur, the server needs to be reconfigured with the newly set policies and settings. By the system administrators participation in the weekly Change Management meetings, these changes would be identified. Due to the large volume of logon events from the application, the log files need to be increased in size and reviewed daily for anomalies, and reviewed weekly to ensure that events are being stored for an appropriate length of time.
Cost: By reviewing the policies and implementing the updated security policies, there would be no additional costs to the company. Nor would there be an additional cost to the company by requiring the attendance of the system administrators at the weekly Change Management meeting, or reviewing the log files on a daily basis.
Compensating Controls: Automated software can be purchased to notify via email of the occurrence of a specified event in the log files for less then $1000. Group Policy could be used by the Domain Administrator to make security policies, audits, and settings for all servers in the XYZ domain.

Audit Finding #4 – Anti-Virus and Patch Management

Reference: Audit steps #9, #11
Background/Risk: Currently anti-virus and system security updates are left up to the owners of the application. There is not a information security department that performs analysis of released vulnerabilities or makes suggestions and recommendations to groups or other business units of the company
Recommendation: Assign the specific task of analyzing and testing security patches and updates to the system and anti-virus to one administrator. Ask that

the system administrator include in his weekly status report the functionality of the anti-virus auto-update feature as well as any new released vulnerabilities from credible information security companies.
Cost: By performing these practices, there would be no added expense to the company
Compensating Controls: Initiate a corporate information security team to create recommendations for producing a standard among all of the business units of XYZ Enterprises. The cost of two security engineers would be a salary cost of $150,000

Bibliography

“Mastering Windows 2000 Professional” – Mark Minasi

“Mastering Windows 2000 Server” – Mark Minasi

“Securing Windows 2000 Professional Using the Gold Standard Security Template” – Ben Bower, Dean Farrington, Chris Weber

“Hacking Exposed, Windows 2000” Joel Scambray and Stuart McClure

“Incident Response, Investigating Computer Crime” Kevin Mandia and Chris Prosise

“Security, A Guide To Security System Design And Equipment Selection and Installation” Neil Cumming

“SANS Institute Track 7, Auditing Networks, Perimeters, and Systems” Training provided by Ron Ritchie

“Microsoft’s Technet” - http://www.microsoft.com/technet/

“Microsoft’s Baseline Security Analyzer”
http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=e987ab2f-3c97-4fdc-aa7b-21992ff9af7a

“Center for Internet Security’s Benchmark and Scoring Tool”
http://www.cisecurity.com/benchmarks.html

“An ACME application user guide and system documentation”
www.nexwatch.com

“Protect Yourself” by Justin Bois
http://www.sans.org/rr/papers/index.php?id=271

“Building the Ideal Web Hosting Facility: A Physical Security Prospective” - Seth Friedman http://www.sans.org/rr/papers/index.php?id=270

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

“HOW TO: Rename the Administrator and Guest Account in Windows 2000”
http://support.microsoft.com/default.aspx?scid=kb;en-us;320053&Product=win2000

"Using passwords as a defense mechanism to improve Windows security (Part 1)"
http://windowsecurity.com/articles/Passwords_Improve_Windows_Security_Part1.html

"Audit Account Logon Events" -
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/maintain/monitor/logevnts.asp

"Manage logging and other data collection mechanisms" -
http://www.cert.org/security-improvement/practices/p092.html

"Security Bulletins" http://www.microsoft.com/security/security%5Fbulletins/

"Auditing Your Disaster Recovery Plan: A Closer Look At High Tech Crime Will This Be Your Most Likely Disaster in the 21st Century?" - Jack Wiles
http://www.disaster-resource.com/cgi-bin/article_search.cgi?id='93

"Automated Backup and Restore" – Michal Simek
http://www.ntsystems.com/db_area/archive/1998/9803/203fe1.shtml

XYZ Enterprise policies:

- Anti-virus practices for Windows 2000 Server and Professional
- Local Security Policy for Windows 2000 Server and Professional
- Patch Management Policies
- Change Management Policies
- Disaster Recover and Business Continuity Practices
- Obtaining Ethernet Network Connectivity Policy
- Badge Approval Policy
- Badge Creation Policy