Global Information Assurance Certification Paper

A Compendium of Security tools for the NetWare 5.1 Server Console

GSEC Practical Assignment, Version 1.4
Option 1
October 22, 2002
By Sheila Corey

Abstract:

In this paper I explore basic NetWare 5.1 server console security, focusing on physically securing the server by mechanical and software means. This research has been conducted primarily as background information for a server upgrade planned in my agency. Having little previous NetWare experience I needed to gain an understanding of the security issues specific to NetWare 5.1 servers, how to remedy them, and how to maintain the most secure server environment. Although there are multitudes of issues that could be covered on this topic, I have selected this abbreviated list of console security tools that I regarded as useful in my agency's environment, and that I have a particular interest in learning more about.

I address these issues logically as a hacker may in attempting to exploit a system:

- Getting into a server room,
- Getting to a server,
- Accessing the server console,
- Tampering with or destroying the operating system, data, programs and user accounts.

Introduction

The logical place to start any broad security discussion is with the physical security of servers, workstations and the network infrastructure. Network administrators already know the importance of physical security, and it isn't specific to NetWare servers, but it is basic. Servers must be secured, preferably in locked rooms, to keep unauthorized access to a minimum. An unsecured NetWare server is open for anyone to enter console commands. The list of offenses an intruder could commit with physical access to a NetWare server is long. Some of the most notorious are:

- Load and unload NLMs, (**N**etWare **L**oadable **M**odule; basically, a NetWare program),
- Remove NDS, (Novell Directory Services)

- Place the server into debug mode, to allow manipulation of the operating system
- Obtain unauthorized supervisor access
- Take over with supervisor-level permissions
- Leave back doors
- Crack passwords past the server
- Set a new password
- Disable passwords
- Defeat console logging functions
- Set console passwords to known values
- Detect hidden files on the server
- Access server startup (NCF) files
- Detect audit status
- Introduce Trojan horses
- Prevent server configuration from being changed
- Prevent console security parameters from being changed
- Shut the server down
- Remove the disk drives, install them on another NetWare server, and have full access to the data!

The following discussion will take a quick look at some of the tools available in the NetWare 5.1 System Administrator's arsenal to reduce the risk of having an intruder compromise a server from the console.

Lock up the Server

As the list above demonstrates, it is VERY easy to gain access to a NetWare server and compromise it if there is direct, physical access to it. Fortunately, there are some simple and inexpensive ways to control this direct access, and hinder attempted console exploits.

The server room should be secured in a manner that is consistent with the needs of a particular business environment. For many sites what this means is that the server room is simply accessible with a key or touch pad combination. In other environments key cards may be desired for a higher level of security since they can be tracked if needed, and for some sites a door guard or other more sophisticated security mechanism may be desirable. Once inside the server room, the server box itself should be locked with a supplementary lock and key (if the hardware came with a door and lock), or mounted in a locking rack. Some sites like the added security of keeping the keyboard and other input devices in a separate, locked room. The keys for locking doors, racks and hardware should be stored in a secure area known to and accessible only to authorized Network Administrators.

These “lock it up” safeguards significantly reduce the opportunity for unauthorized access to the power switch, floppy, CD, and hard drives of a server and to the server console.

Power-on Password

Many manufacturers have built servers that provide the ability to configure a CMOS power-on password. This option, when selected, will require manual intervention; supplying a password when the server is physically powered on. An additional barrier that can be used is a password that can be configured which secures the CMOS editing tool! The power-on password is only used to secure a system during its initial power up. The password is set in the BIOS and requires the password be entered before the system will boot. The password can be changed at any time once it has been entered correctly and the system allows you to enter the BIOS.

Although this allows another level of security, it is not the perfect fail-safe. There are ways an intruder could remove or defeat the power-on password, although each requires physical access to the server. The power-on password for the system will never do a "lock out". The server could be re-booted indefinitely and new password attempts made each time. Eventually, given enough time, an intruder could crack the password and be in. Other methods an intruder could employ (depending on the system, and what is most useful to the intruder to perform a hostile “take over”) would be to either reset a jumper on the motherboard itself (referred to as a "clear CMOS" jumper), or by removing the CMOS battery. Removing the battery clears NVRAM in CMOS and resets the system to default settings. (DEW Associates Corporation, 2000)

System Administrators need to be aware of and plan for the implications power-on passwords present. With a power-on password, server "power up" or "cold start" requires that the password be entered manually. If the system were to go down during a power outage, for example, the password would have to be entered for the server to boot. If a server has the "lights out" feature board installed, this password could be entered remotely but would still need to be done manually. (Compaq Computer Corporation, 2000).

Securing the Console

NetWare’s server console can be and should be secured with software. With access to the system console an intruder can easily wreak havoc on the network. Console attacks that can be launched at the console prompt include:

- Load hostile NLM’s or unload existing NLM’s on the server
- Gain Supervisor access by running a hostile NLM or hacker program

- Defeat the console logging processes by unloading NLM's and editing log files
- Bypass a console locked by the MONITOR utility
- Permit a remote console attack
- Remove NDS with DSREMOVE
- Detect audit "on" status by checking for the active audit file
- Remove auditing features
- Gain access to the console debugger for code modification, to disable password checking and to perform file editing.

SCRSAVER.NLM utility

A utility that comes shipped with NetWare 5.1 for the purpose of securing the console is the SCRSAVER.NLM. In previous versions of NetWare, this function was provided by the MONITOR.NLM. (Urbanek, 2001). SCRSAVER.NLM will lock the screen and display the server load "snake". It will prompt for a NDS user name and password to allow entry. Only an account with Supervisor access to the server can unlock the console.

This utility has a variety of commands that can be used to set parameters for the screen lock/console lock. Setting these parameters correctly is absolutely necessary for maximum security. Since the screen saver can be enabled with or without console locking, it is important to enable the console-locking feature, but beware! Remember that SCRSAVER uses NDS to authenticate the console login user and password. If NDS were unavailable or locked for any reason, and the console were also SCRSAVER locked, there would be a situation where console login could not occur because NDS authentication would be required, which couldn't happen because NDS is unavailable. Access to the server console would be available only by rebooting or otherwise exiting NetWare. (Daryn, 1999).

One solution to this is to load SCRSAVER with the NO PASSWORD option. A password would still be required when NDS is available, but in the remote chance that NDS were unavailable, a password would not be required to unlock the console. To ensure that SCRSAVER is loaded when the server starts, place SCRSAVER in the autoexec.ncf file, with appropriate parameters. Refer to Novell's TID #10020745 for specifics on the SCRSAVER utility, the commands available and how to set it up in the autoexec file.

Use SECURE CONSOLE

The SECURE CONSOLE command is a NetWare utility. SECURE CONSOLE does not lock the server console, rather it removes DOS from the server memory, freezes the servers current DOS search path, prevents changes to the

system clock and deactivates the system debugger. (Burnett, 2002) Typing SECURE CONSOLE at the command prompt has the same effect as issuing the REMOVE DOS command. Removing DOS from memory effectively prevents an NLM from being loaded from the server's floppy drive or boot partition (unless it is already in a search path), minimizing the chance that hostile NLM's can be loaded by intruders.

SECURE CONSOLE protects the server code from unauthorized changes by disabling keyboard access to the operating system debugger (SHIFT + SHIFT + ALT + ESC), and prevents date and time changes by anyone, including Admin. Entering the debugger would allow an intruder to directly patch the running server code and possibly bypass security mechanisms. Time and date changes could be made to password expiration, lockout intervals, login restrictions and expired accounts allowing an intruder to gain access through old accounts. To remove SECURE CONSOLE, the server must be re-booted. If SECURE CONSOLE is part of the autoexec.ncf file, that file must be edited prior to rebooting or the console will not be un-secured. For additional information or clarification on using SECURE CONSOLE refer to Novell's NetWare 5 Documentation. (Novell NetWare 5 Documentation).

Disable Rconsole and RconsolJ

Rconsole and RconsolJ, are two NetWare remote access DOS utilities. Both have a known weak password mechanism: an intruder with access to packet capture tools (like HACK.EXE) might be able to trap the REMOTE password, decode it, and gain access to the console. This is possible because these utilities both operate over nonencrypted connections.

Rconsole is like rlogin or telnet in that it connects a user to a remote machine. Characters typed remotely are interpreted exactly as if they had been typed at the console, and status/monitoring information written to the console appear in the Rconsole session. System Administrator's can perform the following functions from a remote console:

- Use console commands as you would at the server console.
- Scan directories and edit text files in both NetWare and DOS partitions on a server.
- Transfer files to, but not from, a server.
- Bring down or reboot a server.
- Install or upgrade NetWare. (NetWare 5.1 online documentation, Rconsole. 2002)

Many System Administrators feel that remote access to their server is mandatory, as it can ease system administration tasks significantly. However,

this can also be the bane of a System Administrator's existence if this helpful tool became available to a hostile intruder.

For Rconsole and RconsolJ to execute on start-up, passwords must be entered into a text file that is often left as clear text. Clear text passwords alone make remote access a popular hack for intruders. NetWare has the means for encrypting remote console passwords with options within the utilities themselves. For the best remote security encrypted passwords should be required. (Novak, 2000).

It is good practice not to use Rconsole and RconsolJ under any circumstances unless the security vulnerabilities are well understood and the business environment is willing to accept the risks.

Installation issues

When the NetWare 5.1 operating system is being installed on a server there are a few key issues that should be considered for enhanced security.

First is to check for security alerts and patches available on the Novell web site: http://support.novell.com/security-alerts/, http://support.novell.com/filefinder/9331/index.html and http://support.novell.com/produpdate/patchlist.html
Download and apply all those that are pertinent for your server environment.

It is appropriate and necessary for the System Administrator to choose the services and applications that will be needed in the network environment prior to installation of NetWare. Unnecessary products and services simply add to administrative overhead and provide additional opportunities for intruders to exploit the system. A simple rule of thumb is: "Don't load what you don't need."

Since NetWare 5.1 comes with several networking products several choices must be made. Many auxiliary services are not critical and can be removed from the server or never loaded to begin with. Such services as FTP server, telnet, DHCP, Rconsole and RconsoleJ should be considered carefully before leaving them on the server.

It is a known security issue that the default NetWare 5.1 installation contains several sample applications that allow remote users to gain sensitive server configuration information such as passwords! The only way to remedy this problem currently is to remove the sample applications before putting the server into production. (CERT Advisory Vulnerability Note VU#159203, 2002).

The ADMIN Account

The most powerful user object in NetWare 5.1 is the Admin user object. This user has complete access to all other objects in the NetWare tree. The Admin account has access to the console and can unlock it if it is locked. Because of this all encompassing power, and the fact that it is a standard, integral part of NetWare and NDS implementation, it is not surprising that Admin is the target of many NetWare hacks. Because the Admin object is like any other user object it can be renamed, deleted, moved and locked out.

Some security measures to protect the Admin object are to rename it and place it in a typical user container, using it only when absolutely necessary. Create another object named Admin, lock it out and audit it. Check the logs frequently to ensure that intruders are not trying to enter, or worse, that they have! Allow System Administrators only the rights they need to perform their particular job. (Novak, 2000). Change the Admin password every 60 days and keep it in a secure place that is accessible by only those System Administrators that require it.

Monitor System logs

There are many ways to monitor systems, and unless something is in place it would be difficult, at best, to determine if passive intruders have been meddling. One way is to purchase third party software that automatically monitors systems by reading logs, watching for well-known hacking "signatures" and other signs that an intrusion is taking place or has already taken place. (Compaq, 2002).

NetWare has system and network logs that should be reviewed daily. The NetWare log file that is most often a target for hackers is the CONSOLE.LOG file. This file is created when the CONLOG NLM is loaded on the system. All system responses are recorded in this log. Hackers wishing to hide evidence of their intrusion may utilize the following quick steps (if they have access to the console and supervisor privileges):

1. Unload CONLOG
2. Delete or edit CONSOLE.LOG file to remove evidence of the "visit"
3. Delete or edit SYS$LOG.ERR file

Novell's AuditCon utility can be used to monitor all aspects of network activity, including Supervisor authentication, NDS container changes, login script changes and user-policy compliance. (Novak, 2000). These are items of concern when unexpected changes occur, perhaps at unusual times.

Viruses

"…the bulk of all security breaches result from computer viruses. This one fact tells you that you want to ensure that your business-critical applications don't run on systems that are overly susceptible to viruses."
(Compaq, 2002)

This quote taken from the Compaq/HP website indicates that although hackers and intruders are a definite threat to enterprise business systems, they are not the threat that is most predominant. With this knowledge, System Administrators should make it a priority to secure their servers with up to date antivirus software and signature files.

NetWare is susceptible to viruses, worms, bombs, and trojan horses, all of which are malicious programs that can destroy or damage data or perform undesired or unintended operations. Although these programs can be stored on a NetWare file system, NetWare architecture provides no way for a non-administrative user to run the malicious code. A user or intruder with Supervisor access could however. To reduce the risk of damage to the server by malicious code, the following tasks should be incorporated into the antivirus policy for the business enterprise:

- Configure virus software to immediately send virus notification(s) to the network administrator and the user.
- Enable the virus expiration warnings to alert the System Administrator when signatures are outdated.
- Set the server's virus scanning software to scan both incoming and outgoing files.
- Include all file types when scanning.
- If possible, do not give users the option to cancel the virus check or virus repair.
- Use Novell's ZENworks for Desktops to mass-distribute virus signature updates. With ZENworks, updates can be automatically downloaded to all workstations without user intervention.
- Update the write-protected emergency boot diskette whenever new signature files are received.
- Scan all incoming and outgoing e-mail and attachments.
- Discourage users from downloading non-work-related e-mail attachments.
- Configure e-mail servers to filter and eliminate unsolicited junk e-mail that could contain a virus or malicious code.(Foust, 2000)

Conclusion

Much of the effort needed to physically secure a NetWare 5.1 server is common sense in securing any server. Locked server rooms, locked racks and screen locking mechanisms all play a role in keeping any server safe and healthy. The specific issues for NetWare security rise from the well known and widely

exploited physical vulnerabilities that exist on most NetWare servers if left configured to their defaults.

Fortunately, several utilities and safeguards can be employed with minimal effort to accomplish magnitudes of gain on the security front. Simple utilities such as SCRSAVER and SECURE CONSOLE when properly implemented can greatly reduce risk at the console, while the simple act of changing the Admin account to an ordinary user and creating a new Admin equivalent account will foil many would be hackers.

Knowing the system and the business requirements of the environment will help the System Administrator decide on what services are critical and which ones can be removed from the system, keeping system administration more simple with fewer services to worry about, and removing potential security holes for hackers to exploit.

References:

1. Accepted Answer from Daryn. "How to activate screen saver under NW5?", December 23,1999
   URL:http://www.expertsexchange.com/Networking/Netware/Q_10250653.html

2. Burnett, Kevin. "Console Commands in NetWare 5.1: SCAN ALL, SCAN FOR NEW DEVICES, SEARCH, SECURE CONSOLE, SEND", September, 2001.
   URL:http://developer.novell.com/research/sections/netmanage/netnovice/2001/septembe/n010901.htm

3. CERT Advisory Vulnerability Note VU#159203 "Novell NetWare default installation contains sample files that disclose sensitive server information". September 19, 2002
   URL: http://www.kb.cert.org/vuls/id/159203

4. Compaq Information Technologies Group, L.P. "Compaq AlphaServer GS Series Systems". December 2000
   URL: http://nonstop.compaq.com/view.asp?IO=Gssystpd#4

5. Compaq Information Technologies Group, L.P. "Security best practices for NonStop Servers". April 2002.
   URL: http://nonstop.compaq.com/view.asp?IO=SECBESTAR

6. DEW Associates Corporation. 2000
   URL: http://www.dewassoc.com/support/bios/bios_password.htm

7. Foust, Mark. “NetWare Security: Closing the Doors to Hackers”, June 7, 2000
URL: http://developer.novell.com/research/appnotes/2000/june/03/apv.htm

8. Hughes, Jeffrey F and Thomas, Blair W. "Learning and Applying the Rules of NDS Security", August, 1997
URL: http://developer.novell.com/research/appnotes/1997/august/02/apv.htm

9. Jeffress,Terry L. “Novell's Protected Security Model: Keeping Out the Bad Guys”, 1998.
URL: http://www.nwconnection.com/sep.96/pro96/

10. Liebing, Edward A. “What’s New in the NetWare 5 Operating System?”, September 1998.
URL:http://developer.novell.com/research/appnotes/1998/septembe/01/a980901 .pdf

11. Novak, Kevin. “Securing Your NetWare Environment”. October 16, 2000
URL: http://secinf.net/info/nw/novak/1120ws1.html

12. NetWare 5.1 online documentation, Secure Console. 2002
URL:http://www.novell.com/documentation/lg/nw51/index.html?page=/documentation/lg/nw51/utlrfenu/data/hm9phvjr.html

13. NetWare 5.1 online documentation, Rconsole. 2002
URL:http://www.novell.com/documentation/lg/nw51/index.html?page=/documentation/lg/nw51/utlrfenu/data/hhi58tbu.html

14. Novell AppNote."Protecting Your Network Against Known Security Threats". Nov 97 (updated December 1998)
URL:http://developer.novell.com/research/appnotes/1997/november/06/apv.htm

15. Novell Technical Information Document. “Console Lock / Screen Saver in NetWare 5 - TID10020745”. (last modified October 9, 2002)
URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10020745.htm

16. Novell Technical Information Document. “How do I disable Secure Console? - TID10059929” (last modified 29JUL2002)
URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10059929.htm

17. Novell Technical Information Document. “Disabling Passwords using the NetWare Debugger - TID2917696” (last modified 03DEC1996)
URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2917696.htm

18. Novell NetWare 5 Documentation. 2002
URL:http://www.novell.com/documentation/lg/nw5/docui/index.html#../usserver/ssec_enu/data/hpmfqfmr.html

19. Simple Nomad. “The Unofficial NetWare Hack FAQ,Beta Version 6. May 1, 1997
URL: http://www.nmrc.org/faqs/netware/index.html

20. The Santa Cruz Operation, Inc “Comparing the NetWare bindery and NDS”. March 19,1999
URL:http://docsrv.caldera.com/SDK_wcpg/wcpgC.Comparing_the_netware_bindery_a.html

21. Urbanek, Robert. “NetWare 5 and Microsoft NT4 Installation and Support” January 27, 2001.
URL: http://www.algonquinc.on.ca/~urbaner/review.htm