Global Information Assurance Certification Paper

Roger Black
Version 1.4b
Novell Netware 3.X Exploits and Defense

SUMMARY:

Ancient by most standards of technology, Novell Netware 3.X remains in many IT shops around the world. Ignoring the security of legacy systems such as Netware 3.X in any networked environment can prove as disastrous as ignoring the security of your most current systems. A breach in their security (perhaps uncovering the Supervisor password that happens to be the same as the NT/W2K Domain Admin?) should be considered with equal importance. It is the purpose of this paper to provide a description of the most common Novell 3.X attacks and exploits, and to note the recommended countermeasures. This paper assumes an administrator level of Netware 3.X knowledge.

SKELETONS IN THE CLOSET:

Network operating systems have changed significantly over the last decade. Software manufacturers continually produce version upgrades and/or revisions (if not whole sale replacements) of their products. For a variety of reasons, businesses continue to use "older" operating systems. In some instances, they are using software designed to run on that specific OS and no upgrade path is available, they cannot afford or do not have the technical expertise to implement a pricey upgrade solution, or they are often unaware of the risks that they are exposing their company to by continuing to have the OS on their network. Just as often, administrators find a balance of performance and functionality that they hesitate to break from. What becomes of these systems? They most certainly don't simply disappear and stop functioning. Instead, they chug along, with a great many administrators chanting the mantra "If it ain't broke, don't fix it." One such operating system line, Novell Netware 3.X, is still firmly entrenched in many IT shops throughout the world. Third party vendors such as Symantec and Veritas still provide support and updates for their products running on the Netware 3.X platform as well.

Unfortunately, these systems seldom have attention paid to them from an information security perspective. Because Windows and Unix based servers are prevalent in most networked environments, information security prevention and techniques typically focus on those two operating systems. Additionally, information security tends to pay attention to the primary protocol of these operating systems, TCP/IP. But the attention paid to both Windows and Unix systems belies the fact that there are still a great many legacy systems in use today. According to Novell, approximately 300,000 Netware 3.X servers are currently in production worldwide[i], making up roughly 30% of its Netware installed base (this does not include unregistered or illegal installations)[ii]. While a server presence this small may seem relatively trivial, it is essential that system administrators, management, and executive level information security personnel

have knowledge of every object on their network, and that the security of these machines be placed on the same level as any other networked device.

Complicating issues for the administrator, support for older operating systems is usually limited to internet based user groups and resources. Trying to find what weaknesses your system may have and how to fix them can become difficult and time consuming with no authoritative source of information. As a result, these systems can be neglected and all but forgotten from a security standpoint.

Novell no longer directly supports earlier versions of Netware 3.X, or provides current system updates and patches.[iii] The company's primary recommendation for administrators who are security conscious is to immediately upgrade to Novell Netware 5.1, or at a bare minimum, apply all of the patches available to bring your system to 3.2.[iv] This leaves some 3.X administrators in the unfortunate position of having to determine how to secure their Novell OS without specific information, patches, or updates from the manufacturer.

It is the purpose of this paper to give administrators a condensed resource to either to help secure their Netware 3.X network, or to help rationalize an upgrade of their OS to a platform that has the ability to be more secure. There are individual patches available that prevent many of these exploits, but many attacks remain valid unless a major upgrade is performed (predominantly, an upgrade to Netware 4.X or 5.X). This paper in no way attempts to document every known Netware 3.X exploit or vulnerability. Instead, it discusses and synthesizes the most popular exploits and vulnerabilities (many of which are still widely available via the internet), and the defenses against them. Because many exploits are comparable in their functionality, the most common executable name will be followed by similar exploits in parenthesis. In addition, Netware 3.X specific defenses will be suggested for these common exploits, as well as information security defenses in general.

NOVELL NETWARE 3.X SECURITY:

The first step in securing these legacy systems is to recognize the types of attacks available, and to apply some of the same security measures that should be adhered to regardless of the operating system. According to estimates, approximately 80% of Netware attacks occur on the 3.X line.[v] Most attacks and exploits of Netware 3.X fall under the same broad categories as other operating systems. These include viruses, DoS (Denial of Service), password attacks, and general operating system exploits based on bugs in the code. In addition, many of the exploits that are known are made available (or at least aided) by utilities that Novell provides with Netware! It should be noted that some of these exploits can be prevented from upgrading the OS (from Novell 3.11 to 3.12, for instance) or downloading individual patches from Novell. But many remain fully functional across the entire 3.X line (including Netware 3.2), and are not prevented unless migrating from the 3.X bindery to Novell's NDS (Netware 4.X, 5.X, or 6.X). . NDS offers far more granular security than the Bindery of the Netware 2.X and 3.X line, featuring scalability and flexibility while keeping manageability (and the management of security elements) simple. The 3.X Bindery, in contrast, is a

"flat" database which isn't very scalable, and makes management of security fundamentals troublesome.[vi] But again, the expense in upgrading to NDS services may not be a viable option for administrators.

CONSOLE/PHYSICAL ACCESS EXPLOITS:

In researching Netware 3.X exploits, some of the most common and damaging attacks demand physical access to the console. This infers that an individual can walk up to the server itself and access the console. The adage "There is no security without physical security" holds true here. There are a sundry of different hacks that can be used if an attacker has physical access to the console. Typically, the first thing that comes to an administrator's mind when a user has access to a server is powering the server down. But this is actually the tip of the iceberg with respect to what can be done with this level of physical access. Aside from downing the server (a very basic DoS), a more worthwhile pursuit for the hacker is to strive to get "supervisor privileges" on a targeted system. Physical access to the server makes their job much easier as the number of exploits is substantial. Some of these exploits leave much more visible signs of their use than others.[vii] [viii]

- Using a disk editor at the server, you can gain access to the physical password file positions and attributes on the hard drive. After renaming the appropriate supervisor password files and rebooting, Netware 3.X believes that the Supervisor password is blank.[ix]
- An intruder could run *Lasthope.nlm* which resets bindery security on all directories, users, groups, and files, to their default permission settings. Obviously, this tactic will quickly be evident to an administrator.
- *Burglar.nlm (Password.nlm, Security.nlm)*—these utilities are run from a floppy on the server. It creates a user with supervisor privileges (username and password can be user assigned).
- A variety of different .NLMs can be used to rest user passwords via the console as well. Some of the most popular, *Setpass.nlm*, (*Setspwd.nlm*, *Setpwd.nlm)*, will all change the password of a username that is passed to it via the command line.[x]

Additionally, there are a variety of other attacks that can occur if physical access to the server is not secured. These include placing the server in "debug" mode via keyboard commands to alter or eliminate passwords and password checking, getting access to *autoexec.ncf* (as well as other files that are execute at startup) and altering them to start trojans, turning off intrusion detection, and limiting/stopping other security measures that are configured to run at startup. If the server is also a print server, a well known exploit is to down the print server via *pconsole*. This then allows an intruder to get to a console screen and unload the *monitor.nlm*, even if it has been locked. Additionally, if the administrator is using console logging to detect intrusions, the log can be edited by unloading the *Conlog.nlm* and then editing the associated text file.[xi] Obviously, if unauthorized

individuals have physical access to the server the damage that they can inflict is great, and the security of your network can be severely compromised.

CONSOLE/PHYSICAL ACCESS DEFENCE:[xii] [xiii] [xiv]

As with any server or network device, physical access considerations should be placed at a premium. The likelihood of an intrusion (or even an accidental shutdown) is far greater when the device can be accessed physically. Defending against physical access to a server is theoretically simple, but can be difficult to implement. Considerations for Netware 3.X physical security follow the same general tenets as other information security principles, but also include a few specific recommendations. These take into consideration the prevention of physical access, as well as techniques to thwart intrusions once physical security is breached:

General

- All means of entry into the server room should be locked at all times. Entry into the room should be logged.
- Keep the server in the secured area with only limited access for qualified personnel.
- Use some sort of personal identification to help ensure identity (key cards, biometrics, etc) when accessing the room.
- Personal identification combined with a "secret" password (i.e., a key card used with a private P.I.N.) adds an additional layer of protection.
- Mounting devices in lockable racks provides another barrier for an intruder to overcome.
- Consider the use of security hardware that makes the physical removal of devices difficult or impossible.
- Keeping the keyboard and other input devices in a separate location from the server is an even more drastic (but effective) security measure.
- Although not considered a true "physical" security measure, console and/or screen locks can help prevent intrusion should physical access be given (see below).

Netware 3.X Specific

- Use the command "*Secure Console*" so that debugging exploit cannot be used, and to limit the loading of additional .NLMs from anywhere else but the console.
- Load and run "*Monitor.nlm*" so that the console can be "locked" via the display.
- A critical step in preventing these utilities to be run is to disable access to additional .NLMs. The loading of .NLMs from the server console or from a removable media source such as a floppy drive can be thwarted by using the "*remove DOS*" command at the console. Any additional .NLMs can not be accessed to be loaded.[xv]

- Use different password when loading the Monitor.nlm, Supervisor accounts, and (if needed) Rconsole. This prevents intruders from having one key to open up all doors.

While the Netware specific recommendations are more a "logical" defense against a physical attack, they are equally important as door lockas and barriers when protecting your server physically. They provide additional layers of defense when an intruder already has physical access.

REMOTE ACCESS (non-physical) EXPLOITS :[xvi] [xvii]

Not having physical access to a server is an inconvenience to an intruder, but by no means precludes the possibility of an intrusion. In fact, the amount of exploits that can be used by simply being "on the wire" outnumbers those that demand physical access to the server, and can be more difficult to detect, defend, and prevent.

One of the largest issues concerning Novell Netware (this applies to version 3 through 5) is that users do not have to be logged into the server to retrieve valuable information from it. Users can simply "attach" to the server without logging in, and then once attached, have the ability to use a variety of reconnaissance tools. The ability to attach to a server without logging in is still available in the latest releases of Netware. Utilities such as *On-Site Admin*, *Userinfo*, *Userdump*, *Slist*, as well as other bindery viewing tools such as *Bindin* and *Bindery* give intruders varying degrees of information regarding users and groups on the server. As mentioned, all of this information comes without the intruder having to log into the server itself, thus not having a concern about intrusion detection or accounting/auditing.

The above mentioned utilities provide a wide range of reconnaissance information from the server, but the real damage is not done there. The remote exploits generally abuse file permissions, administrative oversights and Netware operating system bugs to give a user access to the server, and often attain supervisor privileges as well. In most cases, a user will merely need to be "on the same wire" as the server to run these utilities, meaning that the user only needs network access and the ability to attach (not necessarily login) to the system. Because these exploits utilize so many different techniques, the defense from them relies on in depth knowledge of the system's installation, configuration, and default settings. The exploits listed below are well known Novell 3.X exploits.[xviii]

- *NW-Hack.exe* is run on a network workstation and is basically a "man in the middle" attack. It will search out the network node that the supervisor is currently logged in from, and then imitates that node. Now that the server believes it is still receiving information from the real supervisor, the program changes the supervisor password and gives all users supervisor rights. Obviously, network administrators will eventually notice the security breach, and will run utilities that enable them to see who has supervisor access. The basic defense against this type of attack is to

enable packet signature on the server. This ensures that packets have originated from the server (this option can also be set on workstations to verify their authenticity as well).

In conjunction with the NW-Hack exploit, the following utilities build upon the compromised supervisor or supervisor equivalent account.

- *Login.exe/Prop.exe* can be used with supervisor privileges as well. By running prop.exe, a new object is created in the bindery which, when used in conjunction with an altered login.exe (placed in the sys:login directory on the server) acts as a repository for all usernames and password that login into the server. Although these are two of the common programs used for Novell hacks, most key logging programs will work in a similar fashion, storing console keystrokes in a directory to be accessed at a later time.
- After gaining supervisor level access, intruders can run the *Super.exe* utility which lets them toggle on/off the supervisor privileges. When an administrator runs a supervisor equivalency tool, he/she will not detect the account that has the potential for supervisor access.

Once an intruder can access a server (even if just by attaching to a Novell 3.X server), a frequently occurring security problem in all server contexts is the creation of users with no passwords, or the username as the password. The utility *Chknull* will locate accounts on a Netware installation and report back the users who do not have passwords, or users who have their usernames as passwords. The accounts will not be locked out as there are no attempts at logging into the server while using this utility. Another well known technique to gain access to a server is to use password crackers. There are many utilities that will perform this function (both brute force based and dictionary based). Some that are well known in the Novell 3.X world include *Novelbfh.exe, Nwpcrack.exe…..*Most of these password guessing programs will only function successfully (or at least with little chance of discovery) if intrusion detection is turned off on the server. If not, accounts will be locked out and/or the administrator notified.

- *Rconsole.exe*

Rconsole could be considered one of Novell 3.X's largest threats, and many security experts recommend using it only if necessary. Its weaknesses stem from its location and typical usage. By default, it is located in the *SYS:PUBLIC* directory to which all users have access. Also by default, the *Rconsole* password is blank. This means that any user could have console access to the server remotely. In addition, even if a user knows the supervisor password, this password by default will also work to enable Rconsole. With this utility being available and the password known, a user need not be physically at the server in order to manage it.

To thwart possible attempts at getting into the server via *Rconsole*, it is recommended to use the "*load remote pwd*" command in the *autoexec.ncf*. If at all possible, use the "*load remote*" command in conjunction with encryption so that the password is not visible in the *autoexec.ncf*. *Rconsole* is also vulnerable to anyone who happens to be sniffing the same wire that the server is on. The password is by default sent over the wire unencrypted (or very near unencrypted…it only takes an IPX/SPX packet analyzer called *Rcon.exe* to extract the password. Newer versions of Rconsole will not send the password across the network.

REMOTE ACCESS (non-physical) DEFENCE:[xix] [xx]

There are varied countermeasures to thwart network based attacks. Again, some of these techniques can be applied to all network operating systems, while some are specific to Novell 3.X.

General:

- As with any OS, ensure the use of proper password policies. Set a minimum password length as well as allowed password age and reoccurrence frequency.
- Consider implementing time constraints (when users can access the network), as well as how much time users are allotted. This helps define usage patterns and violations.
- Change the default username and passwords for system and software accounts. These usernames are typically well known and are set as defaults.
- Match directory and file level permissions with the appropriate users and groups. Although the default configuration of Novell 3.X is more secure than other operating system defaults, it still leaves many doors open for the vigilant intruder.
- Use antivirus on clients and servers. Not only will it detect virus, but it will also detect Trojans, as well as other utilities that can cause harm to the network.

Netware 3.X Specific:[xxi] [xxii] [xxiii] [xxiv][xxv]

- Attaching to a Novell server remains a security concern, even with the newest releases. Utilities such as "On-Site Admin" can reveal a wealth of information concerning users, groups, as well as the hardware address of the server. In this event, the best precaution is to enforce routine administration of user accounts/password policies, and to review directory permissions and give only those permissions that are necessary (this can prevent accidental directory read and browsing rights)
- Become aware of the different utilities and the executables needed to run them. A group of utilities widely available for hacking Netware servers, *Pandora*, comes prepackaged with a variety of utilities and instructions on how to use them. By becoming familiar with the "tools of the trade", an alert administrator can avert disaster.

- It is widely recommended to use the Supervisor account (or supervisor equivalent accounts) as little as possible. This helps prevent packet sniffing utilities from getting the supervisor password. The Supervisor account itself cannot be renamed or deleted, so hackers have a head start by default.
- Intruder detection should be set to disable accounts after a predetermined number of attempts. Administrators may wish to consider re-enabling the account after a certain period of inactivity, or manually enabling the account themselves after a proper inquiry into what exactly caused the lockout. It should be noted that the messages that Novell 3.X sends to the user typically will alert them of the presence of intrusion detection. These messages will unfortunately also alert an intruder.
- Enable Accounting on the server to track logon successes and failures. This could prove useful if an intruder knows that Intrusion Detection is turned on, and knows how long to wait between attempts. An administrator could observe errant or strange logon attempt, behaviors, and patterns.
- Enabling packet signatures will prevent users who sniff the wire from impersonating the server or client (packet signature needs to be set on the workstation and the server). Packet signatures can be set to reject connection attempts by clients who do not have the option enabled.
- If necessary, disable concurrent connections. While it may be inconvenient for some users, it ensures that the user can only be connected once, and that multiple sessions don't remain open.
- Use an updated version of *Rconsole* (if the use of *Rconsole* is absolutely necessary). Versions of Netware above 3.12 will not send passwords across the network.
- Remove *Rconsole*, as well as any other program that should not be publicly accessible, from the sys:public directory.
- As with any operating system which has the capability of file and directory security, check to makes sure that only the appropriate users have permissions to directories. For example, a well know configuration issue in the Novell 3.1X "Sys:Mail" directory gives the group "Everyone" create permission. Because this is where user login scripts are stored, anybody could create a login script (run programs, files, etc) for other users. Disable the create permission for "Everyone" to counter this.
- Much like the recommendations for Physical Security, load "*monitor.nlm*" and set a password for it. Even if a remote intruder gets *Rconsole* access, the password locked monitor provides and extra layer of protection.
- Routinely run the *Security* utility to get information on user accounts, passwords, and rights.

Securing any server from unintended remote access is a daunting challenge for even the most diligent administrator. Recognizing the names and techniques of these various exploits and taking the appropriate countermeasures makes the security of the server much more of an obstacle for intruders.

CONCLUSION

Although the Netware 3.X line is over 10 years old, its presence (as well as other legacy systems) in networks across the world necessitates that it be scrutinized from a security perspective. A simple search on the web provides a bounty of hacking utilities.[xxvi] A great many businesses keep legacy systems on their network and feel no reason to change, and to ignore this fact is to ignore a potentially disastrous network security hole. The attacks and exploits delineated throughout this paper represent some of the most commonly documented Novell 3.X exploits, but by no means mirror a completely definitive list of vulnerabilities.

As illustrated, many of the attacks listed are thwarted with basic information security measures that are proven across the gamut of network operating systems. In the case of Netware 3.X, some of the vulnerabilities are eliminated by either patching or upgrading to Novell 3.22 (this patch was necessary for Y2K compliance, but many businesses still do not have it in place and are vulnerable to some of the attacks mentioned). Novell's upgrade recommendation to Netware 4.X, 5.X, or 6.X alleviates many of these issues by eliminating the Bindery and using the much more secure NDS, but introduces other security concerns as well. Also, by loading TCP/IP protocol support on a Netware 3.X server, you make available many of the same vulnerabilities as other TCP/IP based network operating systems (and Netware has incorporated TCP/IP more and more as it has evolved). But, it serves to reason that the techniques used to analyze current network systems have the same effectiveness on legacy systems, and constant re-evaluations of network security are always necessary. By maintaining the same diligence towards securing legacy systems that is placed on Windows and Unix systems, administrators take another step towards providing a safe and protected network.

---

[i] -Conor, p.1
[ii] -Conor (2), p.1
[iii] -Novell (1), p.1
[iv] -Novell (2), p.1
[v] -Virginia Community College, p.1
[vi] -Shi, p.1
[vii] -Phreak.org, p.1
[viii] -Mirza, p.1
[ix] -Foul/Decay, p.1-4
[x] -Nomad, p.1
[xi] -Nomad, p.1
[xii] -Novell Appnote (3), p.1
[xiii] -Infosyssec, p.1
[xiv] -Nomad (2), p.1
[xv] -Faust, p.15-20
[xvi] Mirza,p.1
[xvii] -Nomad (1), p.1
[xviii] -Infosyssec, p.1
[xix] -Novell Appnote (1), p.12-19
[xx] -Higginbotham, p.1-6
[xxi] -Novell Appnote (1) (3), p.12-19
[xxii] -Nomad, P.1

[xxiii] -Novell Appnote (2), p.4-6
[xxiv] -Ciac, p.1
[xxiv] -Novell Appnote (3), p.1
[xxiv]-Netwarefiles.com

List of References:

CIAC.org. "Novell Netware Access Rights Vulnerability" 14 October 1992 URL:http://ciac.llnl.gov/ciac/bulletins/d-01.shtml

Conor (1), Deni. "Novell Seeks to Upgrade Netware 3 Users" Network World Fusion. 01 July 2002. URL:http://www.nwfusion.com/news/2002/0701novell.html

Conor (2), Deni. "Netware 3.2 Users Mull Options" Network World Fusion. 20 March 2000. URL:http://www.nwfusion.com/news/2000/0320infra.html

Faust, Mark. "Netware Security: Closing the Doors to Hackers" 07 June 2000 URL:http://developer.novell.com/research/appnotes/2000/june/03/apv.htm

Foul/Decay, Lord. "Having Phun With Novell" 13 July 1991 URL:http://security.tsu.ru/netware/archive/novhack.html

Higginbotham, Peter. "Securing a Novell Netware Server: Preventing Unauthorized Access" 08 July 1998, rev. 14 April 2002 URL:http://www.oucs.ox.ac.uk/novell/secure/index.xml.ID=Preventing

Infosyssec, "Novell Security Information" 2000 URL:http://www.infosyssec.org/infosyssec/novsec1.htm

McClure, Stuart; Scambray, Joel; Kurtz, George. Hacking Exposed-Network Security Secrets and Solutions. Berkeley: Osborne/McGraw-Hill, 1999. 170-205.

Mirza, Fauzan. "Comp.os.netware.security faq" 22 July 1995 URL:http://www.faqs.org/faqs/netware/security/

NetwareFiles.com. 2002 URL:http://www.netwarefiles.com/categories.shtml

Nomad (1), Simple. "The Unofficial Netware Hack FAQ" 01 May 1997 URL:http://www.nmrc.org/faqs/netware/

Nomad (2), Simple. "NetWare Vulnerabilities and How to Fix Them: Step-by-step "
URL:http://216.239.39.100/search?q=cache:0gBDpJVJXaUC:razor.bindview.com/publish/presentations/files/Netware.ppt+rconsole+exploit&hl=en&ie=UTF-8

Novell (1). "Product Specific Support- Unsupported Products" 2002
URL:http://support.novell.com/products/psMenu.jsp?supp=f

Novell (2). "Netware 3.2: Upgrade to 5.1" 2002
URL:http://www.novell.com/products/netware3/eol/index.html

Novell AppNote (1)-"Protecting Your Network Against Known Security Threats" November 1997
URL:http://developer.novell.com/research/appnotes/1997/november/06/apv.htm (December, 1998)

Novell Appnote (2) Novell Appnote "Protecting Your Network Against Known Security Threats" November, 1997
URL:http://developer.novell.com/research/appnotes/1997/november/06/04.htm

Novell Appnote (3) Novell Appnote "NetWare-Specific Security Threats and Countermeasures" April 1994
URL:http://developer.novell.com/research/appnotes/1994/april/02/02.htm

Phreak.org, "Index of /archives/exploits/novell/3.x"
URL:http://www.phreak.org/archives/exploits/novell/3.x/

Shi.com. "NDS for NT Fact Book"
URL:http://www.shi.com/Global/Content/Vendors/Novell/nds/nds_facts.html

Virginia Community College, "Novell Security Best Practices"
URL:http://www.so.cc.va.us/its/Best_Practices/Novell_Security_Best_Practices.htm