Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Security Best Practice - Novell NetWare 6.5 Remote Management Utilities

It's not always what you know, it's who you know. Whether it is a good deal on a product, a free place to stay on a vacation or the extra edge to beat out competition for a job, knowing the right people helps people get the things they want. This 'knowing the right people' is a form of social engineering. Social engineering is using relationships with people to attain a goal. Unfortunately, when it comes to the security of an organization's data and infrastructure, social engineering can be as bad as 'knowing the right...

Copyright SANS Institute
Author Retains Full Rights

AD

Security Best Practice - Novell NetWare 6.5 Remote Management Utilities

Adam Schieman, CNA, CCNA

© SANS Institute 2004, Author retains full rights.

February 2, 2004
GIAC Security Essential Certification (GSEC) Practical Assignment
Version 1.4b
Option 1

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

Table of Contents 2
Abstract 3
General OS Security Issues Related to Remote Management Utilities 4
The “New” Knowledgebase of a NetWare Administrator 4
Firewalls 4
Installation and Patches 5
Physical Access 6
Secure Console 6
Server Console Screen Saver 7
Users and Passwords 7
Remote Console (RConsoleJ) 8
End-User Welcome Web 10
Administrator Welcome Web Site (NetWare Web Manager) 10
NetWare Remote Manager (NRM) 11
HTTP Log 13
HTTPSTK IP Address and Port Setup 13
IP Address Access Control 13
iMonitor 14
OpenSSH 15
iManager 17
Apache HTTP Server and Tomcat Servlet Container 19
List of References 20

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Abstract

Novell has been developing remote management utilities since early versions of NetWare. Many of the current utilities for operating system and product administration are web-based. According to Novell, iManager, which is built on Apache Web server and Apache Tomcat Servlet Container, will become the management utility for eDirectory and many of the products developed for NetWare. With the move from client/server based administrative utilities, such as NetWare Admin and ConsoleOne, to web-based and other remote utilities, Novell administrators must broaden their knowledgebase to identify and limit security risks.

The purpose of this paper is to investigate the remote management utilities available in NetWare 6.5 and identify ways to limit security risks. Although some general NetWare security issues will be addressed, the paper will focus on the utilities Remote Console (RConsoleJ), NetWare Remote Manager, iManager, iMonitor and OpenSSH.

Note: The content of this paper is based on a Management Server pattern installation from the NetWare 6.5 SP 1.1 OS and products overlay CD.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

General OS Security Issues Related to Remote Management Utilities

The "New" Knowledgebase of a NetWare Administrator

NetWare administrators can no longer limit their technical and security knowledge to NetWare. Novell's recent embrace of open-source software creates a need for administrators to broaden their knowledgebase to include Apache HTTP server, Apache Tomcat servlet container, OpenSSL and OpenSSH. Security risks discovered in one of the open-source products will most likely affect the version compiled to run on NetWare. For example, eDirectory prior to version 8.7.3 on all platforms is affected by the SSL/TLS ASN.1 decoder vulnerabililities found in OpenSSL.[2]

Here are some recommendations to keep updated on NetWare security issues:

- look for product updates that are security related at http://support.novell.com/filefinder/security/index.html
- watch for security related product updates indicated by a caution symbol on the NetWare 6.5 product update page at http://support.novell.com/filefinder/18197/index.html
- subscribe to the novell.support.security-alerts news group on the support-forums.novell.com news server
- watch for security advisories at http://www.cert.org or subscribe to the CERT Advisory Mailing List at http://www.cert.org/contact_cert/certmaillist.html
- sign up for one or more Computer Security Newsletters and Digests at http://www.sans.org/newsletters

Firewalls

The move to web-based management utilities requires careful planning to allow access to the utilities from inside and outside of an internal network, while maintaining secure NetWare servers. NetWare servers that are providing file and print functions should not be accessible from outside of an internal network. In order to access NetWare Remote Manager, iMonitor and other utilities from the Internet, administrators should be required to access the internal network through VPN with minimum access needed to use the utilities. For example, by default, the HTTP server used by NetWare Remote Manager and iMonitor listens on TCP ports 8008 and 8009. A VPN would only need to allow access to these 2 ports for an administrator to use the utilities (table 1).

[2] "Regarding NISCC vulnerability advisory on SSL (secure sockets layer) and TLS - TID10087450."

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Table 1. Ports used by NetWare 6.5 Administrative Utilities

Administrative Utilities	Application	Port
administrator Welcome web site, OpenSSH Manager	Apache (Admin instance)	2200, 2211
end-user Welcome web site, iManager	Apache	80, 443
NetWare Remote Manager, iMonitor	HTTPSTK	81, 8008, 8009
authentication for various utilities	LDAP	636

Installation and Patches

The NetWare installation process allows a lot of flexibility in what products are installed. Administrators should only install the products necessary for the server to fulfill its defined role. One of the new features of NetWare 6.5 is the addition of Pattern installations, which may be chosen to install the products based on a specific role. Choose a Customized NetWare Server to install any combination of products.

If you are installing the first server in an eDirectory tree, you will be prompted to set up an Admin user object for the tree. Choose a username other than “admin” to limit the risk of a password attack on this well-known username. Create an organization unit (OU) in the organization (O) container to hold just administrative level accounts and specify the new OU as the context for the Admin object. Maintaining a separate OU for normal user objects and administrative user objects allows for stronger account policies to be applied to all administrative users.

If a Manual Installation was chosen at the beginning of the NetWare 6.5 install process, you will be able to specify the LDAP port and encryption settings for the server. Many of the web-based utilities in NetWare 6.5 use LDAP for authentication. Checking the box “Require TLS for Simple Bind with Password” on the LDAP Configuration page will configure the server to accept only LDAP simple binds with a password over a secure connection. Although the bind will be rejected using this setting, the username and password can still be captured during a failed bind attempt using an unsecured connection. To prevent the capture of a username and password during an unsecured bind, use ConsoleOne or iManager to select the “Require TLS For All Operations” option in the LDAP Server object properties page.

The most current service pack should be installed after installing a NetWare server. Novell releases overlay CDs for both the operating system and products that already contain patched files from a service pack. All new installations of servers or products should be done from an overlay CD to ensure the most current service pack fixes are installed. Novell maintains a list of minimum recommended patches for many products at http://support.novell.com/produpdate/patchlist.html. Additional patches are listed on the Product Update page for each individual product. The Novell support pages

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

(http://support.novell.com) are a good starting point for finding product patches and support.

Physical Access

All servers, whether running NetWare or other operating systems, should be physically secure and only accessible to the appropriate personnel. Regardless of the steps taken to secure an operating system, if the machine is stolen, it is only a matter of time before the data on the server is compromised. Servers should be located in an access-controlled room with proper electrical (UPS) and environmental safeguards. Battery or generator backup systems should be in place to ensure data and applications are accessible.

By default, the NetWare operating system is accessible through the console screens without authentication if physical access to the server is achieved. Access to the server console could allow the steps taken to secure the remote management utilities to be reversed. For this reason, SECURE CONSOLE and SCRSAVER should be used to limit access to the server console.

Secure Console

Issuing the SECURE CONSOLE command at the server provides the following security features:

- Prevents NetWare Loadable Module programs from being loaded from any directory other than sys:system or c:\nwserver. This will prohibit an invasive NLM from being loaded from a server's disk drive or boot partition, unless it is already in a search path.

- Prevents keyboard entry into the operating system debugger. This restricts the ability to alter the operating system.

- Prevents anyone from changing the date and time. Some security and accounting features depend on date and time for their enforcement.[4]

These security features affect the server console and remote console sessions initiated through Remote Console (RconsoleJ), NetWare Remote Manager and OpenSSH. Once the SECURE CONSOLE command is issued, the server must be shut down and re-booted to disable SECURE CONSOLE. The SECURE CONSOLE command should be placed in the AUTOEXEC.NCF so that it is loaded each time the server is restarted. Please see SECURE CONSOLE in the NetWare 6.5 Utilities Reference for more information.

[4] "SECURE CONSOLE."

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Server Console Screen Saver

The SCRSAVER utility allows the server console to be secured by requiring eDirectory authentication in order to access the console prompt. Normally the utility displays a screensaver on the server console. When any key is pressed SCRSAVER prompts the console operator for a username and password. Authentication is also required when accessing the console prompt through remote console sessions that have been initiated by Remote Console (RconsoleJ), NetWare Remote Manager or OpenSSH. The user object associated with the supplied username must have write access to the server object access control list (ACL) in eDirectory to access the console prompt. The delay before the screen saver is activated, along with other options, can be configured when loading SCRSAVER from the console prompt. Please see SCRSAVER in the NetWare 6.5 Utilities Reference for more information.

Users and Passwords

NetWare Remote Manager, iMonitor and OpenSSH all require supervisor rights to the server object in eDirectory. Administrators should use separate user accounts for normal and administrative duties, such as managing a server through NetWare Remote Manager. Intruder detection should be enabled on all organizational units containing user objects to protect against password hacking attempts. Organizational units containing users with supervisor-level rights should have more restrictive intruder detection settings such as the following:

- Enable intruder detection
- Set incorrect login attempts to 3
- Set intruder attempt reset to 12 hours
- Enable lock account after detection
- Set detection period to 15 minutes

Intruder detection settings do apply to accounts when authenticating to web-based management utilities.

A strict password policy requiring long passwords should be applied to organizational units containing user objects with supervisor-level rights:

- Set Minimum Password Length to 20 or greater. User objects in eDirectory can have passwords up to 128 characters in length.
- Require Unique Passwords. This setting disallows the reuse of the last 8 passwords.
- Force periodic password changes every 90 days.

By default, eDirectory passwords have some limitations that affect security:

- Passwords are not case sensitive
- Password complexity cannot be enforced

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

In NetWare 6.5, administrators have the option to enable the Universal Password that supports case sensitive passwords and passwords containing extended characters. Nsure Identity Manager 2.0 (http://www.novell.com/products/nsureidentitymanager) can be purchased separately to allow definition of password policies through iManager 2.0 that enforce password complexity.

Remote Console (RConsoleJ)

Remote console has been used since early versions of NetWare, but has been abandoned by many administrators since older versions sent all communication in clear text, including the remote console password. Starting in NetWare 6, remote console has supported the use of SSL to secure communications.

The Novell remote console utility allows administrators to execute server console commands from a workstation using IP or IPX. All console screens on the server are accessible, except the server GUI screen. The utility consists of a remote console client that runs on a workstation and a remote console agent that runs on the NetWare server. A proxy agent is also available to allow communication with a server that only supports IPX.

The functionality of remote console has been improved in NetWare Remote Manager and OpenSSH in NetWare 6.5. Remote console use should be phased out due to difficulty of password maintenance, lack of connection logging and absence of eDirectory authentication. At a minimum, remote console connections should be limited to the private network. NetWare administrators who are continuing to support remote console should follow the recommendations below to ensure server integrity through the secure use of remote console. If you are uncertain that remote console is being used on a server, search for the following NLMs using the MODULES RC* command:

> RCONAG6.NLM - remote console agent running on a NetWare server that listens for incoming remote console client requests.
>
> RCONPRXY.NLM - remote console proxy agent running on a NetWare server that listens for incoming remote console client requests and forwards them to the appropriate NetWare server running IPX.

The remote console password and listening ports are set up when the remote console agent is loaded on a NetWare server. Remote console should be configured to use TCP, encrypted with SSL, with the password encrypted during initial set up. The remote console agent should not be configured to use IPX since the communication cannot be encrypted with SSL. Follow these steps to set up remote console:

1. Comment out any line in the AUTOEXEC.NCF file referencing RCONAG6.NLM

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

2. At the console prompt, enter RCONAG6.NLM ENCRYPT

3. Choose the IP address that RCONAG6.NLM should use if multiple IP addresses are bound on the server.

4. Enter a strong password that administrators will use when accessing a NetWare server with remote console client software.

5. Enter the TCP port number (default 2034) to use for unsecured communications.

6. Enter the TCP port number (default 2036) to use for secured communications. The Key Material Object named SSL CertificateDNS must exist to use remote console over secure TCP.

7. Enter the -1 when prompted for the SPX port to disable listening for SPX connections. The set up utility will choose 65535 as the SPX port number.

Steps 1-7 will create a script file SYS:SYSTEM\LDRCONAG.NCF which contains the following line:

LOAD RCONAG6.NLM <encrypted password string> 2034 65535 2036

8. Add LDRCONAG.NCF to the AUTOEXEC.NCF file to start the remote console agent when the server loads.

Administrators should note the date when the LDRCONAG.NCF file was created. The modification date on LDRCONAG.NCF file should be audited regularly to ensure that it has not been modified in between password changes.

The remote console client included with NetWare, RConsoleJ, is Java-based and can be run from any Java-enabled workstation or from the server GUI. Unfortunately, even when the remote console agent is set up on the server using the above steps, a remote console client can initiate a non-SSL TCP session. Administrators must choose secure IP in the connection options of RconsoleJ or the password and all commands will be sent in clear text.

There are no dedicated logs generated on the server by the remote console utility. The remote console agent does log connections from a remote console client to the Logger Screen. The following text is a sample remote console entry from the Logger Screen:

Wed Jan 21 15:28:16 2004
RCONAG6 192.168.1.1:1593 Remote console connection granted.

Wed Jan 21 15:32:17 2004
RCONAG6 192.168.1.1:1593 Remote console connection cleared.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

End-User Welcome Web

The NetWare 6.5 Welcome Web site is a collection of web pages containing information for end-users about the products available in NetWare 6.5. The site can be accessed through the following URLs:

http://<server IP address>
or
http://<server DNS name>

The end-user Welcome Web site is hosted from an instance of Apache web server that is loaded from the AUTOEXEC.NCF file by executing the AP2WEBUP.NCF file. This file loads an instance of Apache for Netware using the standard configuration file SYS:APACHE2\CONF\HTTPD.CONF which includes a specific configuration file for the Welcome Web site from SYS:ADMINSRV\WEBAPPS\WELCOME\WEB-INF\WELCOME-APACHE.CONF. Apache is configured to listen on port 80 for normal access and port 443 for secure access using SSL.

The end-user Welcome Web site only serves the purpose of introducing the features of NetWare 6.5. Since it displays information that identifies the server platform and potential web-based services that may be hosted on the server, it should be disabled. This instance of Apache may also be needed to host a production website. The Welcome web site can be disabled by commenting out the following line in the SYS:APACHE2\CONF\HTTPD.CONF file:

Include “SYS:/adminsrv/webapps/welcome/web-inf/welcome-apache.conf”

The SYS:APACHE2\HTDOCS\INDEX.HTML file should then be changed to discontinue redirection to the Welcome Web site, which will produce an error message.

Administrator Welcome Web Site (NetWare Web Manager)

The administrator Welcome web site, also called NetWare Web Manager, provides authenticated access to web-based administration utilities and configuration settings for the site. The administrator site can also be accessed through the following URLs:

https://<server IP address>:2200
or
https://<server DNS name>:2200

The administrator Welcome Web site is hosted from an instance of Apache web server started from the AUTOEXEC.NCF file by executing the ADMSRVUP.NCF file. This file loads Apache for Netware in the ADMINSRV address space using the configuration file SYS:ADMINSRV\CONF\ADMINSERV.CONF. This instance of Apache is configured to listen on port 2211 for normal access and port 2200 for secure access using SSL. Since

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

there are no services dependent on non-secure access through port 2211, it can be safely closed by commenting out the following line in the ADMINSERV.CONF file:

```
LISTEN 192.168.1.1:2211
```

The administrative instance of Apache will need to be reloaded for any changes to ADMINSERV.CONF to take effect. Issue the following commands at the console prompt to unload and then load Apache:

```
ADMSRVDN
ADMSRVUP
```

Once authenticated, an administrator can access web-based management tools for the server depending on which products are installed. The site contains an Admin Preferences page that allows configuration of the Web Manager port (default 2200), indicates whether encryption is required (default On) and shows the server certificate used for secure communications. Error and access logs can be viewed and searched through this page. The access and error logs are stored in SYS:ADMINSRV\LOGS in the ACCESS.TXT file and ERROR.TXT file respectively. By default, the ADMINSRV instance of Apache is not set up to rotate the log files. A routine should be configured to rotate these log files on a regular basis to maintain a history of access to the web site. More information about Apache log files and log rotation can be found in the Apache 2.0 documentation pages at http://httpd.apache.org/docs-2.0.

NetWare Remote Manager (NRM)

NetWare Remote Manager is a secure web-based utility that provides most of functionality of MONITOR as well as some functionality of other server console-based utilities. NRM provides the ability to monitor server health and change the server configuration as well as performing diagnostic, debugging and reporting tasks. NRM contains a web- based remote console utility similar to RconsoleJ that requires no additional configuration and also provides access to the server GUI screen.

NetWare Remote Manager requires PORTAL.NLM and HTTPSTK.NLM, which are installed by default in all NetWare installations. HTTPSTK.NLM is a custom HTTP server created by Novell for NetWare Remote Manager and iMonitor. PORTAL.NLM and HTTPSTK.NLM can be configured through the NetWare Remote Manager Configuration Options page. NRM is loaded from the AUTOEXEC.NCF file when the server is started using the following lines:

```
LOAD HTTPSTK.NLM /SSL /KEYFILE:"SSL CertificateIP"
LOAD PORTAL.NLM
```

Once started, NetWare Remote Manager can be accessed a number of different ways:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

1. https://<server IP address or server DNS address>:8009

2. http://<server IP address or server DNS address>:8008 (Note: This option always forwards your web browser to the web address in option 1 to enable secure access to NRM.)

3. Click on the NetWare Remote Manager link after logging into the administrator Welcome web site.

A login dialog box will appear prompting for a username and password. Accessing the management functions of NRM requires authentication using a user object with Supervisor rights to the server object. NRM will attempt to authenticate the user object using eDirectory context in the SET BINDERY CONTEXT line in the AUTOEXEC.NCF file or the default eDirectory context specified in NRM Configuration Options page. A user without Supervisor rights to the server can obtain access to NRM, but only file access and Simple Password management functions will be available.

A disclaimer page can be set up to appear before logging into NRM by modifying the SYS:LOGIN\PRTLTXT.HTM file and renaming it SYS:LOGIN\PRTLDISC.HTM. The disclaimer page should specify that the system is for authorized uses only and that all people accessing the system may be monitored and any data collected may be shared with law enforcement officials.[12]

Clicking on the Configure icon in the header frame will access the NRM Configuration Options page. The icon is only available by authenticating with a user object that has Supervisor rights to the server object being managed.

Emergency (SAdmin) Account and Debug (SDebug) Account

The SAdmin and SDebug accounts are special bindery-based accounts that can only be managed through NetWare Remote Manager. The SAdmin account allows an administrator to login to NRM if eDirectory is unavailable. It has the same access rights as the eDirectory Admin user. The SDebug account can be used by IS staff to troubleshoot server problems without having Supervisor rights to the server object. It has the same rights as SAdmin but cannot perform the following functions:

1. Partition disk operations
2. Access the server console (does have access to the console logs)
3. Schedule tasks
4. Load new modules
5. Access eDirectory through the tree walker to create users, groups, or assign trustees.
6. Change the password for the SDebug account [13]

[12] Cole, Fossen, Northcutt, Pomeranz, p.1523.
[13] "NetWare 6.5 NetWare Remote Manager Administration Guide."

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The passwords used for each account has different properties than an eDirectory password:

1. they are case-sensitive
2. they can have maximum of 80 characters

Intrusion detection policies cannot be applied to the SAdmin or SDebug accounts because they do not exist in eDirectory. Each account should be configured with a strong password that is changed regularly to limit the risk of a password attack.

HTTP Log

The log for HTTPSTK.NLM is located in the SYS:\HTTPLOG.TXT. "The log file contains the following information: an entry number; the date and time stamp in Greenwich Mean Time (GMT); host name; the program making the call; the level of the call (whether it's done by the server or by users); and a description of the entry itself with information including IP address of the source machine making the request, messages, status, etc."[13]

The HTTPSTK log can be configured to clear the log when it reaches a specific size. The default setting is 8 megabytes. In order to keep an archive of old log files, logging must be disabled in order to close the file before it can be copied to a new location.

HTTPSTK IP Address and Port Setup

In NetWare 6.5, the IP address and port used by HTTPSTK can be configured through NRM. Regardless of the requested configuration, HTTPSTK must be bound to one IP address/port combination that is configured for secure access with SSL. If all SSL enabled IP Address/Port combinations are deleted or only non-SSL enabled combinations exist, a new binding will be generated when HTTPSTK is restarted. The auto-generated binding will use the primary IP address of the server and port 8009 configured with SSL enabled.

On a basic file and print server, with two network cards, HTTPSTK could be bound to one network card that is attached to a private network only accessible to administrators. This configuration would provide a secure setup for using NRM and iMonitor, through HTTPSTK, behind a firewall.

IP Address Access Control

If NRM or iMonitor are being used on a public network, access should be restricted by IP address or subnet. Access to HTTPSTK can be restricted to 8 IP addresses or 8 IP address ranges specified with a combination of subnet and subnet mask. The HTTPSTK must be re-started for new IP address restrictions to take affect.

[13] "NetWare 6.5 NetWare Remote Manager Administration Guide."

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

iMonitor

Novell iMonitor is a secure web-based tool for monitoring and diagnosing the eDirectory agents running on all servers in an eDirectory tree. The utility functions as an alternative or replacement for many of the server console based eDirectory utilities such as DSBrowse, DSTrace, DSDiag and DSRepair.

iMonitor requires NDSIMON.NLM and HTTPSTK.NLM, which are installed by default in all NetWare installations. HTTPSTK.NLM is the same HTTP server used by NetWare Remote Manager. Any changes to the HTTP server made through the Configuration Options page in NRM also affect the operation of iMonitor. iMonitor is loaded from the AUTOEXEC.NCF file when the server is started using the following line:

LOAD NDSIMON.NLM

Once started, NetWare iMonitor can be accessed a number of different ways:

1. https://<server IP address or server DNS address>:8009/nds

2. http://<server IP address or server DNS address>:8008/nds (Note: This option always forwards your web browser to the web address in option 1 to enable secure access to iMonitor.)

3. Click on the NDS iMonitor Link under the Manage eDirectory section in the Navigation frame of NRM.

The iMonitor configuration file (SYS:SYSTEM\NDSIMON.INI) contains a LockMask setting (table 2) that allows the administrator to control the level of eDirectory authentication required for iMonitor to process URL requests. This setting provides some control over who could launch a DoS attack against the iMonitor utility using malformed URLs.

Table 2. iMonitor LockMask Levels[14]

LockMask Level	Description
0	iMonitor will process requests without authentication. The eDirectory rights of the Public identity are applied to all requests.
1	iMonitor will only process requests after a user has successfully authenticated to eDirectory. The eDirectory rights of the authenticated user are applied to all requests. This is the default setting.
2	iMonitor will only process requests after a user has successfully authenticated to eDirectory with supervisor rights to the server object. The eDirectory rights of the authenticated user are applied to all requests.

[14] "Using Novell iMonitor 2.1."

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Level 0 provides no protection against DoS because iMonitor will attempt to process all requests. Level 1 and 2 provide some level of protection because authentication is required before iMonitor processes a request. However, someone who has authenticated to the server could launch a DoS attack. LockMask level 2 would only allow users with supervisor access to the server to launch an attack. Assuming only the appropriate people have supervisor rights, this level of security would virtually eliminate this risk.

The LockMask setting does not override the eDirectory rights required to run processes through iMonitor.

There are no audit logs specifically generated by the iMonitor utility. Similar to NRM, the logs generated by HTTPSTK.NLM show authentication attempts to iMonitor.

OpenSSH

NetWare 6.5 includes OpenSSH version 3.6sp1 as an optional product that can be installed on a server. "OpenSSH encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks. Additionally, OpenSSH provides a myriad of secure tunneling capabilities, as well as a variety of authentication methods."[16] The OpenSSH package on NetWare includes most of the standard SSH utilities ported to NLMs as well as:

- OpenSSH Manager - a web-based utility to manage SSH on NetWare by providing a simple interface to modify the SSHD_CONFIG file.
- SSH Log Daemon - generates log files from NetWare SSH utilities
- LDAP Authentication - SSH on NetWare uses password authentication through LDAP

OpenSSH Manager runs from the same instance of Apache that hosts the administrator Welcome web site. OpenSSH Manager can be disabled by commenting out the following line in the SYS:ADMINSRV\CONF\ADMINSERV.CONF file:

Include "SYS:/adminsrv/webapps/sshdadmin/web-inf/sshadmin.conf"

The utility allows administrators who are members of the sshdadmn-Administrators group to configure SSH on NetWare and monitor SSH connections. The configuration can also be changed by modifying the SYS:ETC\SSH\SSHD_CONFIG file directly. OpenSSH Manager can be accessed through:

1. https://<server IP or DNS address>:2200/sshdadmin/index.html

[16] OpenSSH.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

2. From the OpenSSH page in the administrator Welcome web site

Ensure the Use SSL option is checked when logging into OpenSSH Manager to enable secure LDAP communication when authenticating to eDirectory.

In OpenSSH Manager, the eDirectory page allows administrators to add eDirectory search contexts that will be used to find user objects that can authenticate through SSH. Access to a server with SSH can be restricted by limiting the search contexts. Clicking on the Server Logs icon enables administrators to view SSH logs and change log preferences. SSHLOGD.NLM generates access and error logs from all SSH utilities. The Log Preferences page can be used to configure:

- the log file path (default: sys:/etc/ssh/logs)
- log level (default: INFO)
- maximum file size (default: 4M)
- maximum files (default: 7)
- rotation interval (default: 24 hours)

SSHLOGD.NLM will rotate the SSH log file when the maximum file size is reached, or at the rotation interval. The archived log file will be named SSHD<file number>.LOG, where <file number> is between 1 and the maximum files setting. The current log file is named SSHD.LOG. The default settings provide a good history of SSH activity in case a security incident occurs. The maximum files setting could be increased, or files could be archived in a different directory to maintain a longer history.

After authenticating to a server, a user's current working directory will be their home directory. If a home directory is not set up for a user object in eDirectory, the current working directory will be set up as the root of the server volumes. File rights that have been assigned to a user through eDirectory apply to SSH sessions. Users with supervisor rights to a server object will have access to the server console through the SSH terminal.

The default SSHD_CONFIG file should be modified to disable listening for SSH version 1 and to include a banner that will be displayed when a connection is established:

1. Change the Protocol directive from "Protocol 2,1" to "Protocol 2"

2. Add the line "Banner sys:/etc/ssh/banner.txt" which references a file with a warning message similar to the one suggested for NRM.

3. Restart SYS:SYSTEM\SSHD.NLM to reload SSH with the new configuration file settings.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

iManager

iManager is a secure, web-based utility that provides:

- All the functionality of its predecessor, ConsoleOne
- Single point of administration for Novell eDirectory objects, schema, partitions and replicas
- Single point of administration for many other network resources
- Management of many other Novell products through a Web browser and various handheld devices
- Role-Based Services (RBS) for delegated administration [19]

iManager is built on a portal interface provided by Novell exteNd Director Standard Edition software that runs on the Apache Tomcat servlet container. More information about exteNd Director and building portal interfaces can be found on the exteNd Director Standard Edition documentation web site:

http://www.novell.com/documentation/lg/nedse41/index.html

iManger can be accessed through:

1. http://<server IP address or server DNS address>/nps/iManager Note: This option always forwards your web browser to the iManager login page using HTTPS.

2. From the iManager page in the administrator Welcome web site

The iManager utility is hosted from an instance of Apache web server that is loaded from the AUTOEXEC.NCF file by executing the AP2WEBUP.NCF file. This file loads an instance of Apache for Netware using the standard configuration file SYS:APACHE2\CONF\HTTPD.CONF which includes a specific configuration file for iManager from SYS:/TOMCAT/4/CONF/NPS-APACHE.CONF. Apache is configured to listen on port 80 for normal access, and port 443 for secure access using SSL.

iManager should be hosted on a single-purpose server that is located behind a firewall and should only be accessible from the Internet through VPN. Apache should be configured to only listen on port 443 using SSL by commenting out the following line in the HTTPD.CONF file:

LISTEN 192.168.1.1:80

Apache will need to be reloaded for any changes to HTTPD.CONF to take effect. Issue the following command at the console prompt to restart Apache:

[19] Novell iManager 2.0.x Documentation.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

AP2WEBRS

iManager allows administrators to delegate administrative tasks to users through a series of roles and tasks. This feature is known as Role Based Services (RBS). When a user authenticates to iManager, they will only see their assigned roles and tasks and only have the eDirectory rights to accomplish them. For example, a help desk employee can be assigned the Helpdesk Role that gives them access to the necessary tasks in iManager and rights in eDirectory to clear an account lockout, create a user and set a user password. In addition, the scope of a role for a user can be limited to a specific part of eDirectory. In an organization with separate organizational units (OU) for part-time and full-time employee groups, the Helpdesk role could be assigned to a help desk employee with the scope limited to the OU containing the part-time employees.

RBS is not installed by default. A user with administrator level rights to the eDirectory tree must create a RBS collection object through the iManager Configuration Wizard. The user object used to install RBS automatically becomes the collection owner. Collection owners are able to delegate roles and tasks through the iManager Role Configuration page. Additional owners can be assigned through iManager.

Administrators must be aware of how eDirectory rights are assigned when using RBS. A user who is assigned the User role requires create and delete rights to an eDirectory OU to complete the Create User and Delete User tasks of the role. If the role is assigned with a scope of an OU containing user and printer objects, the user has been assigned delete rights to the entire container – including the printer objects. The user view in iManager will not contain a task to delete printer objects, but ConsoleOne could be used to perform this task. Here are a few ways to limit this risk:

1. Create separate containers for like objects in eDirectory - one OU for users, one OU for printers etc. Roles and tasks can be scoped to include only the OU with the required objects. For example, a help desk employee who is assigned the Users role with a scope over the users OU will not be assigned the eDirectory rights to delete a printer in the printers OU.

2. When delegating a role through iManager, clear the Assign Rights checkbox option. This option will disable the automatic assignment of eDirectory rights to perform the assigned role. The administrator will need to manually assign the rights needed to perform the assigned roles and tasks through user or group objects.

Auditing eDirectory changes becomes more important as administrative tasks are delegated to a larger number of users with varying levels of rights. An auditing tool such as NSure Audit (http://www.novell.com/products/nsureaudit) should be implemented when utilizing RBS.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Apache HTTP Server and Tomcat Servlet Container

Apache HTTP server and Tomcat Servlet Container are not remote utilities themselves, but provide the platform for many web-based utilities in NetWare 6.5. This section provides a brief overview of the interaction between Apache and Tomcat.

Both instances of Apache, normal and administrative, have a corresponding instance of Tomcat to process servlets and JavaServer Pages (JSP). The normal and administrative instances of Tomcat are started from the AUTOEXEC.NCF using the TOMCAT4.NCF and TC4ADMUP commands, respectively.

A servlet is a small program written in Java that runs on Tomcat. A JavaServer page (JSP) contains XML tags and scriplets written in Java that generate HTML or XML content that can be displayed by a web server.

Apache uses the mod_jk plug-in module to communicate with Tomcat using the AJP 13 protocol. The Apache configuration files, HTTPD.CONF and ADMINSERV.CONF, contain JKMount statements that create connections between Apache and Tomcat through the mod_jk module. The mod_jk connection parameters for both instances of Apache/Tomcat are located in the SYS:/ADMINSRVCONF/MOD_JK/WORKERS.PROPERTIES file.

Here is the flow of a typical request processed by Apache using Tomcat:

1. A request is received by Apache from a client web browser
2. Apache identifies that Tomcat is needed to process the request since it requires a JSP page
3. Apache passes the request, through the mod_jk module to Tomcat for processing
4. Tomcat processes the JSP page and returns a response page in HTML or XML to Apache through the same connection
5. Apache returns the response to the client web browser

NetWare administrators should increase their knowledge of Apache and Tomcat to identify the security risks of the remote utilities on their NetWare 6.5 servers. More information about Apache HTTP Server and Tomcat Servlet Container can be found on the following web sites:

- http://httpd.apache.org/
- http://jakarta.apache.org/tomcat/index.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

List of References

1. Lunardi, Guy. “From the Inside Out: Moving Toward a Single Management Console.” 13 Jan. 2004. URL: http://www.novell.com/coolsolutions/nds/features/a_insideout_imanager_edir.html (14 Jan. 2004).

2. “Regarding NISCC vulnerability advisory on SSL (secure sockets layer) and TLS - TID10087450.” 15 Jan. 2004. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10087450.htm (17 Jan. 2004).

3. “Securing the Server Console.” NetWare 6.5 Documentation. URL: http://www.novell.com/documentation/lg/nw65/sos__enu/data/hpmfqfmr.html (14 Jan. 2004).

4. “SECURE CONSOLE.” NetWare 6.5 Utilities Reference - NetWare 6.5 Documentation. URL: http://www.novell.com/documentation/lg/nw65/utlrfenu/data/hm9phvjr.html (16 Jan. 2004).

5. “SCRSAVER.” NetWare 6.5 Utilities Reference - NetWare 6.5 Documentation. URL: http://www.novell.com/documentation/lg/nw65/utlrfenu/data/hrs18jbe.html (16 Jan. 2004).

6. “Password Policy.” The SANS Security Policy Project. URL: http://www.sans.org/resources/policies/Password_Policy.pdf (19 Jan. 2004).

7. “Can Novell passwords be case sensitive? - TID10058370.” 25 Aug. 2003. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10058370.htm (28 Jan. 2004).

8. Kennard, Linda. “Tech Talk #4 - Nsure Identity Manager 2.0.” Novell Connection Magazine Nov/Dec 2003. URL: http://www.novell.com/connectionmagazine/2003/12/tech_talk_4.html (28 Jan. 2004).

9. “NetWare 6.5 Administration Overview.” NetWare 6.5 Documentation.URL: http://www.novell.com/documentation/lg/nw65/admin_ovw/data/front.html (29 Dec. 2003).

10. “NetWare 6.5 Remote Server Management Administration Guide.” NetWare 6.5 Documentation. URL: http://www.novell.com/documentation/lg/nw65/sman_enu/data/hw63v9ob.html (29 Dec. 2003).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

11. “Log Files” Apache HTTP Server Documentation Version 2.0. URL: http://httpd.apache.org/docs-2.0/logs.html (21 Jan. 2004).

12. Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security Essentials with CISSP CBK Version 2.1, Volume 2. SANS Press, April 2003.

13. “NetWare 6.5 NetWare Remote Manager Administration Guide.” NetWare 6.5 Documentation. URL: http://www.novell.com/documentation/lg/nw65/remotemgr/data/a7hjvxo.html (29 Dec. 2003).

14. “Using Novell iMonitor 2.1.” Novell eDirectory 8.7.3 Documentation. URL: http://www.novell.com/documentation/lg/edir873/edir873/data/agwkqvb.html (29 Dec. 2003).

15. “How to modify the default iMonitor port for NetWare - TID10079341.” 27 Jan. 2003. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10079341.htm (17 Jan. 2004).

16. OpenSSH. URL: http://www.openssh.com (21 Jan. 2004).

17. “OpenSSH Administration Guide for NetWare 6.5.” NetWare 6.5 Documentation.URL: http://www.novell.com/documentation/lg/nw65/openssh/data/front.html (29 Dec. 2003).

18. “SSH_CONFIG.” OpenBSD Manual Pages. URL: http://www.openbsd.org/cgi-bin/man.cgi?query=sshd_config (19 Jan. 2004).

19. Novell iManager 2.0.x Documentation. URL: http://www.novell.com/documentation/lg/imanager20/index.html (29 Dec. 2003).

20. “Novell iManager: Planning Security for Delegated Administration.” URL: http://www.novell.com/collateral/4621360/4621360.html (29 Jan. 2004).

21. “Tomcat Administration Guide for NetWare 6.5.” NetWare 6.5 Documentation. URL: http://www.novell.com/documentation/lg/nw65/web_tomcat/data/a7hjvxo.html (29 Jan. 2004).

22. “JavaServer Pages Technology - Frequently Asked Questions.” URL: http://java.sun.com/products/jsp/faq.html (29 Jan. 2004).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced