GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

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

Novell NetWare 6 Security Baseline Configuration. Security best practices for deploying and managing a NetWare environment.

March 2004

John Saley
GSEC Practical 1.4b
Option1

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Summary

Novell Netware 6 provides a host of network services and access options. At NetWare's core is a robust file and printer server, and eDirectory. As with most standard OS installations, it attempts to install components that are often not needed and should not be installed. Securing the server OS (NetWare) to a standard baseline configuration reduces many security and support issues in small deployments and even more issues in larger deployments. This baseline configuration includes support for the following NetWare services: Files access, NDPS, iManager, and Netware remote manager. The heart of access control and password management in a NetWare environment is the eDirectory. Properly managing objects within this directory structure is key to providing end users with access to the appropriate network resources.

The scope of this document is to provide a baseline for deploying and managing a Netware 6 environment using the best-known security practices. This document assumes you have a strong working knowledge of NetWare and eDirectory (which will be referred to a eDir within this document). Although NetWare does not appear to be a frequent target of attacks, that does not mean that you can disregard security in implementation. The base install product has relatively good security, although there are a couple of inherent security weaknesses within the NetWare 6 product where 3rd party solutions can be implemented to correct these shortcomings.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

All network design and security must be based on a common baseline of standards. These standards should be fully documented within a strategic company security policy. This security policy should provide the basis for all implementations throughout the enterprise. Whether the implementation involves a switch, router, firewall, Netware server, Windows server, or Unix server; the security principles within the security policy should apply. The security policy should define the proper procedures and controls to sustain a manageable but secure network. The importance of this underlying security policy cannot be understated. If it has not been determined what should be classified as sensitive information, determination of access rights cannot be made.

Netware programs which are created c+ programs with the extension of NLM. Java applications and perl scripts can now also be run on the server (4). The ability for any exe or com virus to directly infect the server is unlikely. However this does not mean the server cannot be the storage area for such infected files, or be on the receiving end of a virus that deletes files on mapped drives.

The server should be provided adequate physical security. The server should be located in a self-locking server room. Only authorized people should have access, preferable with an electronic keycard, so entry times are properly logged. The server room environment should be temperature- and humidity-controlled. The server should be provided adequate backup power in the event of a power outage.

The server should be physically attached to a private internal segment that is protected by several layers of defense, including firewalls, router ACLs , and VLANs. Configure the hardware with minimum RAID 5 drive configuration for drive redundancy. Hardware should have redundant power supplies to reduce the possibility of any server outage (physical denial of service).

Document all server builds with corresponding documentation on responsible parties for providing maintenance to the server including software, hardware, and backup responsibilities. Provide copies of the documentation to parties responsible for providing maintenance to the server, including software, hardware, and backup responsibilities.

Verify that the system bios, array bios and any other device firmware are current versions.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Selection of which server components to install should be fully understood before proceeding with server installation. To minimize exposure to unknown vulnerabilities, only services that are required should be installed. This baseline installation is designed to provide sufficient access to file and print services for end users within a protected private network. Any access required outside this protected network should be provided with a VPN solution, which is outside of the scope of this document.

Base Netware installation

Create SYS volume as 4 Gig NSS; do not install compression. Create VOL1 NSS pool with the remainder of the drive space less %10. The 10% extra is spare drive space that can be assigned only when a critical need occurs. Specific components not installed in this baseline include:

- Enterprise Web Server – Web services are a highly targeted technology. It is uncommon to use NetWare as a web server platform. If the server does not require its use, then remove it.
- Web Search – Again a possible target for attacks. it is uncommon to use NetWare as a web server platform. If you do not use it, remove it.
- Native File Access Pack – Native access pack allows for non-NetWare clients to connect to NetWare storage as native storage (AFP, NFS,CIFS). If using a simple password for authentication using native file access, the password is sent in clear text and should be avoided.
- FTP Server – Since FTP passes network credentials in the clear, running the FTP server is not recommended.
- LDAP – If not needed, LDAP should be removed as it can be used to acquire account information from within the eDirectory
- ifolder- I-Folder allows synchronized data access to data located on the server. If this product is to be used, additional Apache security should be implemented. If no plans exist to use this technology, remove it.
- Netstorage – Allows access to file system using standard web browser. This should not be installed unless required.
- WebAccess – Allows a centralized web portal to various web-enabled services with links to Netstorage, WebAccess, and iFolder. Do not install this component unless required.

Inetcfg settings

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

This baseline assumes a single bound network adapter configured as “end node” using only IP protocol with routing disabled. I think it is best to leave the routing to devices (hardware routers) that are more suited for it. Disable routing protocols (RIP, OSPF) and add LAN static routing table whenever feasible. Configure SNMP parameters by setting strong community names for both the monitor and control community. Never use public and private as community names. Disable remote control access. Other remote console methods should be used. Make sure you are using current TCPIP NLMS and network drivers.

Edit autoexec.ncf file.

- Remove STARTX- having a gui interface on NetWare is unnecessary and a bit silly; save server resources and don’t load it. As always, if it is not needed, remove it.
- On HP (Compaq) servers, remove CPQIML (integrated management log viewer) and CPQONLIN (array configuration utility)
- Load scrsaver enable lock – Enables a console locking screen saver that requires console rights credentials to unlock.
- Do not load RCONAG6.NLM – This remote console does not encrypt the console session and should not be used.

Do not set a bindery context - many legacy bindery attack tools still exist; although they may not be successful in the attack, don’t even open up the opportunity. Update any equipment or software that still requires the bindery emulation.

Since the included remote console options rconsole and rconJ have security weakness that would allow for the possibility of credentials being compromised, a 3rd party option should be used. In this baseline configuration, we use sfConsole from Adrem Software (1). This software allows for strong encryption of the remote console session, and uses eDir credentials to authenticate to the console.

When creating NDPS Manager to provide print services, make sure you place the queue on VOL1. Never put a conventional print queue or NDPS manager on the SYS volume; a denial of service could occur if the SYS volume runs out of disk space. The SYS volume should be utilized for Netware OS files only.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Netware with only IP bound will use the following type of TCP/UDP protocols (13)

ICMP Type 8
NCP (NetWare Core Protocol) TCP/UDP 524
SLP (Sevice Location Protocol) TCP/UDP 427
HTTP (Apache web server) TCP 80
HTTPS (Apache Web server) TCP 443
HTTPS (Netware Remote Manager on Apache Web Server) TCP 8009 (port configurable)
HTTPS (iManager on Apache Web Server) TCP 2200 (port configurable)

A port scan should be done before implementing a filter configuration. Port scans can be done by a variety of products, such as Nmap or Nessus. If additional ports are found that are not listed above, a determination of the service should be completed before proceeding. Matching any open ports to the port number assignments in Appendix A will help in identify what service may be running. If that service is not required, remove the associated component.

Filter Configuration
All traffic that is not specified should be dropped by using filter configuration. The best practice is to drop all traffic except that which is explicitly defined. Define IP packet forwarding filters. Although the name “IP packet forwarding filters” imply routing, these filters will also be in effect when the server is configured as an end node without routing enabled. It is imperative that all required services are documented so that valid ports are not mistakenly blocked (7).Use FILTCFG.NLM to configure all protocol filtering

Console logging
Load conlog Archive=Yes next=01:00 Entire=Yes Maximum=10000 (15)(14) will log all console events and archive daily at 01:00 up to 1000 days worth of logs.

Load secure console at the end of the autoexec.ncf file. This prevents nlms from being loaded from locations other than sys;system, and c:\nwserver. It also prevents the time from being changed at the console (8) Many backup agents or other add on products are loaded from other volumes than sys: make sure they are loaded before securing the console.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Set a BIOS-level password to prevent unauthorized boot order changes. Access to this password information should be restricted to members of the server admin group, who are responsible for maintaining the server. Change boot order in BIOS configuration to prevent booting from the CDROM drive.

When using the hardware manufacturer's management utilities, such as Compaq Insight Manager and Dell Open Manager, make sure that you have the current version installed and verify that default passwords are changed to strong passwords.

Stay aware of current revisions of services packs and other updates at http://support.novell.com/filefinder/13659/index.html . Read what the patch fixes and test in a lab environment before deploying into production.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

All of NetWare's access control is based in a directory called eDirectory. This directory contains numerous object types and object properties. The eDirectory tree should have a hierarchical design that should properly reflect the company's layout. Replication of the Edirectory partitions (replicas) should be considered when designing the tree structure, to provide directory fault tolerance. All eDir partitions should have a Master and 2 read/write replicas for redundancy. Since the security within eDirectory is inherited from higher up in the tree, tree design is critical to proper security management. Rights assigned should reflect the principle of least privilege, thus only assigning rights to container objects where all subordinate objects should have these same rights. Group Objects should be used to assign common rights among users with the same access needs. Assign explicit rights to users only when they do not meet group criteria. Below are important objects that need special consideration regarding security:

- Admin (User Object) This account is installed when the first server is installed into the tree. This account has full rights to the entire tree ([root]) and directory schema. This account should be renamed and moved to a context that contains other users so that it does not stand out. This renamed account should only be used rarely (3).An additional account with supervisor rights to the [root] object should also be created, as a backup administrative "full rights" account for doing high level directory changes, such as extending schema or merging trees. Otherwise these accounts should not be used on a daily basis. A "fake" admin user object should be created with no rights and disabled in the organization context. This "fake" admin account should be audited and audit logs checked regularly.
- All NetWare administers and help desk specialists should be granted only the trustee assignments that they need to perform their required jobs.
- Guest accounts should be deleted. No common accounts should be used amongst multiple end users. All users should have their own login credentials.
- The Everyone group should not be used.
- Container Objects – when rights are assigned to a container, all objects within that container inherit those rights. Make sure that you want all objects to receive assigned container rights. Assigning an IRF (inherited rights filter) can limit these rights down the tree, but should be used

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

sparingly, as they often become difficult to manage in a large environment. Remember to assign rights based on need of the end user, using the principle of least privilege. Set intruder detection at the container level; set lockout at 3 failed attempts and lock account for 2 hours. Although this may increase the number of help desk calls, it will significantly reduce the ability to brute force attack a password.

- Groups Objects offer a good method of assigning rights to specific groups of users that have the same access needs. Make sure group membership is audited frequently, as users move from different job functions and likely should be removed from previous group memberships. Group Objects should be consistently named throughout the tree and properly documented, to simplify administration. For example, a PROJECTS group in one office container should be given the same name in all offices and should correspond to similar data areas.
- Special user accounts - Accounts that are created for specific job runs, such as backups, should also be assigned address restrictions to allow the account to be used only from the defined workstation MAC address.
-

Password Authentication with the Netware client and eDirectory uses a secure challenge response login.

The following password restrictions should be set at the user container level or within the user template so that all users will get the same password restrictions.
☑ Allow user to change password
☑ Require a password – Minimum password length =8
☑ Force periodic changes =30 days – This can be increased if a stronger password 3rd party solution is implemented.
☑ Require unique password – Do not allow users to reuse passwords. Unfortunately this does not prevent users from appending passwords with just a small numeric change at the end of the password;-. a 3rd party solution is required to support password complexity.
☑ Limit grace logins = 1. Force users to change passwords immediately.

If 2-factor authentication is required for a substantial increase in security, NMAS (Novell Modular Authentication Services) can be used with a variety of smart cards, biometric devices, and key fobs (6).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Connectotel software provides a 3rd party solution for providing improved password security that includes the following policy criteria(2). This solution should be implemented to achieve strong passwords (12).

- Minimum and maximum password length
- Minimum and maximum alpha characters
- Minimum and maximum numeric characters
- Minimum and maximum special characters
- Maximum consecutive character types
- Maximum instance of any character
- Algorithm comparison with old password

Additional password security considerations must be taken when using add-on products to allow synchronization of accounts to different directories such a DirXML, Account Management, and Zenworks DLU (Dynamic Local User). Since your account credentials would then be stored in a hash that may not be as secure as the eDirectory. (Not a complete sentence) Make all efforts to protect these passwords in all locations. The network password security is only as strong as its weakest link.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Installing the Netware client without making settings to match your NetWare environment can cause additional unneeded network traffic and degradation of client and network performance. In this baseline configuration, the assumption is that the only server attachments will be made to NetWare servers. The standard installed “Client for Microsoft Networks” cannot be removed due to several dependencies to the client components that exist. For example, the BITS (background Intelligent transfer service) used for automatic updates from Software Update Services requires client components be installed. Although it cannot be removed, it does not have to be bound to the network adapter. Unchecking both “Client for Microsoft Networks” and “File and Printer services” will dramatically improve client performance, by removing the need for both clients to parse network requests. Disabling these options also reduces exposure to many Microsoft client vulnerabilities. Securing Netware extends well beyond the NetWare server itself, always look for the weakest link of attached device or user. Verify NetWare client protocol setting use only the protocols that are needed for name resolution.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

As an eDir tree grows in size, it becomes apparent that manually auditing accounts is not realistic. Various tools need to be utilized to perform these auditing functions. Listed below are some tools and methods that are used to retrieve the needed audit information.
ODBC driver for eDirectory. This read only ODBC driver allows for custom reports to be created with any database reporting tool such as Crystal Reports. Some useful reports that can easily be created and used are:

- Disabled account report – Checking for disabled accounts allows for removal of these accounts after the specified time documented in your company security policy and procedures.
- Unused account report- Checking the last login time will allow you to eliminate accounts that are no longer used.
- Group Membership reports- Listing group membership in groups can be used to verify that they are members of the appropriate group.
- Personal Login script report – Generating a report that lists personal login scripts allows verification of non-standard mappings. Normally, personal login scripts should be avoided, as they become difficult to manage. But in instances where explicit user mapping occurs, it can easily be visible within this report.

Novell Advanced Audit Service (NAAS) is included with NetWare 6, but falls short of providing a good audit tool for larger enterprises, as it does not scale well across partitions of the eDirectory tree (9).

A good 3rd party option for providing audit services is LT auditor + from Bluelance Computer Security Software. This software offers the following benefits (11).

- monitors and audits users, files, and system activity
- Tracks sensitive files and directories
- Immediate notification of security
- Granular reporting for faster and easier forensic analysis
- Monitors all eDirectory/NDS changes

Always check various sources for possible NetWare vulnerabilities and methods or reducing or eliminating the possible exposure(10).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

(1) http://wwwadremsoft.com/sfcon/features-detail2.php?ix=0
(2) http://developer.novell.com/research/appnotes/2000/august/02/apv.htm
(3) http://secinf.net/netware/Securing_Your_NetWare_Environment_.html
(4) http://novell.unc.edu/security/security.htm
(5) http://www.novell.com/documentation/lg/nw6p/adminenu/data/aclkn27.html
(6) http://www.novell.com/documentation/lg/nmas202/admin/data/a53s8fw.html
(7)http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/filtrenu/data/hitaqkml.html
(8)http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/utlrfenu/data/hm9phvjr.html
(9)http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/naas_enu/data/a4fe5v6.html
(10)http://secunia.com/product/78/
(11)http://www.bluelance.com/products/lta_nw/
(12)http://www.novell.com/coolsolutions/zenworks/trenches/tr_pwd_policy_mgr_zw.html
(13)http://www.novell.com/coolsolutions/netware/features/a_ports_nw5_nw.html
(14)http://archives.neohapsis.com/archives/sf/pentest/2001-01/0024.html
(15)http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/utlrfenu/data/hq1lykxx.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix A
Common Novell Port assignments

Apache	80 443
Apple* Filing Protocol (AFP)	548
BorderManager™	21 119 443 1040 1045 1959 7070 8080 9090
Common Internet File System (CIFS)	139
CsAudit	2000
DirXML™ NDS-to-NDS®	8090
DirXML Remote Loader	8000
Domain Name Service (DNS)	53
eGuide	389 636
File Transfer Protocol (FTP)	20 21
GroupWise® Monitor	1099

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

GroupWise Internet Agent (GWIA)	25 110 143 389 636 9850
GroupWise Web Access	80 443 7205
iFolder™	80 389 443 636
iMonitor	80
iPrint	443 631
Lightweight Directory Access Protocol (LDAP)	389 636
Line Printer Requester (LPR)	515
Media Server	554
Message Transfer Agent (MTA)	3800 7100 7180
NetWare Core Protocol™ (NCP™)	524
NetWare Enterprise Web Server	80 443

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

NetWare File System	20 111 2049
NetWare Graphical User Interface	9000 9001
NetWare/IP (NWIP)	396
NetWare Remote Manager (NRM)	80 81 8008 8009
NetWare Web Access	80
Network Time Protocol (NTP)	123
NLSLRUP.NLM	21571 21572
Novell Internet Messaging System (NIMS™)	80 81 110 143 389 443 444 636
Novell Modular Authentication Services (NMAS™)	1242
Portal Services	80 443 8080

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Post Office Agent (POA)	1677 2800 7101 7181
Radius	1812
Remote Console™ DOS	2034
Remote Console Java	2034 2036 2037
Server Compatibility Mode Driver (SCMD)	2302
Service Locator Protocol (SLP)	427
Simple Network Management Protocol (SNMP)	161
Telnet	23
Tomcat	8080
Virtual Private Network (VPN)	213 353 2010
Web Manager	2200
Zenworks™ for Desktops 3	2544 2638 8039

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Zenworks for Servers 2	80 443 1229 2037 2544 8008 8009

Port assignments (5)

© SANS Institute 2004, Author r

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.