Securing the Modern NetWare Environment

By David Bank

CCNA, CCSE, CNE, CNA

Presented to

Triangle Novell User's Group

February 22, 2005

Goals

- It's common to find recent documentation concerning the best practices for hardening server environments using many *NIX OSes, and Windows; however, finding current information on securing the modern NetWare and eDirectory environments can be difficult
- This presentation will discuss recent thinking concerning NetWare/eDirectory hardening, and provide for discussion points to generate new ideas

Existing Sources of Information

- The SANS Institute Information Security Reading Room seems to be the only source of hardening documents for modern NetWare – most other sources cover NetWare v3 or v4
- Documents date from March, 2002 to February, 2004 – the newest for NetWare is over a year old, and not all cover NetWare v6.5
- URL -> http://www.sans.org/rr/whitepapers/novell

Thinking about Installation

- NetWare v6.5 offers as many as 19 different installation configurations (called “patterns”) – some are inadvisable as a starting point
- What functionality is essential for all server installs (for example, perhaps, the JVM)?
- What functionality should be limited in its deployment (for example, iManager)?
- What functionality should generally be omitted in <u>all</u> installs (for example, NWFTP)
- What installation defaults are not controllable at install-time, but present security risks?

Uncontrollable at Install

- SNMP Default Community Name (CVE CAN-1999-0517)
- Fix using INETCFG to change Community name, or better yet, disable SNMP
- INETCFG can be annoying – any other way to fix?

Uncontrollable at Install

- SSH v1 Protocol Support Enabled (CVE CAN-2001-0572)
- Edit SYS:ETC\SSH\SSHD.CONF and change the Protocol line to remove ,1
- Save the change and restart SSHD.NLM if needed

SYS: Volume Vulnerabilities

- What are some of the possible consequences of the **SYS:** Volume running out of space?

- Server Crash
- NDS Corruption
- User data loss
- Logging information loss
- Server may not be able to reboot successfully without intervention

Disk Space Security Strategies

- Place **SYS:** in its own NSS Pool
- Deny user objects the filesystem **Write** or **Create** permissions anywhere on **SYS:**
- Put Print Queues, **PUBLIC** subdirectory, GroupWise databases, MySQL databases, *etc.* on other Volumes
- Configure logging to write files to a different Volume
- Configure NetWare Swap file to use a different (dedicated?) Volume
- Put Apache **DocumentRoot** on a different Volume

NetWare FTP (NWFTP)

- Like all FTP servers, users authenticate in cleartext
- Disable if possible (remove from **AUTOEXEC.NCF**) and substitute SSL-secured iFolder
- If FTP must be available, use **SYS:ETC\FTPREST.CFG** to configure account access restrictions
- Log to a Volume other than **SYS:**

NetWare LDAP Server

- Used to authenticate to eDirectory from web applications – for example, iManager
- Generally, a network only needs one, perhaps two (a backup), LDAP servers
- Remove/Comment-out **NLDAP.NLM** from servers that don't need to host LDAP services
- Exclusively use SSL-encrypted LDAP (Port 636); disable unsecured LDAP over Port 389 (some 3rd-party vendor apps may require unencrypted LDAP support)

SSH – Secure SHell (OpenSSH)

- NetWare v6.5 includes OpenSSH
- This is for secure remote console, <u>not</u> for telnet or file system access
- Use in place of **RCONAG6.NLM**
- Requires SSH client on workstation, such as PuTTY or Secure Shell Client
- Remove SSH Protocol v1 support from **SYS:ETC\SSH\SSHD.CONF**
- Does <u>not</u> support key-based authentication

Console Screensaver (SCRSAVER)

- Use to secure keyboard on remote or unattended server
- Requires eDirectory to unlock – a server running DSREPAIR cannot be unlocked while the NDS databases are locked
- **Hacks:** Use debugger key-sequence to activate the debugger, kill the process, and resume NetWare <u>or</u> Use remote management tool to remotely unload **SCRSAVER.NLM**

NetWare Remote Manager

- Used for administration and troubleshooting of an individual server
- Modules **PORTAL.NLM** and **HTTPSTK.NLM** - the latter is a custom web server, provides the functionality over port 8009, and by default logs to **SYS:HTTPLOG.TXT** (file rolls over when it reaches 8 MB)
- Does **not** require rights to the server object for the ID used to login (unprivileged logins limited to file access and Simple Password management)

NetWare Remote Manager (cont'd)

- User-object-based logins use context specified in **SET BINDERY CONTEXT** or in the default eDirectory context as set of the NRM Configuration Options page
- **Warning!** NRM contains two hard-coded accounts (**SAdmin** and **SDebug)** that **do not exist in eDirectory** - Intruder Detection policies do not apply, password limited to 80 characters but is case-sensitive

Securing NRM

- Consider not using NRM – do not load the **PORTAL.NLM** module and also ditch **HTTPSTK.NLM** if not using iMonitor (NOTE: if using iPrint, see Novell TID #10095728)
- If NRM is needed, force warning page to appear before login by renaming **SYS:LOGIN\PRTLTXT.HTM** to **SYS:LOGIN\PRTLDISC.HTM** and adding appropriate text
- Only use SSL-secured connectivity

Securing NRM (cont'd)

- Using the NRM interface, enable logging, enable the debug screen, increase the logfile size (if appropriate/sensible), disable the **SAdmin** and **SDebug** accounts, configure E-mail notifications,and use the IP Address Access Control page to restrict NRM logins
- If possible, construct a separate network infrastructure for administration and only bind HTTPSTK to that environment
- See the NetWare Remote Manager documentation in the NetWare 6.5 doc library (http://www.novell.com/documentation/nw65/index.html)

iMonitor

- Web-based tool to monitor/diagnose eDirectory on a server – provides same functions as **DSTRACE**, **DSBROWSE**, **DSDIAG**, and **DSREPAIR**
- Uses **NDSIMON.NLM** and **HTTPSTK.NLM** and so is affected by same attacks, and HTTP-related configuration changes, as NRM
- Has no audit logs (**HTTPSTK.NLM** logging will only show iMonitor authentication attempts)
- Default configuration allows any authenticated user to submit requests (processing done under that user's eDirectory rights)

Securing iMonitor

- Change configuration so that only users with **Supervisor** right to server object can make iMonitor requests - in the **SYS:SYSTEM\NDSIMON.INI** configuration file, change **LOCKMASK** value from **1** (default) to **2** (also helps prevent DoS attacks by malformed URLs)
- Use only SSL-secured connectivity

iManager

- Web-based alternative to ConsoleOne – most of the same functionality
- A network only needs one or two iManager-enabled servers, preferably dedicated to the task
- iManager is enabled by the configuration file **SYS:TOMCAT/4/CONF/NPS-APACHE.CONF**; remove reference to this in **SYS:APACHE2\CONF\HTTPD.CONF** on servers not hosting iManager
- Use only SSL-secured connectivity (or configure Apache to only listen on Port 443 by removing the Port 80 **LISTEN** directive from **HTTPD.CONF**

Log Files & Locations

- Console Log – **SYS:ETC\CONSOLE.LOG**
- System Error Log (see **SET SERVER LOG** parameter) – **SYS:SYSTEM\SYS$ERR.LOG**
- Volume log (one per Volume, FAT only) – **SYS:VOL$ERR.LOG**
- ABEND Log – **SYS:SYSTEM\ABEND.LOG**
- DHCPSRVR v2.0g or later – **SYS:ETC\DHCP.LOG**
- CRON log – **SYS:ETC\CRONLOG**
- FTP server – as per FTP configuration file

Log Files & Locations (cont'd)

- Web server logs (regular Apache) – **SYS: APACHE2\LOGS \ERROR.LOG** and **SYS: APACHE2\LOGS \ACCESS.LOG**
- Web server logs (Administration Apache) – **SYS: ADMINSRV\LOGS \ERROR.LOG** and **SYS: ADMINSRV\LOGS \ACCESS.LOG**
- OpenSSH Log (requires **SSHLOGD.NLM**) – **SYS:ETC\SSH\LOGS**
- HTTPSTK log – **SYS:HTTPLOG.TXT**

Log Files & Locations (cont'd)

- DSREPAIR log – **SYS:SYSTEM\DSREPAIR.LOG**
- DSTRACE screen log – **SYS:SYSTEM\DSTRACE.DBG**
- **DSTRACE.NLM** log – **SYS:SYSTEM\DSTRACE.LOG**
- Boot error log – **SYS:SYSTEM\BOOT$LOG.ERR**

Logging Security

- Whenever configurable, store logs someplace other than the **SYS:** Volume - this option exists for the FTP, SSH, Apache and System Error logs
- Read the logs – they don't do you any good if you never look at them
- Some logs can be accessed via the server object properties

SNMP

- SNMP support is loaded/enabled when the TCP/IP stack is loaded – it cannot be disabled, which is bad if you do not have an SNMP-based management environment
- Change the SNMP Community settings using **TCPCON.NLM**
- SNMP is not all bad – it can be used to monitor eDirectory and the MIB has over 100 defined traps

Conclusions

- The various NetWare installation Patterns contain some vulnerabilities
- Like any other environment, the more functionality that is enabled, the more vulnerabilities may be found
- Take a “If we don’t need it, we don’t run it” approach to installation and configuration
- Don’t forget to secure eDirectory

Conclusions (cont'd)

- Controlling end-user access to the **SYS:** Volume is crucial – avoid filesystem permissions that allow user-writes
- Secure web-based management tools such as iManager, NDS iMonitor and iManager
- Avoid running excessive copies of web-based management tools
- Avoid FTP and unencrypted LDAP
- Use SSH instead of RConsole

Conclusions (cont'd)

- Keep NetWare up-to-date on Support Packs
- Keep abreast of Post-SP patches, especially ones for the TCP/IP protocol stack, NSS, eDirectory and web-based tools (*e.g.* iPrint)
- Sleep soundly at night