Assessing Risks to Novell's eDirectory 8.7.3

Ray Strubinger

GSNA Practical Assignment

Version 3.1 Option 1

September 2004

Table of Contents

Abstract

The directory service evaluated for the creation of this paper is real. The directory was in use in a production environment while the evaluation took place. Names, geographic locations, IP addresses and other identifying information have been sanitized to protect the location of the directory service, the hardware that supports it, the people who maintain it, and those found to be guilty or innocent. The facts and findings are otherwise unchanged.

This paper covers an audit conducted on Novell's Directory Service running on Netware 6.5. Sixteen audit items are presented in a checklist format and ten are developed and discussed in detail. Audit findings and recommendations are presented along with general outlines concerning remediation costs.

The author would like to express his appreciation for those who have allowed this evaluation to take place and made this study possible.

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

1.1 System Audited

The subject of this audit is one the more full-featured, mature and established directory service offerings available in the marketplace: Novell's eDirectory[1] version 8.7.3 (reported as 10550.98 by dsrepair[2]). The directory service was running on top of Novell Netware 6.5 service pack 1.1 running on an HP Proliant DL380. The IT department responsible for managing the directory has standardized their production hardware on that make and model of server. Though the hardware is not the focus of this assessment, it is noteworthy that the department has selected server class hardware complete with redundant cooling fans, power supplies, and hot-swappable SCSI disc drives configured in RAID-5.

Novell's directory service offering, eDirectory, formerly known as NDS (Novell Directory Service) is no longer limited to use on the Novell's Netware operating system. In the past several years Novell has developed the directory to run independently from the Netware OS. In addition to Netware, Novell currently offers eDirectory for Linux, Windows, and some flavors of Unix. Novell has recently transformed itself into a company focused on enabling other companies to take maximum advantage of their local networks and the Internet. Novell has been intensely involved, over this same period of time, in the area of Open Source Software and acquired Suse, a German based Linux distribution, in 2004.

The site where the audit was conducted contained several servers running a variety of operating systems including Linux, Netware, and Windows. The organization manages its own electronic mail, web, and Domain Name Service (DNS). The scope of the audit was restricted to include only the directory service installed on the organization's primary directory server, which runs Novell Netware 6.5. No other servers were examined and no desktop systems were examined. These areas may warrant examination in the future.

The organization where the assessment took place is a mid-sized biotechnology firm employing approximately three hundred people. The organization accesses information containing patient information and is therefore subject to the privacy restrictions detailed the Health Insurance Portability and Accountability Act (HIPAA) of 1996. As HIPAA deadlines approach, the organization is in the process of creating policies and procedures to ensure they are fully compliant with the regulations. The principal employees within the organization are researchers generally consisting of people with medical and statistical specialties and backgrounds. The organization has various support staff that

[1] http://www.novell.com/products/edirectory/
[2] A table mapping the version of the directory given by disrepair to the version number used by marketing and patch websites can be found at this URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10066623.htm

typically maintain "regular" eight to five hours. The staff and especially the researchers may work beyond regular hours, at night, and over weekends.

1.2 Most Significant Risks to the System

Risk establishes the likelihood of a successful attack and is the product of the threat level and vulnerability level.[3] It can be represented thus mathematically,

R = Threat x Vulnerability

A threat exists when there is a potential for a security violation that may cause harm.[4] Vulnerability exists when there is a flaw or weakness in a system or a system's process that could be exploited.[5]

The ninth annual (2004) CSI/FBI computer crime and security survey indicates that the number of attacks brought against networks and systems originate equally from the insiders and outsiders.[6] Insiders are considered particularly dangerous because they often possess (or can easily acquire) knowledge about a system they may wish to attack—knowledge that an outsider would have to work harder to obtain. There are other types of threats from insiders--unintentional acts that place systems and networks at risk. These threats are often not considered malicious acts, as they result from human ignorance or an improper configuration and were not the willful intent of causing harm. These types of threats are often found in the Information Technology staff and are often the result of a lack of staffing, time, or training. The organization under study trains its IT staff internally and externally in many areas of information technology. Junior staff members are mentored by senior staff, which supplements and enhances the junior staff's skill.

Geographic location can pose a threat to the system. The biotechnology firm studied is located in an area at risk of hurricanes, tornados, lightning, and occasional flooding. Hurricanes and tornados place the organization's systems in danger of physical destruction should the building become damaged or destroyed through direct action of wind, water, debris, or indirect action such as fire or fire suppression activities. Frequent thunderstorms combined with heavy rainfall make roof leaks, loss of cooling (air conditioning) and electrical power a concern for data integrity. The organization's data center employs two cooling systems, one primary and one secondary to maintain adequate temperature and humidity for the servers. The organization's building contains a diesel generator as well as uninterruptible power supplies (UPS) to maintain and condition power used by the servers. Flooding is a lesser concern for the organization because their data center is not located on a ground floor or basement. The organization's building consists of a flat roof, which could present the risk of a leak if the water is unable to drain from the roof quickly.

[3] http://www.sans.org/resources/glossary.php
[4] http://www.sans.org/resources/glossary.php
[5] http://www.sans.org/resources/glossary.php
[6] http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf page 8.

The organization maintains its own Internet presence and regularly exchanges electronic mail and large quantities of data with other entities via the Internet. The organization employs anti-virus software on its servers and desktops in an effort to prevent data loss, corruption, modification, or theft through malware. Electronic mail is screened at the network's border in an attempt to prevent viruses, Trojan horse programs, malware, and spam from entering the network's core and reaching the users.

1.2.1 Threats and their Capacity to Inflict Damage

Threat	Damage Capacity
Internal Users	• Data Theft/Destruction/Modification/Loss • Denial of Service/Resource Starvation • Hardware Destruction/Theft
External Users (Attackers/Crackers)	• Data Theft/Destruction/Modification/Loss • Denial of Service/Resource Starvation
Human (System Administrator) Error	• Data Loss/Modification/Destruction • Denial of Service/Resource Starvation
Geographic (Hurricanes, Tornados, Flooding, Earthquakes)	• Data Loss/Destruction • Hardware Loss/Destruction
Environmental (Fire, Steam/Pipe/Basement/Roof Leak/Flooding, Halon)	• Data Loss/Destruction • Hardware Loss/Destruction
Malware (Viruses, Trojans)	• Data Loss/Destruction/Modification • Denial of Service/Resource Starvation

1.2.2 Major Information Asset

The principal assets impacted by the directory services system is: research data, intellectual property, and electronic mail of the system users. Destruction or compromise of the directory service system could result in the loss, destruction, theft, improper access and/or modification of any information stored on a directory enabled server.

The organization's reputation could be damaged and the organization could face legal sanctions if they suffer a breach in security. The research conducted and the intellectual properties developed by the organization are vital to its long-term success. The loss, destruction, or theft of these assets could result in a loss of market share or a missed opportunity should a competitor bring a product to market first. The organization could face monetary fines as a result of data theft due to the protected status of the information and the laws designed to protect such information.

1.2.3 Major Vulnerabilities of the Audit Subject

Vulnerability Number	Vulnerability	Likelihood	Potential Impact
1	Compromise by an inside or outside operative.	Medium	• Data destruction or theft. • Public Relations issues. • Legal liability, fines.
2	Human Error/System Admin Error	Low	• Denial of service. • Potential downtime. • Temporary loss of data.
3	Geographic/Weather Related	High	• Data or hardware destroyed.
4	Environmental (building)	Low	• Data or hardware destroyed.
5	Virus/Trojan/Malware	Medium	• Data modified or stolen. • Potential downtime. • Denial of service.

1.3 Current State of Practice

Mark Lovelass, perhaps better known as Simple Nomad, of Nomad Mobile Research Centre (NMRC[7]) and one of the authors of the Pandora password "analysis" utility, has written a number of papers and tools pertaining to Netware and Novell Directory Services (NDS or eDirectory) security. The principal papers related to directory security authored by Lovelass and referenced in this paper are, "Top Ten Security Threats to Novell NDS eDirectory[8]" and "Top Ten Security Threats to Novell Netware.[9]" Lovelass' papers are among the most recent found that pertain to the security of eDirectory.

Mark Foust wrote "NetWare Security: Closing the Doors to Hackers,[10]" also referenced in this paper. Foust's paper, written in 2000, is somewhat older than the papers written

[7] http://www.nmrc.org/
[8] http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NDS_WP.pdf
[9] http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NNW_WP.pdf
[10] http://developer.novell.com/research/appnotes/2000/june/03/apv.htm

by Lovelass, but is still relevant for its treatment not only of the directory but the recommendations made to enhance its security.

SANS Reading Room contains numerous papers containing information on current as well as older versions of NDS/eDirectory and Novell's Netware Operating System.

Adam Schieman wrote a GSEC paper titled " Security Best Practice – Novell Netware 6.5 Remote Management Utilities,[11]" which describes methods that can be used to enhance the security of the software used to remotely manage Netware servers. Schieman does not state that his focus is on directory security, but many of the concepts he presents are applicable for creating a more secure directory environment.

Robert Clarke wrote a GSEC paper titled "Securing a Netware 6.5 Installation and Server Environment[12]" which also describes methods that can be used to enhance directory security. Clarke's paper is notable because he mentions vulnerabilities that are present "out of the box" from a default installation of Netware 6.5.

The entire collection of SANS Reading Room papers related to Novell Netware may be found at http://www.sans.org/rr/catindex.php?cat_id=39.

[11] http://www.sans.org/rr/papers/index.php?id=1364
[12] http://www.sans.org/rr/papers/index.php?id=1359

Part 2 – Create an Audit Checklist

Item Number/Name	1. Anonymous Browsing of e-Directory (NDS) Tree
Reference	http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NDS_WP.pdf page 4. http://developer.novell.com/research/appnotes/2000/june/03/apv.htm page 63.
Risk	Browse rights on the hidden [Public] object enable enumeration of account names by unauthenticated (anonymous) users.
Testing Procedure/ Compliance Criteria	Checks Vulnerability 1 and 2. 1. Boot a Windows workstation containing Novell's Client32 software. 2. Log in to the workstation using workstation only. 3. Run NDSrpt[13] in the following manner to enumerate user objects: • Select a tree • Select a container. • Select the Multi-Object Report tab. • Select the "User" object type on the left panel. • Select the "CN" (common name) checkbox on the right panel. • Click "Object Report." • Record results Compliance No account names (user objects) should be found. Finding account names (user objects) indicates the [Public] object contains browse rights or effective browse rights.
Test Nature (Objective/Subjective)	Objective
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

[13] Developed by Wolfgang Schreiber. Available from http://www.geocities.com/wschreib/wstools/ndsrpt.zip

Item Number/Name	2. Poor or Weak Passwords and Password Implementation
Reference	http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NDS_WP.pdf page 4. http://developer.novell.com/research/appnotes/2000/june/03/apv.htm page 53.
Risk	• Poor passwords or poor password practices expose the directory's resources to loss, theft, damage, or modification. • Accounts with no password jeopardize the security of the directory service.
Testing Procedure/ Compliance Criteria	Checks Vulnerability 1 and 2. 1. Boot a Windows workstation containing Novell's Client32 software. 2. Log in to the workstation using workstation only or log in to the directory. 3. Run DSSec[14] in the following manner to discover accounts lacking a password and accounts not required to change their passwords. • Select "Start Container Tab" • Select a tree • Select a container • Select "Check eDir Security Tab" • Select the "Users who do not have a password" checkbox • Select the "Users with no periodic password change required" checkbox • Select "Start Scan" • Record results 4. Run ConsoleOne • Right click the container where the user objects reside • Select Properties • Select Restrictions tab (Password Restrictions) • Record Settings Compliance • All accounts must have passwords. • All user passwords must be changed periodically. • All user accounts must have passwords of at least 8 characters. • All user passwords must expire.
Test Nature (Objective/Subjective)	Objective

[14] Developed by Wolfgang Schreiber. Available from http://www.geocities.com/wstools/files/dssec.zip

Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

Item Number/Name	3. Admin Account Security
Reference	http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NDS_WP.pdf page 6. http://developer.novell.com/research/appnotes/2000/june/03/apv.htm page 50.
Risk	• The admin account has rights to the entire directory service tree; therefore, it is of interest to attackers. • The admin account should have extra security due to its high level of directory service access.
Testing Procedure/ Compliance Criteria	Checks Vulnerability 1 and 2. 1. Boot a Windows workstation containing Novell's Client32 software. 2. Log in to the network with an administrative level account (a regular user account should not be able to see a custom container containing the admin accounts). 3. Run ConsoleOne[15] in the following manner to determine if the compliance criteria have been met. Locating the admin and admin equivalent accounts:[16] • In the left pane of ConsoleOne, browse to the tree. • Right click the tree and select properties. • Select the NDS Rights tab and Trustees of this Object • Select each object appearing in the list. • Select "Effective Rights" • Note if the Supervisor right is assigned under the "All Attributes Right." Determining password specifications: • Right click the admin or admin equivalent objects. • Select the Restrictions tab (Password Restrictions) • Observe "Minimum Password Length" Compliance • The admin account should be disabled and other admin level accounts must exist. • The admin level accounts must have a minimum password length requirement of 16 characters (to thwart attacks against recovered directory services files.)

[15] Once logged in to the server, the ConsoleOne program can be found on Netware 6.5 on the SYS volume under the directory structure public\mgmt\ConsoleOne\1.2\bin\ConsoleOne. The auditor could also run ConsoleOne from the local workstation if the workstation contained the program and supporting files.

[16] This series of tests assumes the administrator can be trusted, so the check is somewhat "friendly" in terms of how admin level access is determined. The administrator could have granted the auditor directory

Test Nature (Objective/Subjective)	Objective
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

Item Number/Name	4. Account Restrictions
Reference	http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NDS_WP.pdf page 6.
Risk	Unrestricted access to log in to the directory may enable a user to mount attacks against the directory from multiple locations and in parallel with the same account at any time.
Testing Procedure/ Compliance Criteria	Checks Vulnerability 1 and 2. 1. Boot a Windows workstation containing Novell's Client32 software. 2. Log in to the network with administrative level access. 3. Run ConsoleOne in the following manner • Locate the container housing the user objects • Right click the container and select "Properties" • Select the Restrictions tab (Login Restrictions) • Observe the settings • Select the Restrictions tab (Time Restrictions) • Observe the settings • Select the Restrictions tab (Address Restrictions) • Observe the settings Compliance • Limit Concurrent Connections must be enabled. Maximum Connections must be set to 1. • Time restrictions may be used if deemed appropriate. • Station Restrictions may be used if deemed appropriate.
Test Nature (Objective/Subjective)	Objective
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

access using a "special" admin account that limits what the auditor can see. Audit tests presented later are designed to detect objects that have admin level rights that are not found during this test. An un-trusted administrator may require a more forensic approach to directory and file system examination.

Item Number/Name	5. Password Attacks (Offline Remote Password Cracking)
Reference	http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NDS_WP.pdf page 5. http://developer.novell.com/research/appnotes/2000/june/03/apv.htm page 62.
Risk	• Directory services can be compromised if user passwords can be determined by attackers • Tools exist that enable attackers to recover password hashes from backup files containing copies of the directory service. (Simple Nomad's Pandora is such a tool.)
Testing Procedure/ Compliance Criteria	Checks Vulnerability 1, 2 and 5. 1. From a workstation, log in to the server and browse the sys volume. Alternate instructions: From the console, type load edit, press insert, select SYS, then select system. 2. Search for the following files: backup.ds, backup.nds, and disrepair.dib files on the server in sys:\system Compliance The backup and disrepair files should not be found.[17]
Test Nature (Objective/Subjective)	Objective
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

[17] NDS/eDirectory 8.x or better do not use these files any longer. Presence of these files could indicate a server upgrade from an older version of Netware or NDS/eDirectory. See Novell Technical Information Document http://support.novell.com/cgi-bin/search/searchtid.cgi?/10060578.htm

Item Number/Name	6. Intruder Detection
Reference	http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NDS_WP.pdf page 7. http://developer.novell.com/research/appnotes/2000/june/03/apv.htm page 50.
Risk	Directory services may be compromised if attackers are allowed to try as many username and password combinations as they desire.
Testing Procedure/ Compliance Criteria	Checks Vulnerability 1, 2 and 5. 1. Boot a Windows workstation containing Novell's Client32 software. 2. Log in to the network with administrative level access. 3. Run ConsoleOne in the following manner • Locate the container housing the user objects • Right click the container and select "Properties" • Select the General tab (Intruder Detection) • Observe the settings If Intruder Detection is enabled, confirm that it works by attempting to log in with an incorrect password until the user account is locked out. Compliance Intruder Detection must be enabled on the container or containers containing the user objects and admin user objects. If Intruder Detection is working properly the account used to test the functionality of Intruder Detection should be locked out.
Test Nature (Objective/Subjective)	Objective
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

Item Number/Name	7. Supervisor Account
Reference	http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NDS_WP.pdf page 7.
Risk	The Supervisor account provides full access to the File Server object. Full access to the File Server object could enable an attacker to compromise or damage the directory by exposing directory services files.
Testing Procedure/ Compliance Criteria	Checks Vulnerability 1 and 2. 1. Boot a Windows workstation containing Novell's Client32 software. 2. Log in to the network with administrative level access. 3. Run ConsoleOne in the following manner • Select "Edit" and "Find" • Select the proper tree and the top-most container • Check the box marked "Search Sub-containers" • Change the object type to user • Use "super*" as the name • If the account is found, follow these steps: o Right click the name "Supervisor" and select "Properties" o Select Restrictions (Login Restrictions) Compliance • The Supervisor NDS/eDirectory object must exist. • The Supervisor object must be disabled.
Test Nature (Objective/Subjective)	Objective
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

Item Number/Name	8. Hidden Objects within the Directory
Reference	http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NDS_WP.pdf page 8. http://developer.novell.com/research/appnotes/2000/june/03/apv.htm page 61.
Risk	Hidden objects are a common method employed by attackers to create a backdoor into the directory services. Backdoors enable attackers to have unauthorized access to directory services.
Testing Procedure/ Compliance Criteria	Checks Vulnerability 1 and 2. 1. Download the Hidden Object Locator from Novell's CoolSolutions website: http://www.novell.com/coolsolutions/tools/1098.html 2. Unpack the tool. 3. Log in to the directory with sufficient rights (admin level) to copy the hobjloc.nlm to sys:system. 4. From the server console type, "hobjloc.nlm" 5. Verify "[Root]" at the "Search:" line near the top of the utility. (This is the default) 6. Select "Discover Name" 7. The container name should be "[Root]" 8. Use admin as the username (this is the user the objects are hidden from) 9. Press the escape key to start the locating process Compliance The test should return a statement such as: No hidden objects exist in container [Root] for object admin.
Test Nature (Objective/Subjective)	Objective
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

Item Number/Name	9. Physical Server Security (Read/Write Replica Security)
Reference	http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NDS_WP.pdf page 8. http://developer.novell.com/research/appnotes/2000/june/03/apv.htm page 40. http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NNW_WP.pdf page 4.
Risk	Lack of physical security places the directory at risk of being physically stolen (by removing the hardware or media containing the directory) or copied by unauthorized personnel. Once stolen, the directory could be bypassed or attacked by software means.
Testing Procedure/ Compliance Criteria	Checks Vulnerability 1, 2, 4, and 5. Examine the location containing the hardware where the directory resides. • Is the equipment secured under lock and key? • Is the access method (key/card swipe, etc) securing the equipment controlled? • Is the location or equipment monitored by video camera, contact switch, security personnel, or similar means? All questions should be answered "affirmatively."
Test Nature (Objective/Subjective)	Subjective
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

Item Number/Name	10. Malware/Virus Attacks
Reference	http://developer.novell.com/research/appnotes/2000/june/03/apv.htm page 41.
Risk	Malware in the form of a virus or trojan horse software could destroy or lead to a compromise of the directory.
Testing Procedure/ Compliance Criteria	Checks Vulnerability 1, 2 and 5. At the server's console, select the Anti-Virus software's screen. Do one of the following: • Observe that the antivirus software has detected a virus and the antivirus software is up to date. (Consult the antivirus vendor's website.) Or • From a workstation logged in to the network, copy the eicar test virus to the server's file system. • Observe the server's antivirus software detect the test virus. The eicar test virus may be downloaded from this location: http://www.eicar.org/anti_virus_test_file.htm Compliance The antivirus software must be current. The antivirus software must have detected an actual virus or the eicar test virus.
Test Nature (Objective/Subjective)	Objective
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

Item Number/Name	11. Unnecessary Services
Reference	http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NNW_WP.pdf page 11. http://developer.novell.com/research/appnotes/2000/june/03/apv.htm page 57.
Risk	Unnecessary services provide an avenue leading to a security compromise if vulnerabilities are found and exploited by attackers.
Testing Procedure/ Compliance Criteria	Checks Vulnerability 1, 2 and 5. 1. Only necessary services should be running on the server. 2. From discussions with the staff, determine which services are expected to be in use on the server. 3. As the root user on a Linux machine, run the current production version of nmap[18] with the following options: nmap -v -v -sU -sS -O -o <servername>.txt <server-address> -p 1-65535 Explanation of scan options: nmap – the program name -v (twice) makes nmap be extra verbose -sU – Perform a UDP port scan -sS – Perform a TCP SYN stealth port scan -O – Fingerprint (determine) the operating system type -o – Log the results of the scan to a filename ending in txt. <server-address> - The server's IP address or DNS name. -p 1-65535 – Scan ports 1 through 65535 (all ports) Compliance • Compare the scan results to the services the staff claims should be on the server. • Only the services stated as required by the staff or required for the directory to function properly should be running on the server.
Test Nature (Objective/Subjective)	Objective
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

[18] Nmap can be obtained from: http://www.insecure.org/

Item Number/Name	12. Patch Level
Reference	http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NNW_WP.pdf page 9. http://developer.novell.com/research/appnotes/2000/june/03/apv.htm page 56.
Risk	Un-patched systems are a common means by which attackers exploit systems.
Testing Procedure/ Compliance Criteria	Checks Vulnerability 1 and 2. Verify that the server(s) are running the latest patches. From the server console 1. Load nwconfig with the command, nwconfig. 2. Select "Product Options", "View Installed Products." 3. Scroll through the list and compare to Novell's Minimum Patch List at: http://support.novell.com/produpdate/patchlist.html Compliance The server will have all the latest compatible patches installed.
Test Nature (Objective/Subjective)	Objective
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

Item Number/Name	13. Object Equivalency (Security Equal to Me)
Reference	http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NNW_WP.pdf page 9.
Risk	Attackers may employ tools that make a user object security equivalent to an admin user object. This unauthorized equivalency creates a backdoor into the directory.
Testing Procedure/ Compliance Criteria	Checks Vulnerability 1, 2 and 5. At the server console type: Set check equivalent to me Compliance Server should respond with the line: Check Equivalent to Me: ON
Test Nature (Objective/Subjective)	Objective
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

Item Number/Name	14. Known Vulnerabilities
Reference	http://www.georgetown.edu/users/reillyb/gasp/sans99/sld003.htm http://itresearch.forbes.com/detail/RES/1078243494_68.html
Risk	• Vulnerabilities in software enable could enable attackers to damage, destroy, modify, or gain unauthorized access to the directory. • Known vulnerabilities are flaws known to exist in a software package. If the vulnerability is in the public it is quite likely to be known (or discovered) by attackers.
Testing Procedure/ Compliance Criteria	Checks Vulnerability 1, 2 and 5. Invoke the Nessus[19] vulnerability scanner with options appropriate to the server housing the directory service. Nessus may be used from Linux or Windows for this test.
Test Nature (Objective/Subjective)	Objective
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

[19] Nessus is available at: http://www.nessus.org/

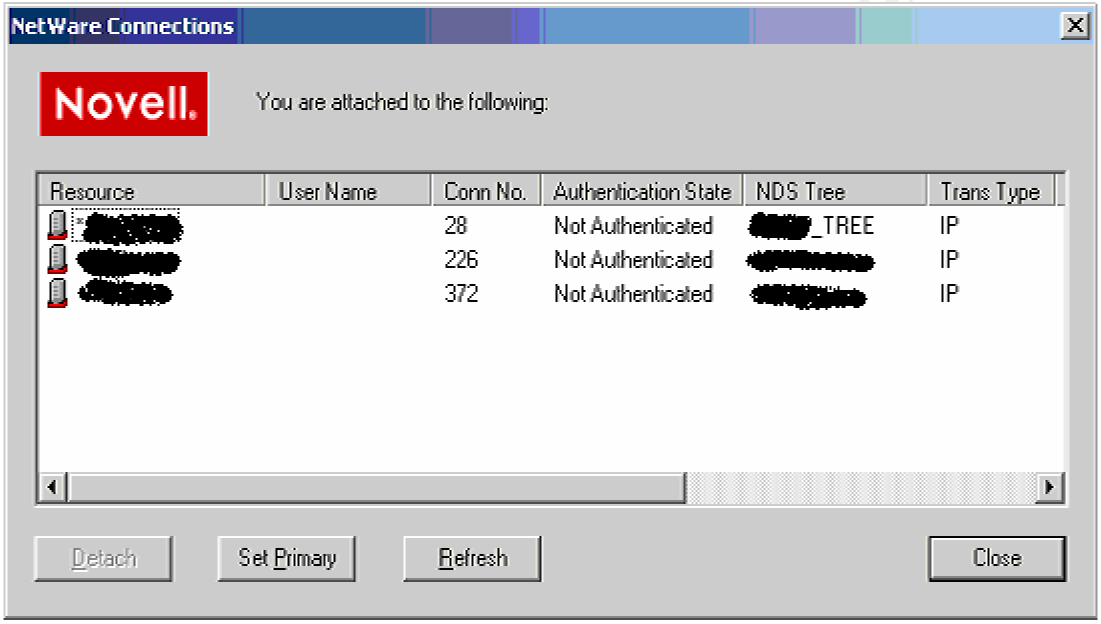
Item Number/Name	15. Environmental Control (Air and Power)
Reference	http://smallbusiness.sbc.yahoo.com/resources/refs/ buyersguides/buyersguide.php?c=Computers&id=Servers
Risk	Loss of electrical or cooling power could lead to hardware failure resulting in corruption or destruction of the directory.
Testing Procedure/ Compliance Criteria	Checks Vulnerability 2, 3 and 4. Examine the location containing the hardware where the directory resides. • Is a redundant cooling system installed and functional? • Are uninterruptible power supplies (UPS) installed, connected to the equipment and functional? Compliance Each question should be answered affirmatively.
Test Nature (Objective/Subjective)	Objective
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

Item Number/Name	16. Logging Who Logs In
Reference	http://www.condreyconsulting.com/production/PRODUCTS/AuditLogin/FAQ.htm
Risk	The 2004 FBI/CSI computer crime and security survey reveals that insiders are as big a threat as outsiders. Insiders pose the risk of compromising, damaging, stealing, modifying, or destroying the directory or the resources protected by the directory.
Testing Procedure/ Compliance Criteria	Checks Vulnerability 1, 2 and 5. 1. Log in the directory with admin level privileges. 2. Examine the log files produced by AuditLogin (if such software is in use.) 3. Alternate instructions: • Examine output from the following command: • nlist user show "last login time" /s /r nlist is the name of a utility found on Netware systems user – this option tells nlist to display user information show "last login time" – causes nlist to display the last login time. /s /r – tells nlist to search recursively from the [Root] (top) of the directory tree. Compliance User names should be observed in the log files or in the output of a utility such as nlist or AuditLogin.
Test Nature (Objective/Subjective)	Objective
Evidence	Intentionally Left Blank
Findings	Intentionally Left Blank

Part 3 – Audit Testing, Evidence, and Findings

3.1 Evidence and Findings from Audit Item 1

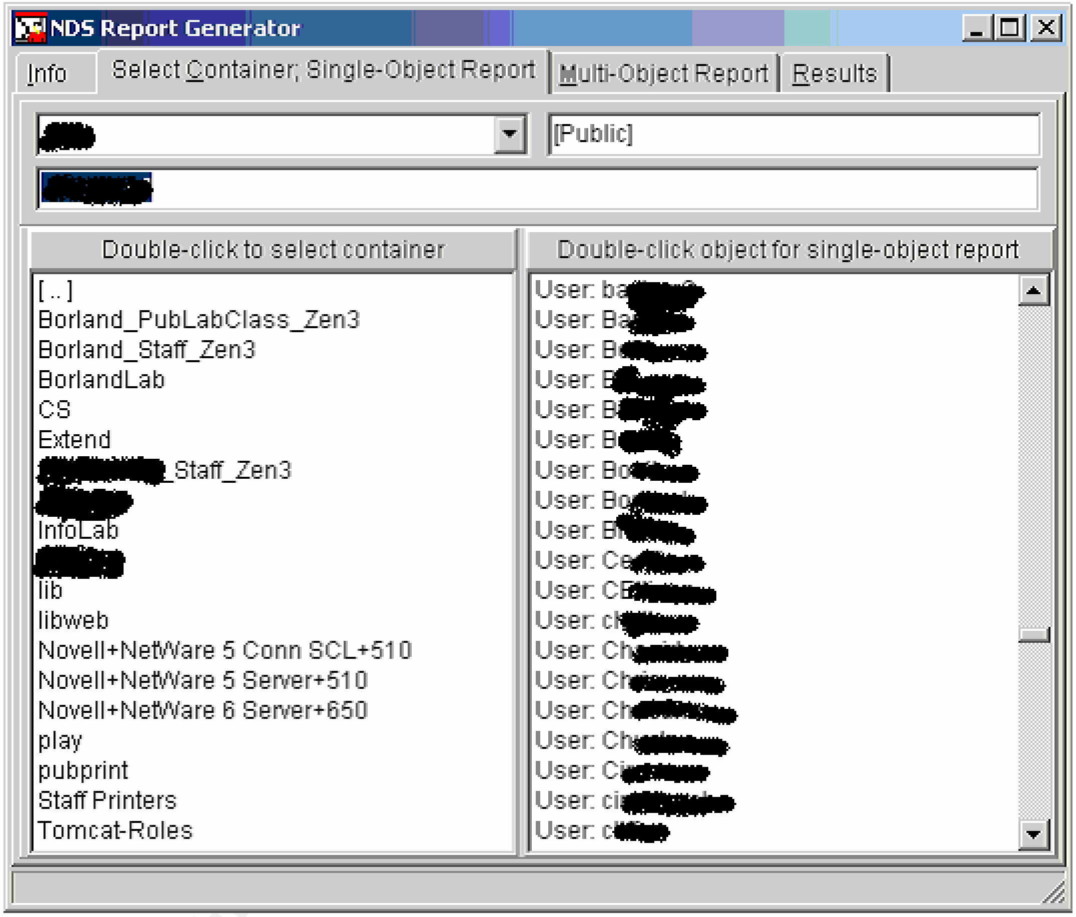
Evidence
This screenshot demonstrates that there are three non-authenticated sessions on separate servers. The server names and tree name have been masked out to preserve confidentiality.



You are attached to the following:

Resource	User Name	Conn No.	Authentication State	NDS Tree	Trans Type
[redacted]		28	Not Authenticated	[redacted]_TREE	IP
[redacted]		226	Not Authenticated	[redacted]	IP
[redacted]		372	Not Authenticated	[redacted]	IP

Wolfgang Schreiber's utility, NDS Report, has found usernames, which are shown in the screenshot below. The tree, context and identifying geographic information have been masked out. Usernames have been partially masked to avoid divulging that information and increasing the risk to the server should its location be determined.



[redacted]

[Public]

[redacted]

Double-click to select container

[..]
Borland_PubLabClass_Zen3
Borland_Staff_Zen3
BorlandLab
CS
Extend
[redacted]Staff_Zen3
[redacted]
InfoLab
[redacted]
lib
libweb
Novell+NetWare 5 Conn SCL+510
Novell+NetWare 5 Server+510
Novell+NetWare 6 Server+650
play
pubprint
Staff Printers
Tomcat-Roles

Double-click object for single-object report

User: ba[redacted]
User: Ba[redacted]
User: B[redacted]
User: B[redacted]
User: B[redacted]
User: B[redacted]
User: Bo[redacted]
User: Bo[redacted]
User: B[redacted]
User: Ce[redacted]
User: CE[redacted]
User: c[redacted]
User: Ch[redacted]
User: Ch[redacted]
User: Ch[redacted]
User: Ch[redacted]
User: Ci[redacted]
User: ci[redacted]
User: c[redacted]

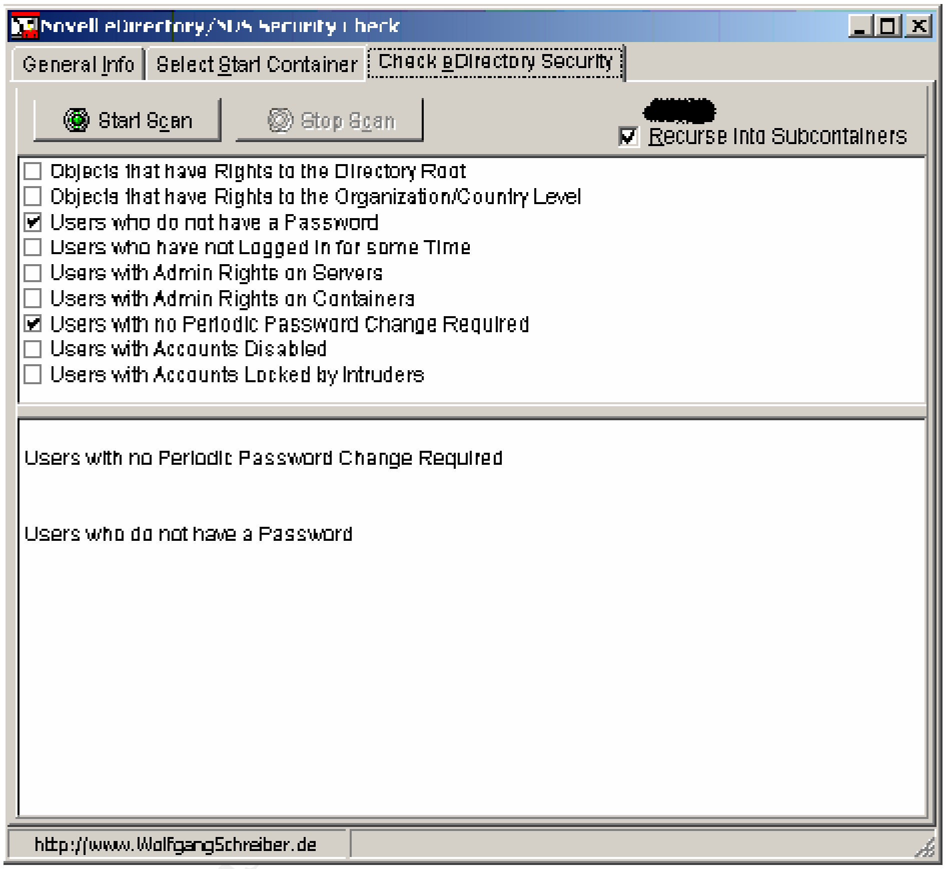
Findings
Clearly the [Public] object has explicit Browse rights or effective Browse rights which enable an unauthenticated user to enumerate usernames. Usernames are represent fifty percent of the necessary information to compromise a system (passwords are the only remaining item.)

Conclusion
Usernames were found through an anonymous browse session therefore audit item 1 is rated: FAIL.

3.2 Evidence and Findings from Audit Item 2

Evidence

This screenshot from Wolfgang Schreiber's utility, DSSec, shows that all users have passwords and are required to change their password periodically.


Novell eDirectory/NDS Security Check
General Info
Select Start Container
Check eDirectory Security
Start Scan
Stop Scan

[redacted]

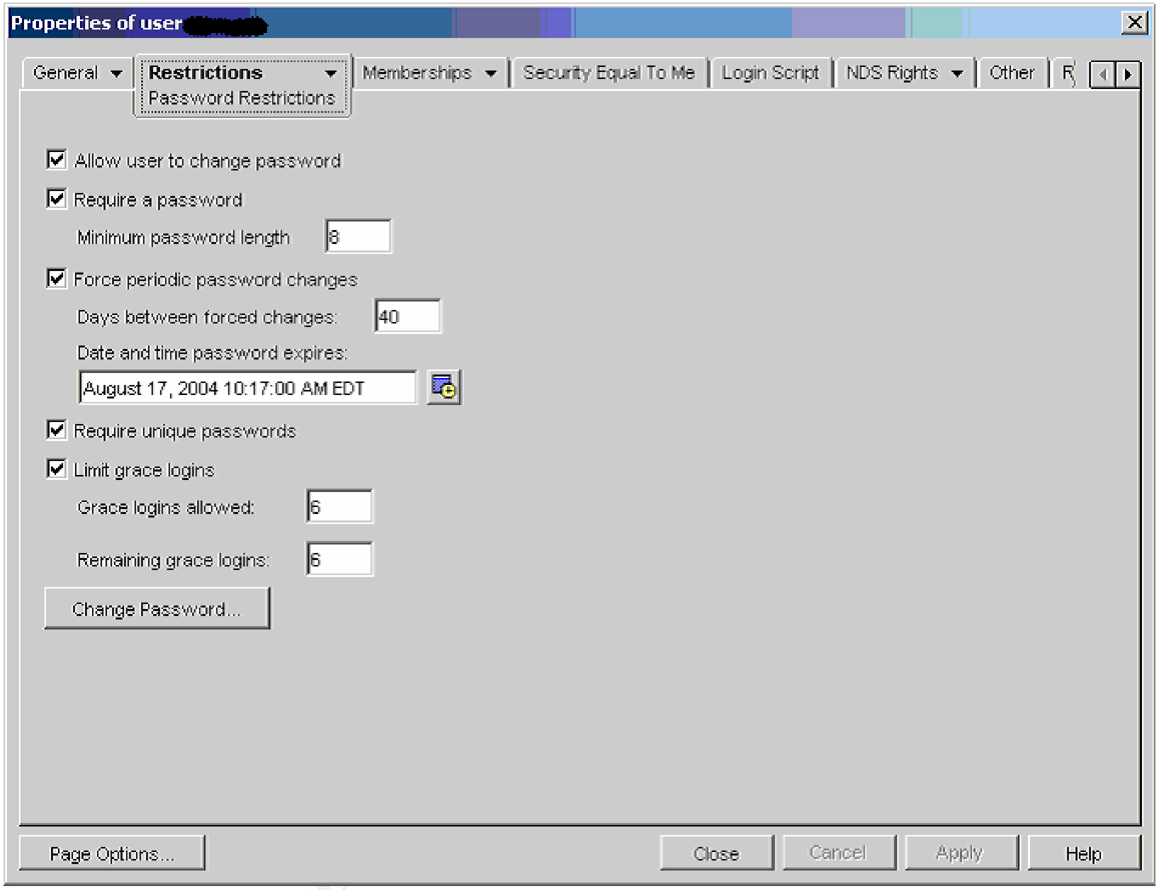
☑ Recurse Into Subcontainers

□ Objects that have Rights to the Directory Root
□ Objects that have Rights to the Organization/Country Level
☑ Users who do not have a Password
□ Users who have not Logged In for some Time
□ Users with Admin Rights on Servers
□ Users with Admin Rights on Containers
☑ Users with no Periodic Password Change Required
□ Users with Accounts Disabled
□ Users with Accounts Locked by Intruders

```
Users with no Periodic Password Change Required


Users who do not have a Password
```

This screen shot of the container where the user objects reside shows the password restrictions placed on the users.



Properties of user [redacted]

☑ Allow user to change password

☑ Require a password

Minimum password length: 8

☑ Force periodic password changes

Days between forced changes: 40

Date and time password expires: August 17, 2004 10:17:00 AM EDT

☑ Require unique passwords

☑ Limit grace logins

Grace logins allowed: 6

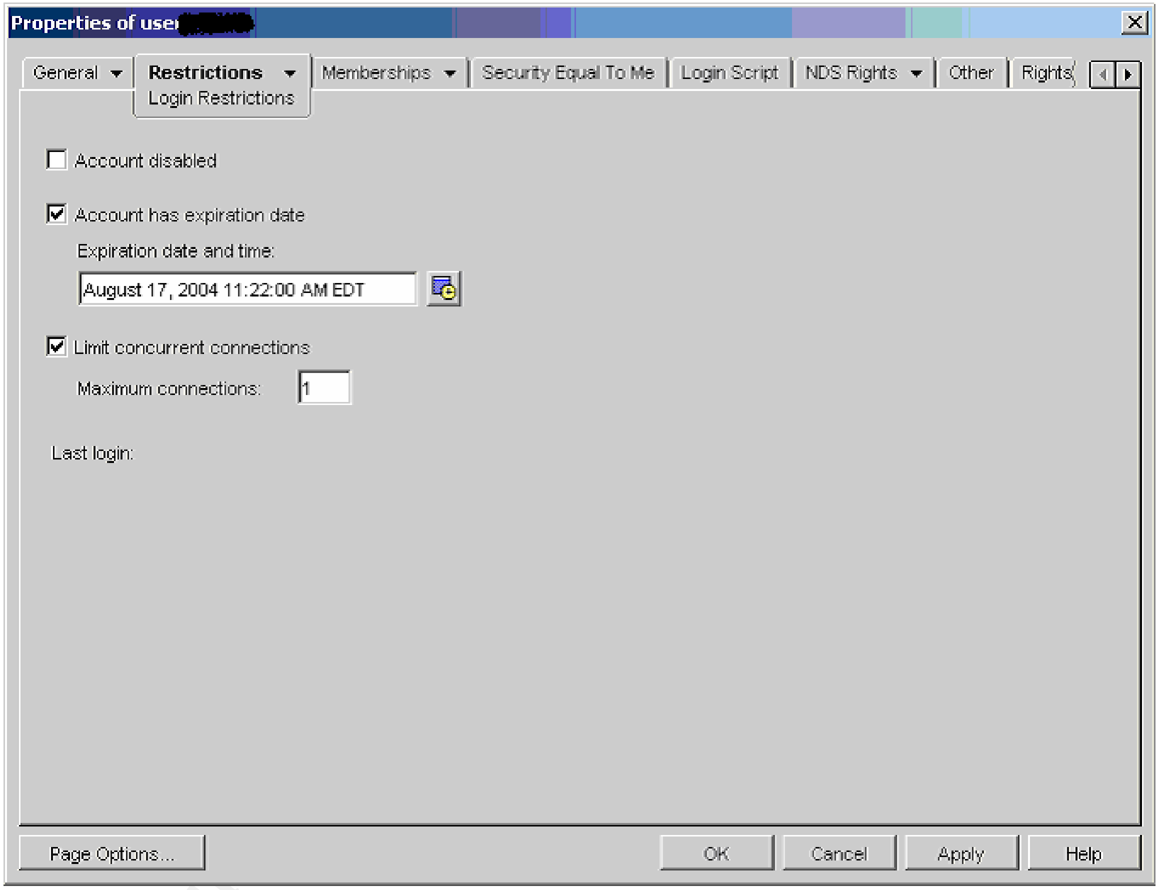
Remaining grace logins: 6

Findings
All accounts were found to have passwords. All user accounts were found to require periodic password changes. All user accounts were found to have a password of at least eight characters. All passwords were found to expire.

Conclusion
Based on the findings, audit item 2 is rated as: PASS.

3.3 Evidence and Findings from Audit Item 4

Evidence
Screen shots from the user settings obtained with ConsoleOne looking at the Login Restrictions tab show that the "Maximum concurrent connections" option has been enabled and set to one. The name of the container where the user objects reside has been masked.



Properties of user[redacted]

☐ Account disabled

☑ Account has expiration date

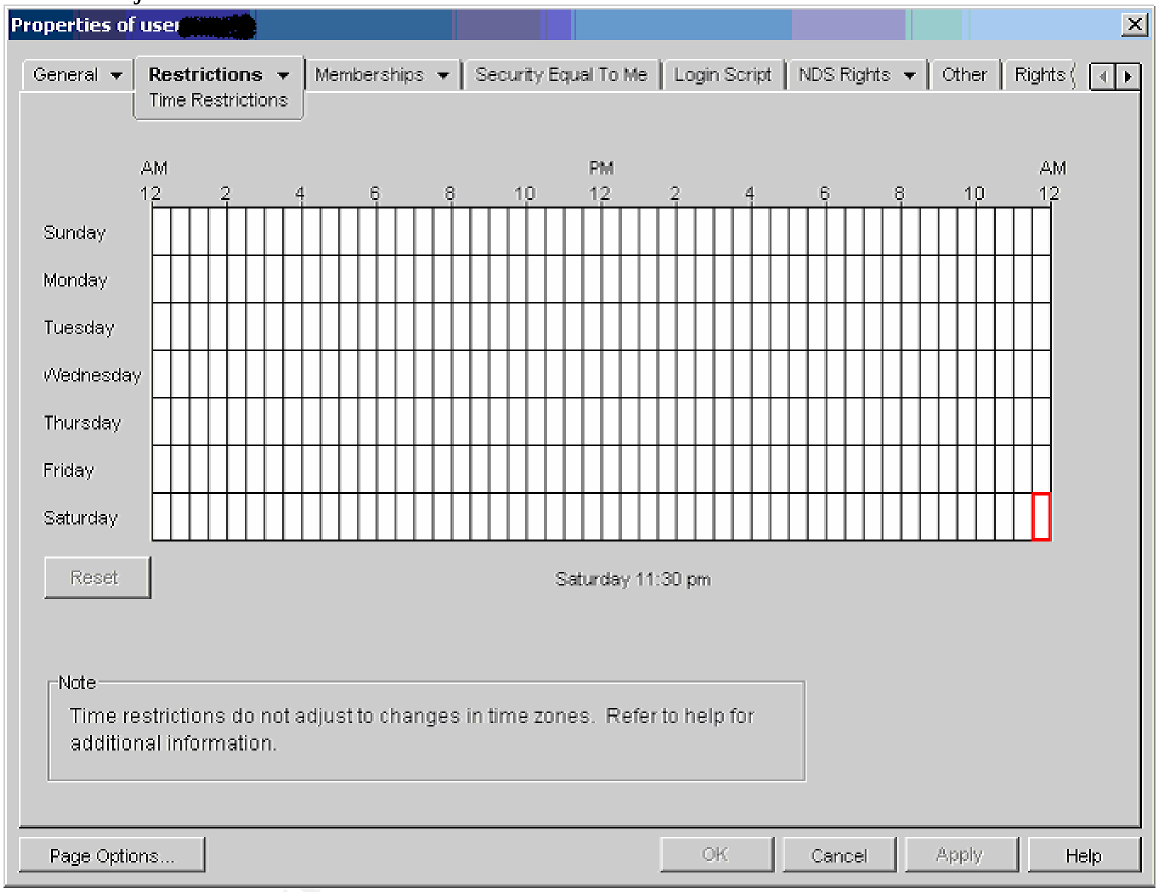
Expiration date and time: August 17, 2004 11:22:00 AM EDT

☑ Limit concurrent connections

Maximum connections: 1

Last login:

Screen shots from the user settings obtained with ConsoleOne looking at the Time Restrictions tab show that no login time restrictions exist. The name of the container where the user objects reside has been masked.



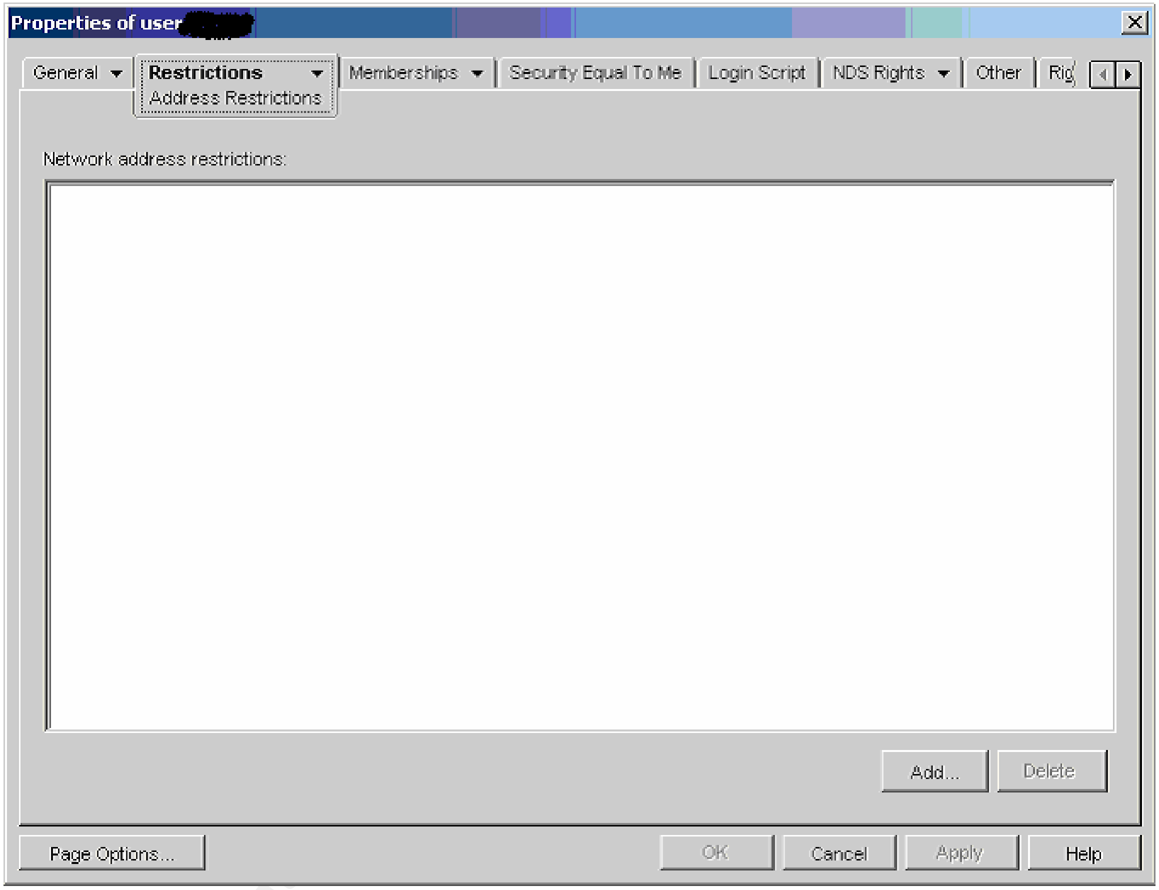
Properties of user [redacted]

Saturday 11:30 pm

Note

Time restrictions do not adjust to changes in time zones. Refer to help for additional information.

Screen shots from the user settings obtained with ConsoleOne looking at the Address Restrictions tab show that there are no address restrictions limiting the networks where users may access the network. The name of the container where the user objects reside has been masked.



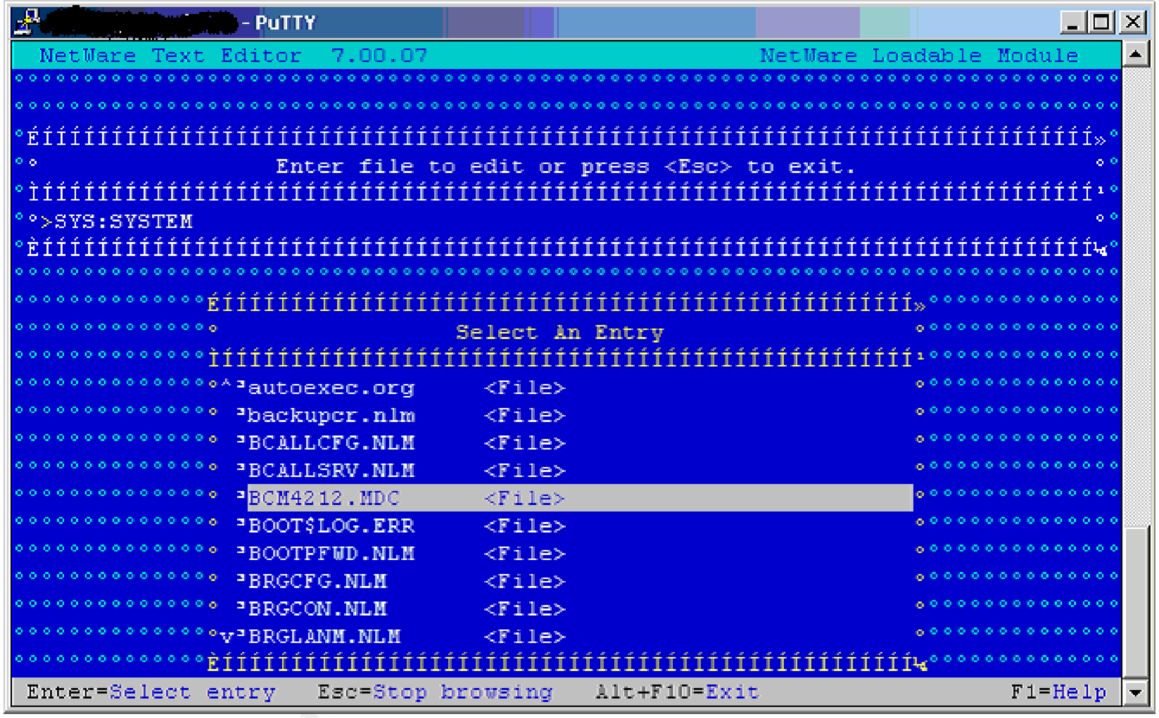
Findings
Limit Concurrent Connections was enabled and set to allow a single connection. Trying to log in from another workstation produced a message stating that the user was trying to log in from too many locations. Time restrictions and Station restrictions were deemed to be too restrictive due to the nature of operations within the organization.

Conclusion
Based on the findings, audit item 4 is rated: PASS.

3.4 Evidence and Findings from Audit Item 5

Evidence

A manual search was conducted from the server's console for the files specified in audit item 5. The screen shot shown below shows the location where the backup.ds and backup.nds files should reside if they are present. The server's name has been masked to protect its identity.



```
[redacted] - PuTTY
 NetWare Text Editor   7.00.07                    NetWare Loadable Module

             Enter file to edit or press <Esc> to exit.

  >SYS:SYSTEM

                            Select An Entry

               ^ autoexec.org      <File>
                 backupcr.nlm      <File>
                 BCALLCFG.NLM      <File>
                 BCALLSRV.NLM      <File>
                 BCM4212.MDC       <File>
                 BOOT$LOG.ERR      <File>
                 BOOTPFWD.NLM      <File>
                 BRGCFG.NLM        <File>
                 BRGCON.NLM        <File>
               v BRGLANM.NLM       <File>

 Enter=Select entry   Esc=Stop browsing   Alt+F10=Exit                 F1=Help
```

Findings

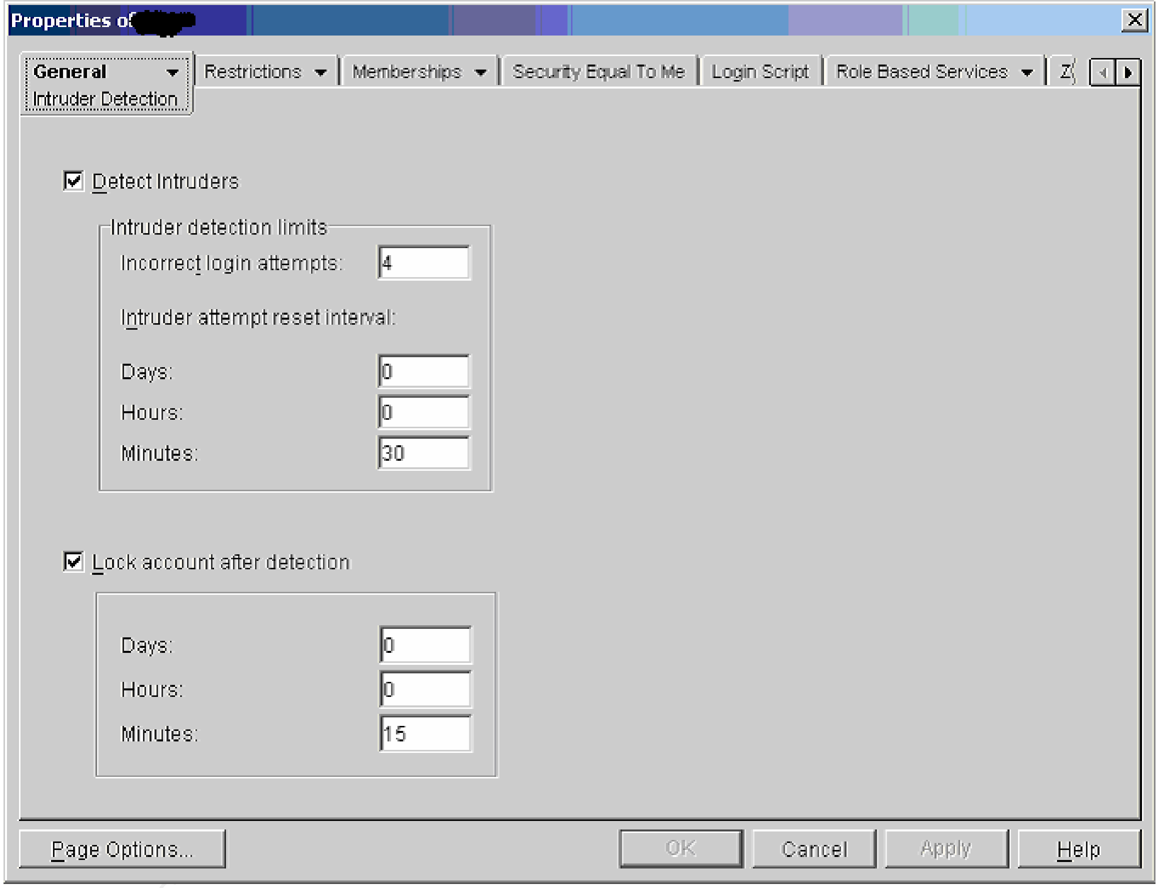
None of the files specified in the audit item checklist were found.

Conclusion

Based on the findings, audit item 5 is rated: PASS.

3.6 Evidence and Findings from Audit Item 6

Evidence
A screen shot from ConsoleOne showing the Intruder Detection settings for the container where the user objects reside.



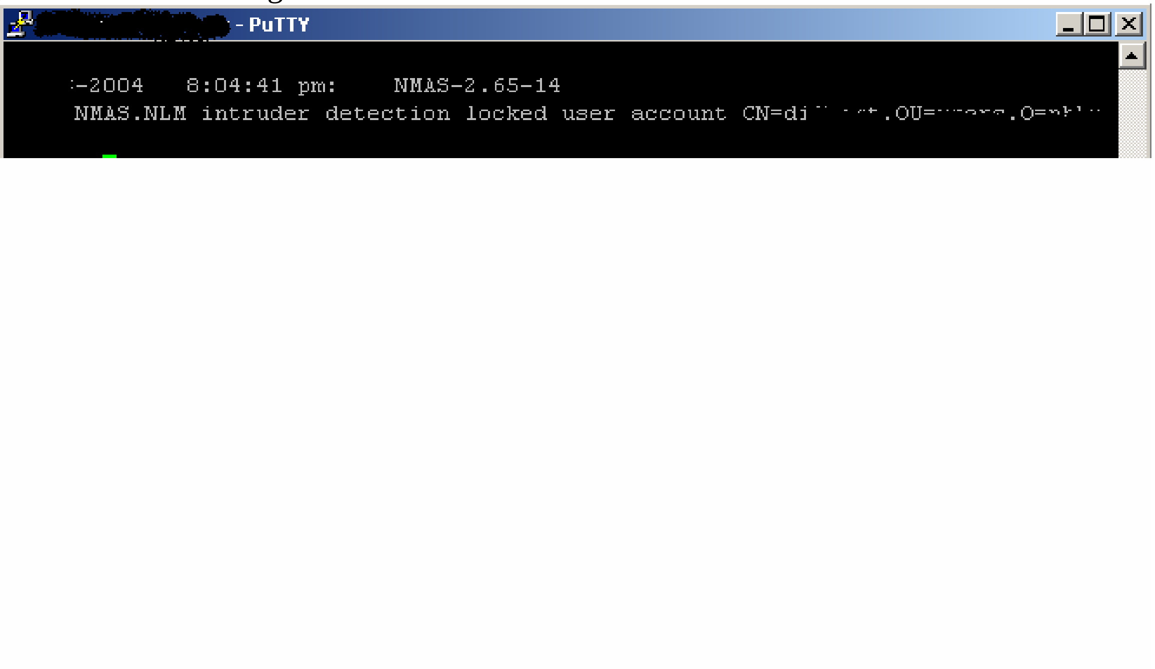
Properties of [redacted]

☑ Detect Intruders

Intruder detection limits
Incorrect login attempts: 4
Intruder attempt reset interval:
Days: 0
Hours: 0
Minutes: 30

☑ Lock account after detection
Days: 0
Hours: 0
Minutes: 15

The intruder detection setting was tested with and found to activate as required. The screen shot below is from the server's console. The server's name, the username used for the test, the container and organization unit have been masked out.



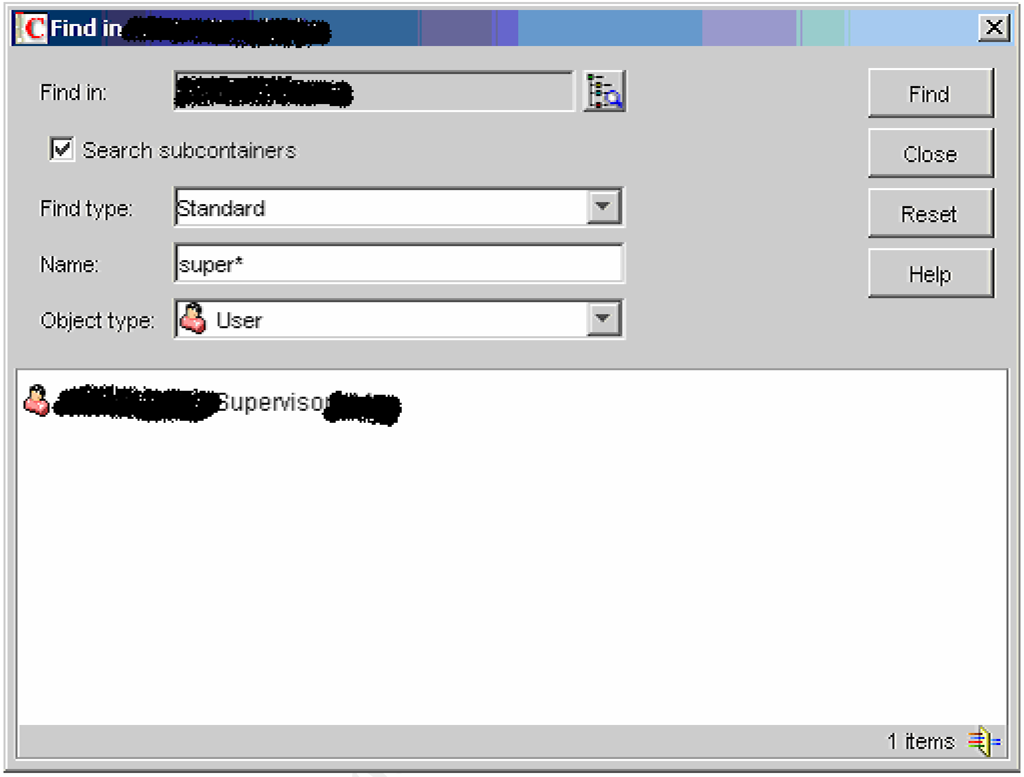
```
[redacted]-2004   8:04:41 pm:    NMAS-2.65-14
NMAS.NLM intruder detection locked user account CN=di[redacted].OU=[redacted].O=[redacted]
```

Findings
Intruder detection was found to be enabled and functional on the appropriate containers.

Conclusion
Based on the findings, audit item 6 is rated as: PASS.

3.7 Evidence and Findings from Audit Item 7

Evidence
The supervisor NDS user object was found to exist as shown in this screen shot from ConsoleOne.



Find in [redacted]

Find in: [redacted]

☑ Search subcontainers

Find type: Standard

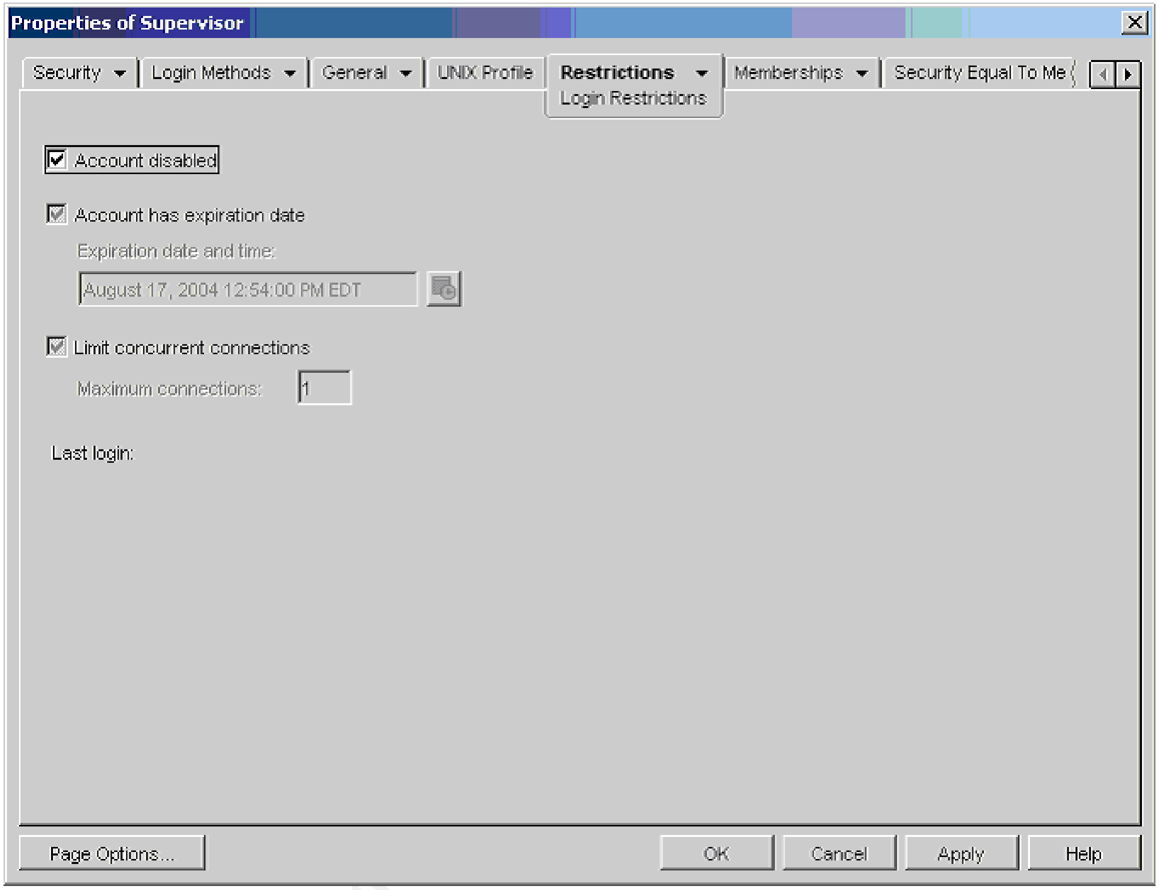
Name: super*

Object type: User

[redacted]Supervisor[redacted]

1 items

The Login Restrictions of the supervisor user object were examined with ConsoleOne and revealed the account was disabled. As shown in the screen shot below.



Properties of Supervisor

☑ Account disabled

☑ Account has expiration date

Expiration date and time: August 17, 2004 12:54:00 PM EDT

☑ Limit concurrent connections

Maximum connections: 1

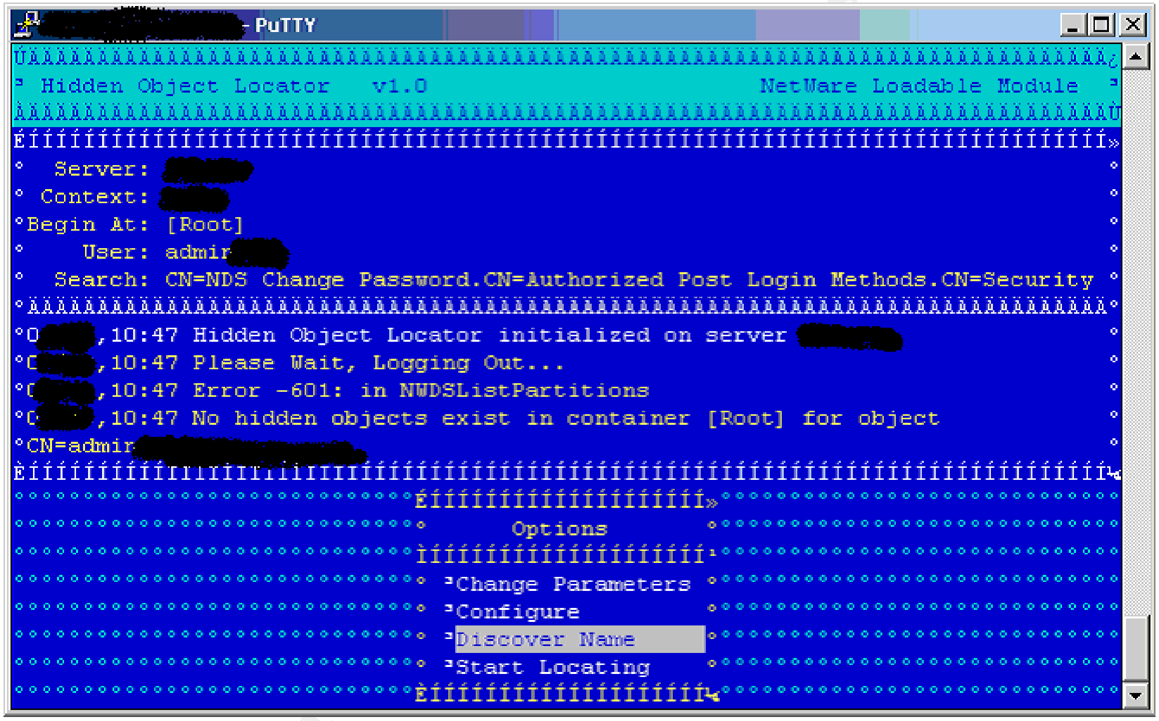
Last login:

Findings
The supervisor object was found to exist and be disabled as required by the audit item.

Conclusion
The supervisor account was found to exist and be disabled as required. NDS authentications take place before bindery based authentications therefore audit item 7 is rated: PASS.

3.8 Evidence and Findings from Audit Item 8

Evidence
The screen shot below is from the server console just after the hidden object locater NLM was used to find any hidden objects from an admin equivalent user object. The screen shot shows the search for hidden object starting from the top most part of the NDS tree, [Root]. Information identifying the server, its location, or the full admin user name has been masked.



[redacted] - PuTTY

```
ÚÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¿
³ Hidden Object Locator   v1.0                           NetWare Loadable Module  ³
ÀÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º  Server: [redacted]                                                               º
º Context: [redacted]                                                               º
ºBegin At: [Root]                                                                   º
º    User: admin[redacted]                                                          º
º  Search: CN=NDS Change Password.CN=Authorized Post Login Methods.CN=Security º
ºÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄº
º0[redacted],10:47 Hidden Object Locator initialized on server [redacted]          º
º0[redacted],10:47 Please Wait, Logging Out...                                      º
º0[redacted],10:47 Error -601: in NWDSListPartitions                                º
º0[redacted],10:47 No hidden objects exist in container [Root] for object           º
ºCN=admin[redacted]                                                                 º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
°°°°°°°°°°°°°°°°°°°°°°°°°°°°°ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»°°°°°°°°°°°°°°°°°°°°°°°°°°°°°
°°°°°°°°°°°°°°°°°°°°°°°°°°°°°º       Options        º°°°°°°°°°°°°°°°°°°°°°°°°°°°°°
°°°°°°°°°°°°°°°°°°°°°°°°°°°°°ÌÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¹°°°°°°°°°°°°°°°°°°°°°°°°°°°°°
°°°°°°°°°°°°°°°°°°°°°°°°°°°°°º ³Change Parameters  º°°°°°°°°°°°°°°°°°°°°°°°°°°°°°
°°°°°°°°°°°°°°°°°°°°°°°°°°°°°º ³Configure          º°°°°°°°°°°°°°°°°°°°°°°°°°°°°°
°°°°°°°°°°°°°°°°°°°°°°°°°°°°°º ³Discover Name      º°°°°°°°°°°°°°°°°°°°°°°°°°°°°°
°°°°°°°°°°°°°°°°°°°°°°°°°°°°°º ³Start Locating     º°°°°°°°°°°°°°°°°°°°°°°°°°°°°°
°°°°°°°°°°°°°°°°°°°°°°°°°°°°°ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼°°°°°°°°°°°°°°°°°°°°°°°°°°°°°
```

Findings
No hidden objects were found to exist in the [Root] container.

Conclusion
Audit item 8 required that no hidden objects be found within the directory. No hidden objects were found therefore audit item 8 is rated: PASS.

3.9 Evidence and Findings from Audit Item 9

Evidence
The photographs shown below are pictures of the outer server room door and the server room itself.

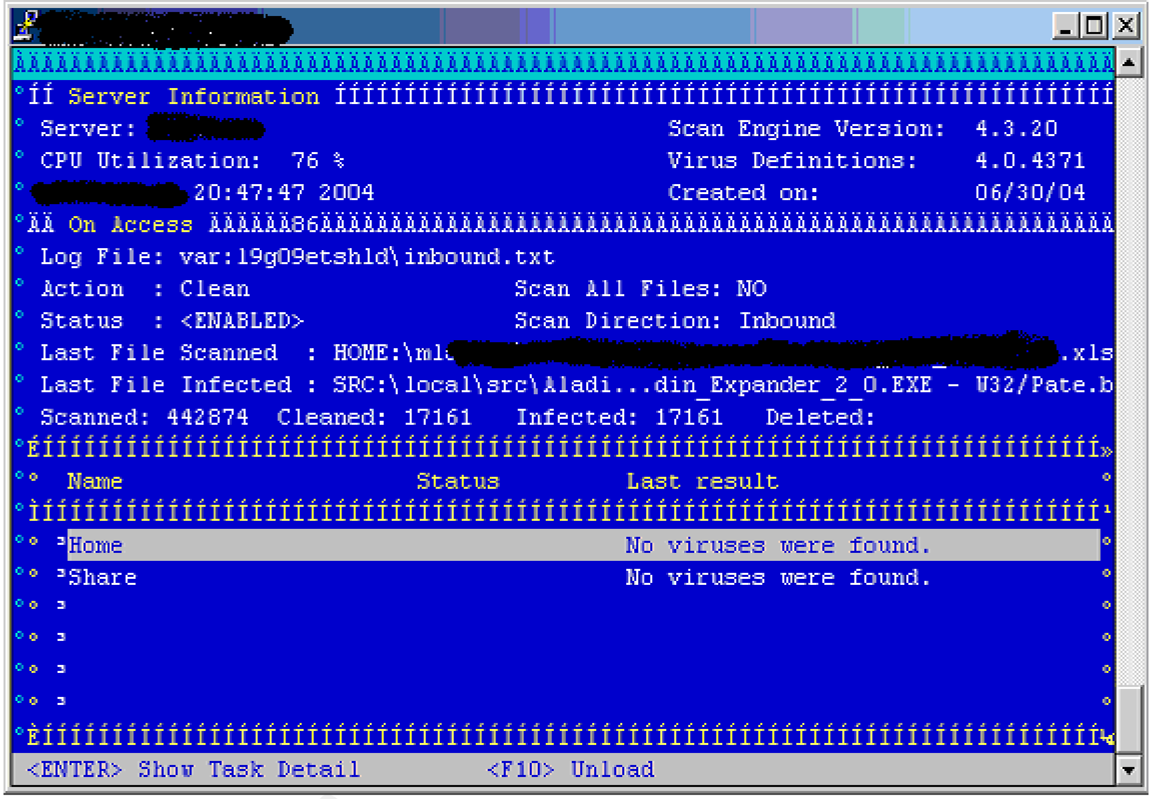
Findings
The server room was found to be under lock and key. Four locked doors must be opened to gain access to the server room. The server room key is restricted to three system administrators. The outer offices just beyond the server room are restricted to the IT staff and are not on the building's master key.

The location is partially monitored by video camera and is periodically patrolled by an armed guard. The equipment itself is not subject to specific monitoring.

Conclusion
Audit item 9 required the equipment to be monitored by video camera, contact switch, security personnel or similar means. Based on the findings, audit item 9 is rated as: FAIL.

3.10 Evidence and Findings from Audit Item 10

Evidence
This is a screen shot of the server's anti-virus software as seen from the server's console. The anti-virus software is clearly detecting and cleaning viruses as they come into contact with the file server. Identifying information has been masked.



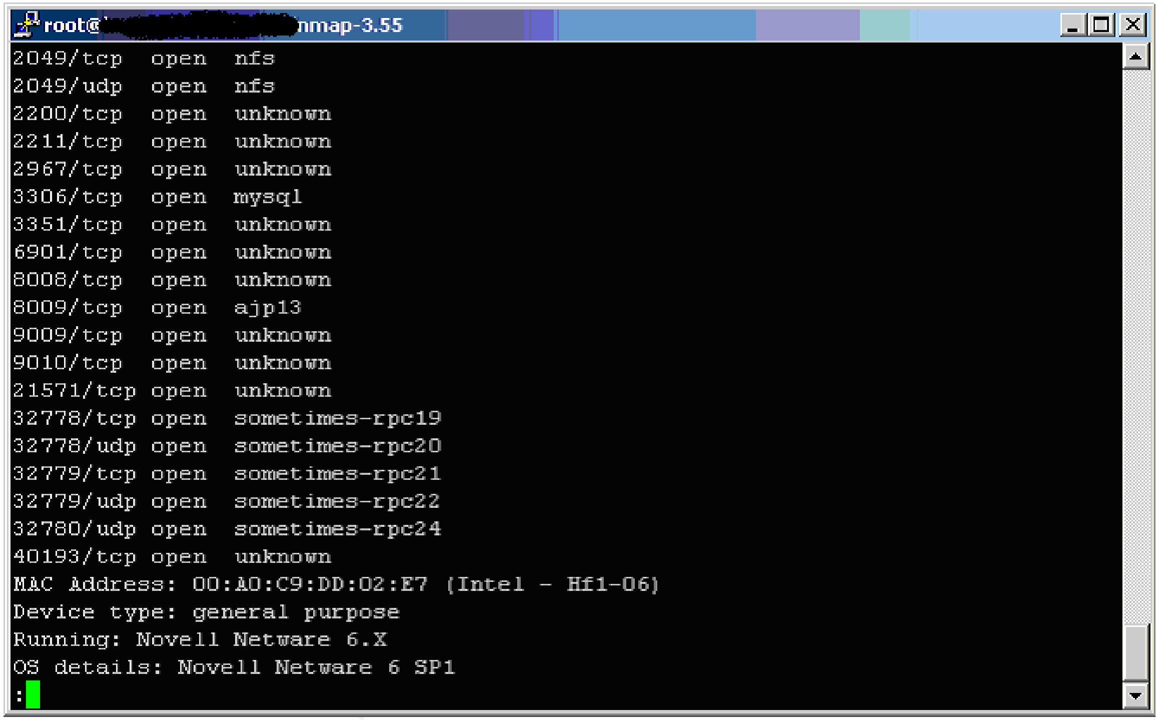
```
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
°ÍÍ Server Information ÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ
° Server: [redacted]                           Scan Engine Version:  4.3.20
° CPU Utilization:   76 %                       Virus Definitions:    4.0.4371
°[redacted] 20:47:47 2004                       Created on:           06/30/04
°ÄÄ On Access ÄÄÄÄÄÄ86ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
° Log File: var:19g09etshld\inbound.txt
° Action   : Clean                   Scan All Files: NO
° Status   : <ENABLED>               Scan Direction: Inbound
° Last File Scanned  : HOME:\ml[redacted].xls
° Last File Infected : SRC:\local\src\Aladi...din_Expander_2_0.EXE - W32/Pate.b
° Scanned: 442874  Cleaned: 17161   Infected: 17161   Deleted:
°ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
°º  Name                        Status         Last result                    º
°ÌÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¹
°º ³Home                                       No viruses were found.         º
°º ³Share                                      No viruses were found.         º
°º ³                                                                          º
°º ³                                                                          º
°º ³                                                                          º
°º ³                                                                          º
°ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
 <ENTER> Show Task Detail          <F10> Unload
```

Findings
The auditor expected to copy the eicar test virus to the file server to test the anti-virus software. When the anti-virus software screen was observed it was obvious that the anti-virus software was working properly. The virus definitions were checked against the McAfee website and found to be current. The IT department has an automated procedure in place to update the anti-virus definition files.

Conclusion
Based on the findings, audit item 10 is rated: PASS.

3.11 Evidence and Findings from Audit Item 11

Evidence
The IT staff was asked which services they offered on their Netware server. After receiving their answer, nmap version 3.55 was invoked with the options provided in the audit checklist. A screen shot of that scan is shown below. Identifying information has been masked.



```
2049/tcp  open  nfs
2049/udp  open  nfs
2200/tcp  open  unknown
2211/tcp  open  unknown
2967/tcp  open  unknown
3306/tcp  open  mysql
3351/tcp  open  unknown
6901/tcp  open  unknown
8008/tcp  open  unknown
8009/tcp  open  ajp13
9009/tcp  open  unknown
9010/tcp  open  unknown
21571/tcp open  unknown
32778/tcp open  sometimes-rpc19
32778/udp open  sometimes-rpc20
32779/tcp open  sometimes-rpc21
32779/udp open  sometimes-rpc22
32780/udp open  sometimes-rpc24
40193/tcp open  unknown
MAC Address: 00:A0:C9:DD:02:E7 (Intel - Hf1-06)
Device type: general purpose
Running: Novell Netware 6.X
OS details: Novell Netware 6 SP1
:
```

Findings
Unexpected services were found above port 10,000. These ports were revealed by nmap to be a combination of TCP and UDP services.

Conclusion
Based on the findings and the statements from the IT staff, audit item 11 is rated: FAIL.

In the interest of time and space, six audit items were not presented.

Part 4 – Audit Report

4.1 Executive Summary

This security assessment was conducted with the intent to provide management with an overview of the security posture pertaining to the directory services used within their organization. The organization has grown over the past few years and so has their network and server farm. Since the organization's beginning, management had the foresight to install a directory based authentication and access service, which has enabled the organization to easily incorporate numerous devices into their diverse network. The organization has been awarded numerous grants from the government and private sectors to conduct top quality research in many areas of medical science. Management understandably desires to protect their investment in view of their organization's growth. This assessment was deemed successful by the auditing party and the technical staff who assisted with the assessment. Overall the audit team's concerns on its findings are minor and the overall quality rating of the organization's security is deemed to be 90 to 95%. Remediation costs, if any, are anticipated to be very modest and within the budget parameters established by management.

4.2 Audit Findings

Overall the security posture of the organization was found to be very good. As with most things, there is room for improvement after careful consideration. Each audit finding which resulted in a failure will be discussed. Recommendations will be presented in the next section.

Audit item 1 found that it was possible to enumerate usernames without having an authenticated connection to the directory. This potentially exposes the usernames to an attacker who could launch a password attack against those users or potentially log in to the directory immediately if a user account were found to contain no password. It is worth noting that although usernames were exposed during the assessment, no user accounts were found to be without a password and steps have been taken to prevent password attacks via the directory's Intruder Detection mechanism. The intruder detection system was tested and found to function properly.

Audit item 9 revealed that server room access was not monitored around the clock. Key access to the server room is restricted to the IT department's system administrators (three people) and the outer offices of the IT department are not on the building's master key. Access to some parts of the building are subject to video monitor but it is possible to enter and exit the building without being monitored. The IT staff pointed out the video system was installed after the building was constructed and was not intended to monitor the server room.

Audit item 11 found that unexpected and unknown ports were open on the directory server. The assessment tool (nmap) suggested that the ports might belong to an RPC service. This was not expected by the IT staff and resulted in a "fail" on this item. The IT staff began to investigate the service or services running on those ports before the audit was concluded. The IT staff stated that they had no reason to believe the system had been compromised or was not functioning as expected. This detect may have been anomalous and will be researched by the auditor when he returns to his office.

4.3 Audit Recommendations

The overall security posture of the organization was found to be very good. The following recommendations are not requirements; they are areas the organization may wish to explore to further enhance their security posture.

Preventing the enumeration of usernames makes an attacker's job somewhat more difficult because they need more than a password to gain access to the directory. One method to remedy username enumeration by unauthenticated users is to remove [Public] as a trustee of [Root] as outlined in Novell Technical Information Document (TID) 10026672. The auditor appreciates that this is a difficult decision that may have unforeseen repercussions for users of the directory. Testing is advised before proceeding with this option. Another course of action that may prove to be effective would be to restrict remote access to the directory via firewall rules. This option must be tested as it may impact the organization's remote users. Removing [Public] as a trustee of [Root] entails no cost other than the time of the IT staff to actually test and perform the work. Recommendations involving a firewall may incur cost to the organization if the organization lacks a firewall or lacks an adequate firewall. This assessment made no determination concerning any of the organization's firewalls.

Monitoring the physical security of the data center's hardware is the surest means of preventing physical theft or damage to the hardware. The data center contains several UPS equipment with modules that are capable of registering switch closures. An alarm technician could install a magnetic switch for a modest fee, which could be connected to the UPS. With the appropriate software, the UPS could alert someone that the data center's door has been opened unexpectedly.

Understanding which services are offered on a server is important in maintaining the server's security. Unexpected ports were found on the server where the directory resides. At the time of the assessment, this was unexpected behavior. Research should be conducted to determine the nature of the services found on the ports above 10,000. Additional monitoring by an external machine may be necessary in order to capture traffic destined to or from those ports to determine its nature.

References

Chase, Philip, Moffat, Iain, Sallot, Ken: *Best Practices for Netware Security*. http://grove.ufl.edu/~pbc/itsa/netware-security-slides.ppt

CSI's '2004 Computer Crime and Security Survey http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

Foust, Mark. *Netware Security: Closing the Doors to Hackers.* http://developer.novell.com/research/appnotes/2000/june/03/apv.htm

Loveless, Mark (Simple Nomad). *Top Ten Security Threats to Novell Netware.* http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NNW_WP.pdf

Loveless, Mark (Simple Nomad). *Top Ten Security Threats to Novell NDS eDirectory*. http://www.bindview.com/resources/WhitePapers/TopTenSecThreats_NDS_WP.pdf

SANS Glossary: http://www.sans.org/resources/glossary.php.

SANS Track 7 Course materials

Software

DSSec (DSSecurity) http://www.geocities.com/wstools/files/dssec.zip

Eicar test virus: http://www.eicar.org/anti_virus_test_file.htm

Hidden Object locator: http://www.novell.com/coolsolutions/tools/1098.html

Locations of NDS files: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10073559.htm

Pandora http://www.nmrc.org/project/pandora/index.html

Mapping DS.NLM versions to eDirectory version http://support.novell.com/cgi-bin/search/searchtid.cgi?/10066623.htm

NDSrpt (NDSReport) http://www.geocities.com/wstools/files/ndsrpt.zip

Nessus: http://www.nessus.org

Nmap: http://www.insecure.org

Novell's Minimum Patch list: http://support.novell.com/produpdate/patchlist.html