Securing Novell NetWare 6

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b (amended September 4, 2002)
Option 1

By: Darren Mattila

November 20, 2002

Abstract

Novell NetWare 6 offers several new services and has displaced the long-standing IPX/SPX protocol with TCP/IP as its primary protocol. These changes have exposed the NetWare servers, long isolated by virtue of the IPX protocol, to more dangers than previous versions. This document will discuss some general and specific procedures, settings and precautions now required to keep the NetWare server secure. This discussion will be limited to the standard services included in NetWare 6 operating system.

General Netware Security

The following are security items specific to securing a Novell server. In addition, precautions common to all servers (regardless of OS vender) should be used (i.e.: remove or disable unneeded services, physically secure the server, etc.).

Activate the Secure Console function.

This limits the actions that can be taken from the console by the following:

1. Restricts NLM loading from only the System and local server NWSERVER directories.
2. Prevents keyboard entry into the operating system debugger.
3. Prevents date and time change from the console.

To activate the Secure Console, simply enter “Secure Console” at the server console prompt. The system must be shut down and restarted to disable the Secure Console feature.

Enable password protection to the console.

Entering the SCRSAVER command at the console will produce a screen saver after 10 minutes of console inactivity. A user login is then required to access the console. The user must have the Write right to the access control list of the server object in the eDirectory in order to access the console. Command options are available to allow you to enable and disable locking, check the status of the lock options, and change the length of time the console is allowed to be inactive before the screen saver is activated. The default is 600 seconds (10 minutes).

Isolate the SYS volume.

NetWare uses the SYS volume for operating system files and this volume should be isolated as much as possible from user activity. Do not create the user home directories on this volume. Also avoid using this volume to host the print queues or application directories. NEVER give users trustee assignment rights to the root of this volume (or any volume for that matter). Users are granted Read and File Scan to the LOGIN and PUBLIC directories by default for login purposes.

Keep an eye on NLM integrity.
Novell makes available a set of free utilities to analyze NetWare server configurations. The CONFIG.NLM is run at the server to produce a text file that contains the server information. The Config Reader program is used to analyze the resulting config.txt file and can be used to compare two Config files. By comparing the current Config file with a previous one, you can detect any changes in the NLM versions loaded at the server. This utility will also track your patch versions and alert you when a patch is needed.

These utilities can be downloaded from the Novell web site at http://www.novell.com/coolsolutions/tools/1500.html.

The Config Reader utilities will also provide you with information about installed patches, licensing, memory, AUTOEXEC.NCF and STARTUP.NCF file contents and volume information.

Look for hidden objects in NDS.
A common method used by attackers, after gaining Admin access, is to create a hidden OU in the NDS tree to place their user object. The attacker creates an OU object and removes browsing rights to the rest of the tree. He then creates his Admin equivalent account in this container. These objects could go undetected without the aid of Novell's Hidden Object Locator. It is available for download at http://www.novell.com/coolsolutions/tools/1098.html. [4]

Remove bindery contexts.
Bindery contexts are often configured to support legacy applications and clients. If the NetWare server has been upgraded the bindery context settings may have traveled with the upgrade. A bindery context setting causes Netware to emulate the bindery database of the earlier NetWare versions. This bindery emulation makes the server vulnerable to hacking tools created for use on the older NetWare versions and should be removed as soon as possible. Check the contents of the AUTOEXEC.NCF file for a SET BINDERY CONTEXT command line. Be aware that removing the bindery context could break any bindery based functions configured on the network. One example of bindery based functions would be printers configured in bindery mode.

Remove NDS backup files.
Check for the existence of files called BACKUP.NDS or a BACKUP.DS on the NetWare volumes. If found they may be old NDS backup files from previous upgrades or NDS troubleshooting. These files could be used by an attacker with the Pandora utility to crack user passwords from the old NDS. This would give an attacker access to accounts that haven't had the passwords changed.

Monitor console activity.
Console activity can be monitored by using the CONLOG.NLM program. This NLM logs console errors and command results to a text file which can be viewed

with a text editor. Command options are available which set log name, location, maximum size and archive options. Look for remote login attempts and other unusual activity in this log such as intruder lockout messages. An example of an intruder lockout message is as follows:

```
8-19-02  10:02:11 am:    DS-6.11-32
     Intruder lock-out on account Lieberher.OAS [279040E1:0002A5974247]
```

The above message would indicate that the account Lieberher has tripped the lockout threshold by entering an incorrect password too many times.

Another message to look for has to do with attempts at Rconsole access. Rconsole is the legacy NetWare remote console utility. This utility should not be used unless absolutely necessary because of its insecure method of authentication. A better option is available in the NetWare Remote Manager which uses SSL authentication. A successful Rconsole attempt would look like this:

```
8-29-02   1:44:07 pm:    RSPX-4.12-28
     Remote console connection granted for 279010E1:080046495014
```

The above message is from a Netware 6 server that had been recently upgraded from Netware 4.11. Old habits are hard to break, but this administrator needs to disable the RCONSOLE utility and move on to using the NetWare Remote Manager.

Install and configure NAAS.
Netware 6 ships with the NAAS (Novell Advanced Auditing System), which is installed by default during the initial install. Configuration and use of this utility is beyond the scope of this document but Novell provides a quick start guide at http://support.novell.com/cgi-bin/search/searchtid.cgi?/10067500.htm and a guide to auditing at http://support.novell.com/cgi-bin/search/tidfinder.cgi?10067501. NAAS is designed to provide auditing for an entire NetWare enterprise.

Install NCP Packet Signature.
According to the Novell product documentation [1], NCP Packet Signature prevents packet forgery by requiring the server and the client to sign each NCP packet with a unique signature. While this feature slows performance, it protects against forged NCP requests, which under the proper conditions, could give an intruder the Supervisor right to the server object. This would allow the intruder unlimited access to the system resources.
There are four levels of packet signature which can be set on both the server and client end. They are:

0 - Do not do packet signature.

1 - Do packet signature only if requested by the other end.
2 - If the other end will allow packet signature, do it.
3 - Require packet signature or don't communicate.

The default setting for both server and client is level 1. If the client side is set to level 0 no packet signature is used. For maximum security against spoofing, set the server to level 3 NCP packet signature. Be aware that this may cause problems with older DOS clients and Windows clients that don't support NCP packet signatures. To set the server side NCP packet signature level, enter the following command at the server console:

```
set ncp packet signature option = 3
```

This will force all NCP packets to be signed.

Do not allow unencrypted passwords.
To support legacy equipment or clients that do not support encrypted passwords, it is possible to configure the server to allow unencrypted passwords. This is a security concern because it allows passwords to be sent over the wire in clear text. To ensure that this setting is off, enter the following command at the server console:

```
set allow unencrypted passwords = OFF
```

If the server has been upgraded, this set command may have carried over in the AUTOEXEC.NCF file from the previous version.

Run, review, save and compare security reports.
The NetWare Remote Manager provides a security report function that can provide the administrator with some "security" information. Although not everything it could be, it is another source of information about some key security elements. To run the NetWare Server Security Report, click Reports / Log Files in the navigation frame in the NetWare Remote Manager, and then click View Security Report on the Reports / Log Files page. The report provides information on the following items [1]:

> *Trustee assignments for the root of each volume* – This information is included because assignments made to the root of the volume grant access to the entire volume unless the rights are specifically revoked with an inherited rights filter or other specific rights assignment at another level.
>
> *Trustee assignments to system folders of the SYS volume* – Users and other objects should have no more than read and file scan rights to Public and Login folders on the SYS volume.

Network Protocol security information - For the IP protocol the report includes the server IP address information, open ports and the corresponding NLM that has the port open. NCP (Netware Core Protocol) information includes protocols bound at the server, addresses and connection information for each active connection to the server. Information about the Common Internet File System (CIFS) consists of the server, workgroup and share name information, authentication source and current sessions.

Admin equivalency list – This is a list of all users that have equivalency to the Admin user. This is similar to obtaining "root" on a Unix system and allows unlimited access to the system.

User list and critical security parameters – Lists users and password requirement settings.

Password Management

As with every system it is critical that a strong password policy is implemented and enforced. NetWare provides some policy settings that help to enforce password policies. The settings provided in NetWare 6 are: password required, password length, password unique, expiration and grace login limit. NetWare also provides intruder detection, which locks the account for a specified time after a specified number of incorrect password attempts. Mark Faust, who wrote the NetWare Security Appnote [4] recommends the following password settings:

1. Enable intruder detection at the OU level.
2. Set incorrect login attempts to 3.
3. Make and use a User Template object to apply password policies to new users.
4. Require users to have passwords with a minimum length.
5. Require users to have unique passwords. Netware remembers the last 8 passwords used.
6. Set grace login to 3.

Additional password considerations are present when NFAP (Native File Access Protocols) is implemented. Early versions of the Novell Netware OS required an additional client (such as the Novell Client32 or the Microsoft Client for Netware) to be installed at the workstations in order to access Netware resources. The Native File Access Protocols product allows Macintosh, Windows and UNIX clients to access Netware server file systems without requiring additional client software. Each client operating system accesses the Netware server via its own "native" protocol. Macintosh clients use the native Apple Filing Protocol (AFP), Windows workstations access the network using the native Common Internet File System (CIFS) protocol, and UNIX based machines use the Network File System (NFS) protocol.

Windows CIFS and MAC AFP cannot use the NDS passwords without the NetWare client so “simple passwords” are stored in the NDS by NMAS (Novell Modular Authentication Services). This additional password adds some complexity to password administration. Both the NDS password and the simple password must be set when creating users. As long as the passwords are synchronized the user is able to change their own password. Administrators can manage passwords either through the ConsoleOne utility or through the NetWare Remote Manager. The NetWare Remote Manager provides the capability to change a single user’s password or populate the simple passwords of multiple users and email the passwords to the users. To access the password management utility in the NetWare Remote Manager, select NFAP Security under the Manage eDirectory option.

More information about NFAP password management can be found at http://www.ncmag.com/2001_11/nativen1/.

Operating System Service Packs

As with every other operating system, service packs and security patches are of extreme importance. As of this writing, Novell has released SP2 for NetWare 6. NW6SP2.EXE can be downloaded from Novell’s support site and should be applied. Novell’s service packs are cumulative and contain all fixes from previous service packs as well. Service packs are installed through the Product Options function of the NWCONFIG program at the server console. Make a point of periodically checking Novell’s minimum patch list for the latest service packs at http://support.novell.com/produpdate/patchlist.html#nw.

Security Patches

Security patches currently available for Novell products can be found at http://support.novell.com/security-alerts. Novell seems to have a policy of only acknowledging a vulnerability when there is a patch for it. It’s a good idea to also keep an eye on other bug tracking sites such as “securitytracker.com”, or subscribe to the BUGTRAQ mailing list. For more information about the BUGTRAQ mailing list see the following web page: http://www.securityfocus.com/popups/forums/bugtraq/faq.shtml#0.1.1.

SNMP Patch

A common vulnerability found in the SNMP protocol also affected Netware 6. Novell has released a patch to fix the problem. SNMPFIX.EXE can be downloaded from http://support.novell.com/servlet/tidfinder/2961546 . This fix is also part of the consolidated support pack NW6SP2.

Netware Remote Manager Patch

The NetWare Remote Manager has a buffer overflow vulnerability that could cause the server to ABEND or possibly allow code to be executed on the server by an attacker. The buffer overflow is caused when an abnormally long name or password is entered into the NetWare Remote Manager login screen. [3]

The NetWare Remote Manager patch can be downloaded from http://support.novell.com/servlet/tidfinder/2962026. This fix is also part of the consolidated support pack NW6SP2.

NetBasic buffer/scripting vulnerability patch

Two vulnerabilities exist in the NetBasic interpreter in NetWare 6. A buffer overflow exists which can cause the server to ABEND when a module name of 230 bytes is submitted. [9] Placing "%5c" in the URL submission can allow access to higher level directories. [9]
A beta patch is now available and is downloadable at http://support.novell.com/servlet/tidfinder/2963297.

Perl Handler patch

Several vulnerabilities exist in the 5.003 version of the Perl Handler. The vulnerabilities include [10]:

1. A remote user could execute code through an HTTP Post command.
2. A remote user can obtain the Perl version information.
3. A remote user could traverse the directory using a "%5c" in the URL.

Novell has released a patch available for download at http://support.novell.com/servlet/tidfinder/2963307.

This patch should only be applied to systems with Perl version 5.003 installed. To check the Perl version, enter the following at the server console:

perl –version

Systems with Perl version 5.6 need not apply this patch.

<u>Traditional File System Security</u>

File system security is an important aspect of the overall network security scheme. Network defense starts with file system security. Netware defaults to allowing only the Admin user full file system rights. Users must be given trustee rights to files or folders through the network administration program as in previous versions of Netware. A good policy is to give users the minimum file system access required. Trustee rights can be assigned to User objects, Group objects, Organizational Role objects, or container objects. Below is the table of available trustee rights and descriptions from the Novell documentation. [4]

Right	Allows you to
Access Control	Add and remove trustees and change rights to directories and files.
Create	Create subdirectories and files.
Erase	Delete directories and files
File Scan	View directory and file names in the file system structure
Modify	Rename directories and files, and change file attributes
Read	Open and read files, and open, read, and execute applications
Supervisor	Grant and exercise all rights listed in this table
Write	Open, write to, and modify a file

Attributes can be assigned to files and directories. Assigned attributes apply to all users (even Admin) and the Modify right is required to change the attributes. These attributes can be used to protect critical files from being deleted or changed accidentally and can provide another level of protection from an attacker. The following page is the table of the available file attributes from the Novell documentation. [4]

Attribute code	Description	Applies to
A	Archive Needed identifies files that have been modified since the last backup. This attribute is assigned automatically.	Files only
Ci	Copy Inhibit prevents Macintosh users from copying a file. This attribute overrides Read and File Scan trustee rights.	Files only
Dc	Do not Compress keeps data from being compressed. This attribute overrides settings for automatic compression of files not accessed within a specified number of days.	Directories and files
Di	Delete Inhibit means that the directory or file cannot be deleted. This attribute overrides the Erase trustee right.	Directories and files
Dm	Do not Migrate prevents directories and files from being migrated from the server's hard disk to another storage medium.	Directories and files
Ds	Do not Suballocate prevents data from being suballocated.	Files only
H	The Hidden attribute hides directories and files so they cannot be listed using the DIR command.	Directories and files
I	Index allows large files to be accessed quickly by indexing files with more than 64 File Allocation Table (FAT) entries. This attribute is set automatically.	Files only
Ic	Immediate Compress sets data to be compressed as soon as a file is closed. If applied to a directory, every file in the directory is compressed as each file is closed.	Directories and files
N	Normal indicates the Read/Write attribute is assigned and the Shareable attribute is not. This is the default attribute assignment for all new files.	Directories and files
P	Purge flags a directory or file to be erased from the system as soon as it is deleted. Purged directories and files cannot be recovered.	Directories and files

Ri	Rename Inhibit prevents the directory or file name from being modified.	Directories and files
Ro	Read Only prevents a file from being modified. This attribute automatically sets Delete Inhibit and Rename Inhibit.	Files only
Rw	Read/Write allows you to write to a file. All files are created with this attribute.	Files only
Sh	Shareable allows more than one user to access the file at the same time. This attribute is usually used with Read Only.	Files only
Sy	The System attribute hides the directory or file so it cannot be seen by using the DIR command. System is normally used with operating system files, such as DOS system files.	Directories and files
T	Transactional allows a file to be tracked and protected by the Transaction Tracking System (TTS).	Files only
X	The Execute Only attribute prevents the file from being copied, modified, or backed up. It does allow renaming. The only way to remove this attribute is to delete the file. Use the attribute for program files such as .EXE or .COM.	Files only

Directory attributes are listed below. [4]

Attribute	Description
Di (Delete Inhibit)	Prevents users from deleting the directory
Dc (Don't Compress)	Files in the directory will not be compressed (if NetWare's file compression feature is activated)
Dm (Don't Migrate)	Files in the directory will not migrate to an offline storage device; used with the data migration option on the volume properties
H (Hidden)	Hides the directory (such as SYS:_NETWARE)
Ic (Immediate Compress)	Every file in the directory will be compressed immediately after being closed (versus waiting the default time of 14 days after the directory was last accessed)
N (Normal)	Default attribute - allows Read and Write to files, but not Shareable
P (Purge)	Flags a directory to be purged as soon as it is deleted, rendering it unrecoverable
Ri (Rename Inhibit)	Prevents users from renaming the directory
Sy (System)	Used to flag a system directory such as SYS:_NETWARE

iFolder

New in NetWare 6, iFolder is a file synchronization mechanism that keeps data on a local machine in sync with the personal iFolder on the server. The iFolder utility can be installed on multiple machines, keeping the data in sync on the local drives and the iFolder server. The personal iFolder can also be accessed via a java enabled web browser over the internet. After successfully logging in to the iFolder site, the java applet is installed to the browser. The contents of the personal iFolder directories are encrypted, eliminating the need for a VPN connection. Both the iFolder utility on the local workstations and the java applet contain the required cryptographic functions necessary to decrypt and re-encrypt the iFolder data.

Two encryption security options are available when implementing iFolder: Unencrypted or Encrypted with pass phrase. If you choose to allow unencrypted iFolders to be created, data in the unencrypted iFolders is not encrypted and does not travel over the network encrypted. This would raise some obvious security concerns. Selecting the Encrypted with pass phrase option causes the contents of the iFolder directories to be encrypted and to travel encrypted. A pass phrase is used to encrypt and decrypt the contents.

The encryption method used by iFolder is called Blowfish. NetWare uses 128-bit encryption keys for iFolder. When an encrypted folder is created the user is prompted for a pass phrase which is used to create the 128-bit key to encrypt and decrypt the contents of the folder.

If the iFolder server is to be accessible from the Internet, it is best to place it behind a firewall opening up ports 80 (HTTP) and 443 (HTTPS). [5]

iPrint

The iPrint product in NetWare 6 is designed to allow printer access from “anywhere”, using the SSL authentication and the IPP protocol. The primary security item here is to be sure to enable secure printing (with SSL) and select the desired printer security level for each printer. The following table from the iPrint documentation shows the affect of the available security levels. [6]

Printer Security Level	Secure Printing Disabled (No SSL)	Secure Printing Enabled (With SSL)
Low	Full access	eDirectory authentication
Medium (Default)	Users granted access as if they had been assigned the User role.	eDirectory authentication and check user's effective rights
High	Users must use SSL and authenticate to eDirectory Users might receive an error if SSL is not enabled.	eDirectory authentication, check user's effective roles, and connection verification SSL is automatically enabled when a printer's security is changed to High when using Novell iManager.

A note about SSL Security

Novell Netware 6 uses SSL authentication for it’s browser-based management utilities, iPrint and iFolder access. Novell’s implementation of SSL utilizes Nile and Winsock [8] so it is not affected by the Apache SSL vulnerability that is referred to in CERT warning CA-2002-27 [7].

Summary

This document has touched on some general and specific measures for securing NetWare 6 servers. Defense in depth is an important concept when working on NetWare security. Every security point from the user password to the placement of the server in the network infrastructure either enhances or reduces the overall security. Even after applying all the latest patches and configuring the server to be as secure as possible, the job of securing the server is not over. Security is a continuous process of evaluating needs and exposure, careful monitoring, vigilant vulnerability assessment and activity awareness.

Bibliography

1. Novell. “Netware 6 Server Operating System Administration Guide - Managing the NetWare Server – Using NCP Packet Signature.” Feb.2002. URL:http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/sos__enu/data/hc66y4qi.html (Oct. 9, 2002).

2. Novell. “NetWare 6 Server Operating System Administration Guide – Managing the NetWare Server – Tracking Potential Security Risks.” Feb. 2002. URL:http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/sos__enu/data/hpmfqfmr.html (Oct. 9, 2002).

3. SWD Staff. “Remote Manager 6 Patch Expected From Novell.” Security Wire Digest – Vol. 4, No.27. April 8, 2002. URL:http://www.infosecuritymag.com/2002/apr/digest08.shtml#news2 (Oct. 10, 2002)

4. Faust, Mark. “NetWare Security: Closing Doors to Hackers.” June 7, 2000. URL:http://developer.novell.com/research/appnotes/2000/june/03/apv.htm (Oct. 12, 2002).

5. Burnett, Kevin. “iFolder: Data Accessibility Where and When You Need It.” Oct. 2001. URL:http://developer.novell.com/research/appnotes/2001/october/03/a011003.pdf (Oct. 13, 2002).

6. Novell. “NetWare 6 iPrint Administration Guide – Secure Printing Using SSL.” Feb. 2002. URL:http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/iprntenu/data/aaxguq6.html (Oct. 13, 2002).

7. Cert. “Cert Advisory CA-2002-27 Apache/mod_ssl Worm.” Oct. 11, 2002. URL: http://www.cert.org/advisories/CA-2002-27.html (Oct. 15, 2002).

8. Novell. “Technical Information Document 10074700. How Does Novell Implement SSL?.” Sep. 20, 2002. URL:http://support.novell.com/cgi-bin/search/searchtid.cgi?/10074700.htm (Oct. 15, 2002).

9. Novell. “Technical Information Document 2963297. NetBasic buffer/scripting vulnerability patch.” Aug. 16, 2002. URL: http://support.novell.com/servlet/tidfinder/2963297 (Nov. 2, 2002).

10. Unknown. “Novell NetWare Perl Handler Input Validation Bugs” Aug. 21, 2002. URL:http://www.securitytracker.com/alerts/2002/Aug/1005091.html (Nov. 5,2002).