Interested in learning more about security?

SANS Institute InfoSec Reading Room

Assessing and Securing a Novell Netware Environment

Any software application or operating system dominating the market place always receives more attention than one that does not. Novell has been loosing market share over the past years yet Netware is a strong, reliable product, and many IT departments still rely on it as their network backbone. Like any operating system its security must be addressed. Novell and other third party vendors offer many other products to aid the administration and responsibilities that come with network administration, which may be describe...

Assessing and Securing a Novell Netware Environment

Justin R. Northcraft, CNA
November 2002
GSEC Practical Assignment Version: 1.4b

Abstract:

Any software application or operating system dominating the market place always receives more attention than one that does not. Novell has been loosing market share over the past years yet Netware is a strong, reliable product, and many IT departments still rely on it as their network backbone. Like any operating system its security must be addressed. Novell and other third party vendors offer many other products to aid the administration and responsibilities that come with network administration, which may be described or referenced in this document. When performing a Security Assessment, it is critical not to only assess the security of any and all devices connected to the network that have an internal or external presence but to assess physical and administrative security aspects of the network and company.

This paper is designed to aid a Security Administrator and or Security Auditor in assessing the risks and vulnerabilities of a Novell Netware environment and to aid the administrator in removing, limiting, and/or monitoring those risks. Many tools used in this document are freeware; links to all tools can be found in the reference section.

NOTE: This document will reference "TID's." These are Novell "Technical Information Documents" that are located on Novell's web site.

Basic Network Security:

Good network security always starts with a well-written security policy. The appropriateness of the policy will vary from organization to organization. A security policy should contain the following:

- ✓ Determine how access will be controlled.
- ✓ Define responsibilities.
- ✓ Define rules and expectations for proper use of computer and network systems.
- ✓ Define consequences for violations against the security policy.

A security policy should also include procedures to test network security, controls and monitor the network and users to ensure all policies are followed. An awareness program should also be included to educate users of basic security issues and how to deal with an incident when one should arise. There are many books and automated tools to assist in the creation of Information Security Policies. When working with security, you should focus on these three fundamental concepts:

- ✓ Confidentiality
- ✓ Integrity
- ✓ Availability

Physical Security:

Physical security is an essential part of securing a network environment. Any server equipment not physically secure can easily be compromised and/or stolen with few ways to track the intruder. We will look further into these areas:

- ✓ Fire Controls
- ✓ Housekeeping Controls
- ✓ Access Controls

The ideal server room and telecommunications room should not contain any access points external to the building, and all doors should be self-locking. The lock should range from a cipher lock to a biometric lock; if at all possible the lock should hold an audit log of who has accessed the room and when.

There should also be an automated fire suppressant as well as a fire extinguisher in the server and telecommunications room. The fire suppressant should be a HALON 1211 type suppressant or dry pipe; there are a few that are more environmentally safe then HALON that may be more suitable for your environment as HALON is not legal for new installations [6]. As a good precaution, the server room should be kept clean at all times and anything kept in the room

(6) Ziemba, Joe, Waters, Steve "HALON The Search for Alternatives"

should be noncombustible. This includes the material used to construct any raised flooring or ceilings. As a precaution, food and drinks should be prohibited from the room. The air conditioning system for the server room should be separated from the rest of the building and should also be in a secure location.

Only essential peripherals should be connected to the systems. If at all possible, monitors and keyboards should also be removed. Any setup disks or boot disks should be removed from the system and immediate area. Your LAN should be designed carefully; cabling should be as secure as possible and use switches rather than hubs.

Novell Netware Security:

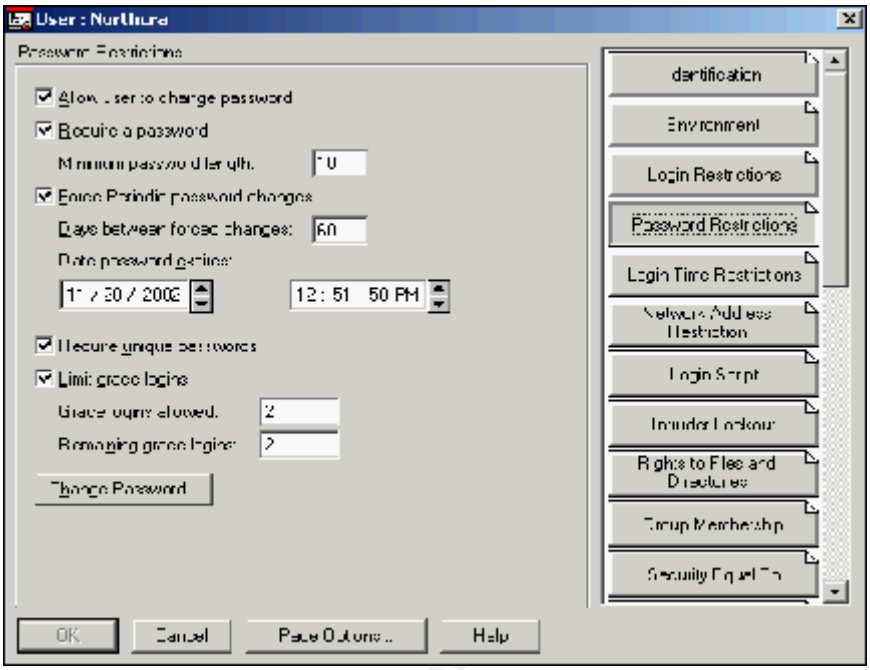
As the backbone to your infrastructure, you want to ensure you are doing all you can to keep your server secure. Netware has a directory called NDS that stores user accounts and passwords among other network settings and parameters. There are also some remote management utilities and security settings located within the operating system that will leave your server very vulnerable to attacks and compromise when not configured correctly. Once you configure and secure your system, you should continually monitor your network for any changes. Below is a listing of system settings and utilities that should be monitored and utilized.

- Administrative Account.
  The administrative account should be at least renamed, hidden and/or moved from its default location. From a security stand point, the local administrator should have two accounts, one low level user account to perform day-to-day retunes and another administrative account to perform administrative functions. The administrative account(s) should be audited on a regular basis to ensure the account has not had unauthorized use.

  To hide the administrative account, place an IRF on the object and restrict all rights.
  **Before doing this, it is recommended that you create a backup administrative account with rights to [ROOT].

- Passwords
  Traditionally, the typical password is predictable, easily crack-able and/or unchanged. At times, password management seems to be one of the hardest aspects of network security to manage. Passwords should be strong (more than 8 characters, 10 or more for administrative accounts), hard to guess (numbers, letters and special characters), and changed frequently (at least every 60 days) and only unique passwords should be used. NDS can restrict a user from using the same password. You will manage

password settings for users in NDS via NWAdmin or ConsoleONE.



In order to enforce strong password settings, you will need an additional tool, Connectotel Password Policy Manager. This tool has two parts, an NWAdmin Snap-In and a DLL that is placed on the workstation. This utility will allow you to specify the characters needed in a password (i.e. numbers, letters, special characters, etc.) For more information on Connectotel Password Policy Manager see [13] http://developer.novell.com/research/appnotes/2000/august/02/a0008023.htm

Another way to manage passwords is to use NMAS (Novell Modular Authentication Service.) NMAS utilizes token or biometric authentication methods.

Tokens are methods of authentication that is two-form-factor-based. The two forms of authentication are something you have (the token) and something you know (your pin). The user must have the specific token and have the pin number to generate a unique dynamic password each time. Tokens are a cost effective way to enforce strong password policies [12].

Biometric authentication utilizes a body part that is unique to each individual person (finger print, retina, palm scan etc.)

(12) "About Strong Authentication & One Time Passwords"
(13) "Options for Enforcing Strong Passwords"

- Console Log (CONLOG.NLM)
  The console log is a log of all events that occur on the console screen. This log should be enabled, in a secure location, and backed up on a regular basis. This log should be loaded in Loadstage 2 (just after the file system mounts in Loadstage 1) on a Netware 5.0 server and above. This should be done in order to capture any and all console commands executed before, during, and after the startup files are executed. To load this you will need to edit the INSTAUTO.NCF located on the DOS partition. To load this, utility, place the following command in the INSTAUTO.NCF file "LOAD CONLOG FILE=SYS:SECRETELOCATION ARCHIVE=YES NEXT:24:00 ENTIRE=YES"

  This command will load CONLOG. Store it in a location other than the default (default is sys:etc\console.log), archive the old logs, create a new log at midnight everyday, and capture what is already on the screen when the command is executed. This is done for forensic purposes. Assuming someone gained access to the system, this log would provide relevant data in tracking what the intruder did and who they might be.

- Remote Console Utilities (RConsole, Adrem)
  There are many ways to remotely manage a Netware server. Unfortunately, the utilities built into Netware are very insecure. Below are some utilities described in detail.

  - ✓ RConsole: RConsole can be loaded by an NLM (remote.nlm). This can be loaded by one or two ways.
    1: Type "LOAD REMOTE.NLM '*password*' ".
    2: In a startup file (AUTOEXEC.NCF) add the above line.
    The problem with adding remote with a password in the AUTOEXEC.NCF file is that if someone gained unauthorized remote or physical access to the server, they could then obtain the REMOTE.NLM password.

    There is an option to encrypt the password. To do this type "REMOTE ENCRYPT 'password' "
    **This will only encrypt the password, not the transmissions.*
    The problem with remote is that all transmissions sent to and from the server/workstation are in clear text allowing someone to sniff the session.

    Because RConsole is so insecure, it is not recommended for use.

- ✓ Adrem: Adrem has a utility called "sfCONSOLE" that will utilize NDS to authenticate a user before gaining access to the server console and encrypt the session.

Limit the use of remote console utilities as much as possible. If an intruder gains access to the console it could have detrimental effects to your network. For more information, see the "NDS Database Files" section below.

- Console Lock (SCRSAVER.NLM)
  The console lock should be used both with and without a remote console utility.
  This utility does not take the place of a secure console utility. The NLM should be loaded in the AUTOEXEC.NCF file during startup. Add the following command to the AUTOEXEC.NCF file "LOAD SCRSAVER NO PASSWORD". If you are wondering why there is a no password option, this option allows you to access the console without a password only when NDS is unavailable.

- Intruder Detection
  Intruder detection should be enabled on the container(s) containing users. The settings for this may need to vary on the organizational needs. Lockout after failed attempts should be set to three and reset account after one day. For most organizations the failed attempts setting of three is a reasonable setting. Setting the "reset account after one day" is configured so that you have time to review your logs and determine if the account locking is from a user error or an actual attack, although the standard is 15 minutes.

- File system rights
  By default, the only directories accessible by a user are SYS:LOGIN and SYS:PUBLIC. When setting file restriction rights on directories, you should also use directory quotas. Directory quotas limit the amount of data an individual user can have in that directory. If you do not use directory quotas, a potential attacker or even end-user would have the ability to fill a directory with data to the maximum capacity of the volume causing the operating system to crash. This would be a Denial of Service Attack (DOS). By using quotas you limit the risk of a DOS. You may want to consider the following types of directories: Print Queues, Mail Spool and Stores, Backup Software databases and catalogues, as well as other log files. These directories are usually available to everyone and, in many cases, overlooked by the administrator.

  Other directories to be considered:
  SYS:SYSTEM (No rights should be assigned to end-users)

SYS:ETC (No rights should be assigned to end-users)
SYS:MAIL (Is not needed, delete it)

These directories are not needed by any end-user. These are system directories only needed by the operating system and administrative users to perform administrative functions.

Using IRF's
By default, when assigning rights to a directory, those rights will flow down through all sub-directories. There may be some instances where you do not want this to happen. In that case, you would want to use an IRF (Inherited Rights Filter). An IRF will not allow but disallow rights flowing down from a parent directory. (2)

Note: You can only block the supervisor right if you have supervisor rights to that IRF. This prevents cutting supervisor level access to a part of the directory tree. In order to change the IRF of an object, you must have at least the write-property right to the ACL property of that object.

- Secure.ncf
The secure.ncf file is used to gain C2 compliance on a Novell Netware server. C2 compliance is a standard security model that ensures the system is within itself secure and has the ability to be audited in various ways.

C2 compliance is a class of TCSEC (Trusted Computer System Evaluation Criteria) from NCSC (National Computer Security Center). In order for a product, or in this case the Novell operating system, to become C2 compliant, it must be independently tested and must not fall below the standard specified in the evaluation.

In order for you to implement C2 compliance on your server, the SECURE.NCF file must be loaded at startup. For the SECURE.NCF script to work correctly, it must be stored in the SYS:SYSTEM directory, and can only be edited with an ASCII editor. To enable the SECURE.NCF file, place the following command in the AUTOEXEC.NCF "SET ENABLE SECURE.NCF=ON."
Below is a listing of the commands listed in the SECURE.NCF file and the detail to each command: (7)

  - SET ALLOW UNENCRYPTED PASSWORDS=OFF
  This command ensures that no password will be accepted during login that is not encrypted. Setting this command to ON would allow clients to login to the server without

(7) "C2 Compliance Under Novell 4.11"

- encrypting the password, thus allowing someone to sniff the password from the wire.

- SET ALLOW AUDIT PASSWORDS=OFF
  This parameter is connected to the auditing capabilities in NDS via AUDITCON. During the auditing process, the auditor has the ability to audit passwords associated with user accounts in NDS. Ensuring this parameter is set to OFF ensures that the auditor does not have access to other passwords (i.e. administrative accounts.)

- SET AUTOMATICALLY REPAIR BAD VOLUMES=ON
  This parameter instructs the operating system to automatically repair a bad volume with VREPAIR.NLM that can not be mounted upon system boot without user intervention.

- SET REJECT NCP PACKETS WITH BAD LENGTHS=ON
  This parameter ensures that the system will reject any NCP packets that have an incorrect packet length. This may cause some issues with older applications.

- SET REJECT NCP PACKETS WITH BAD COMPONENTS=ON
  This parameter, just as above, will reject any NCP packets with incorrect components. This may also cause some issues with older applications.

- SET IPX NETBIOS REPLICATION OPTION=0
  This parameter specifies the procedures that the IPX router is to use for dealing with NetBIOS broadcast messages. The following values are available for selection:

0 = No replication of type 20 IPX packets.
1 = Replication of type 20 IPX packets to all network adapters.
2 = Replication of type 20 IPX packets with two filter functions.
   a) Reverse Path Forwarding: type 20 IPX packets from the same source are forwarded only once to all network cards, even hen packets have been received from different network adapters.
   b) Split Horizon: type 20 IPX packets are not routed back into the network they were received from.
3 = Replication as for option 2, but not over long-distance links.

- SET ADDITIONAL SECURITY CHECKS=ON
  This parameter configures additional security checks which

- are not compatible with early versions of NDS. The parameters listed above are mandatory for C2 compliance. The parameters in the following section can be used for extending the security in Netware.

- # SET CHECK EQUIVALENT TO ME=ON
  This parameter forces the login process to check the NDS attribute "Equivalent To Me" upon login. In order for this to work, the NDS attributes "Equivalence" and "Equivalent" must be synchronized with DSREPAIR.NLM. Configuration of this parameter may have detrimental effects on the system's authentication speed.

- ✓ # SET NCP PACKET SIGNATURE=3
  Communication between a Novell client and server is done through NCP (Netware Core Protocol). During a communications session, data packets are transmitted between a client and server. A potential intruder can monitor and modify packets originating from a user with administrative privileges.

  NCP packet signatures were created to counter this potential threat. When a user logs into the network, a key is generated which generates the packet signatures. When the client sends packets to the server, the signature is attached. The server then checks the signature before processing the request in the packet.

  Packet signatures can be activated with this command (SET NCP PACKET SIGNATURE=3). The following are NCP packet signature levels:

0 = The server will not sign packets regardless of the client level.
1 = The server will sign the packets only if the client requests it. (Client level must be 2 or higher)
2 = The server will sign packets if the client is capable. (Client lever must be 1 or higher)
3 = The server will sign all packets and request that all clients sign, or the login process will fail.

To ensure security, the signature level should be set to three on both the server and client. To set the client signature level you will need to configure the Novell client as follows: In the system tray, right click N. Click "Novell Client Properties," "Advanced Settings." Then select the signature level from the scrollable list.

Note: Enabling NCP packet signatures will increase the network load. Ensure your network can handle the additional load before implementing this setting. (11)

- # SECURE CONSOLE
  The secure console command does the following:

  - ✓ Prevents any NLM's from being loaded from any directory other than sys:system or c:\nwserver. This will prevent an attacker from loading an invasive NLM from other directories or media.
  - ✓ Restricts entry into the OS debugger. This will prevent any alteration of the Netware Operating System.
  - ✓ Prevents any changes to the date and time of the server. (i.e. an attacker gaining access to the console, changing the time, and logging into the server with an account that has time restrictions).

  This command should be loaded in the AUTOEXEC.NCF in the following format "LOAD SECURE CONSOLE." The one drawback from the secure console command is that you are unable to remotely reboot the server. The only way to disable the command is by rebooting the server.

- ## DISPLAY NCP BAD COMPONET WARNINGS
  This parameter will display a message on the server console when an NCP packet is received with invalid content.

- ## DISPLAY NCP BAD LENGTH WARNINGS
  This parameter will display a message on the console when an NCP packet is received with an invalid length.

- NDS (Novell Directory Services)
  When end-users have the ability to browse the NDS tree without logging into NDS possible intruders do as well. This is the default setting. If an intruder browses the NDS tree, it could give them some good "foot printing" information about the network, user names, server names, etc. In order to limit this, you can remove

(11) "Using NCP Packet Signature"

[PUBLIC]'s browse right to [ROOT] on the NDS tree. This will stop unauthenticated browsing of the tree. The only side effect is it will interfere with contextless logins. Contextless logins allow a user not to enter a context on the login screen. The Novell client will then search through the NDS tree or parts of the tree to find an instance of the user name and then populate the context field on the login screen.

Bindery emulation and Backward Compatibility issues.
Bindery services (emulation) was Novell's directory structure before NDS. Bindery emulation is enabled by default on newer versions of Netware for backwards compatibility. When leaving bindery emulation enabled on a server, you leave that server vulnerable to some bindery attacks. Whenever possible, you should disable bindery emulation on any systems that do not need it. The bindery "supervisor" user in Netware 3.x is included in Netware 4.x for backwards compatibility. This user is not recognized when using an NDS utility (NWAdmin). In order to view this user, you must use a bindery utility (syscon.exe). The password set for this user is the same password as the password set for the original administrative user object. Although the "supervisor" user in Netware 3.x is a fully functional user, it's rights and privileges are limited in Netware 4.x and above. Even with limited rights, the user still has access to server configuration files leaving the system open to attacks. To disable bindery emulation, place the following string in the autoexec.ncf "set bindery context=;". Before disabling bindery emulation ensure that there are no services requiring this service on your network.

NDS Replicas
When running multiple Netware servers, it always seams to be a good idea to place a copy of NDS or a portion of NDS on another server for fault tolerance. If a replica is placed on an insecure system, this could compromise your entire network security plan. Always ensure that NDS replicas are placed on secured systems.

NDS Database Files
NDS is made up of four separate files.

Netware 4.x	Netware 5.x	Contains:
ENTRY.NDS	0.DSD	Object and Property Types
VALUE.NDS	1.DSD	Object and Property Values
BLOCK.NDS	2.DSD	Extended Property Values
PARTITIO.NDS	3.DSD	NDS Replication and Synchronization Information

There is also an 0.DSB, that file keeps track of which .DSD file does what function. All of these files are stored in a hidden directory on the sys volume, SYS:_NETWARE. This directory cannot be accessed from a user login including an administrative login. If an intruder gains access to the console prompt, they can utilize SYS:SYSTEM\NETBASIC.NLM and typing "shell." This will give the intruder access to a dos-like command prompt allowing them to copy NDS files from SYS:_NETWARE to SYS:LOGIN and copy them off of the server without ever logging into the system! From there, the intruder can crack user accounts and passwords giving them administrative access to the system. The best bets to protect yourself from someone extracting password hashes is to protect the console. Do not utilize rconsole and protect administrative accounts (i.e. strong passwords). [17][22]

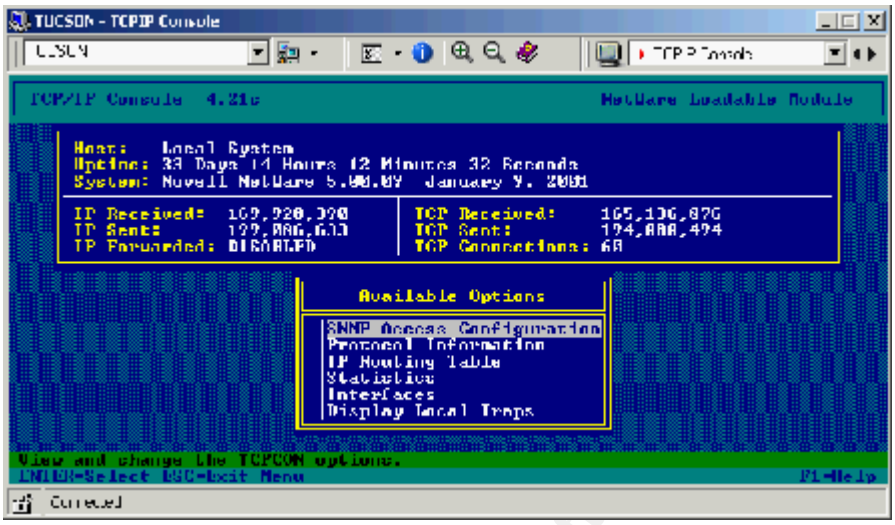
- TCP Connections and TCPCON.NLM
  Just as in Windows NT, you have the ability to close and/or shut down ports on the server. As with any server-based system, you need to have ports open in order to service network clients, although you do not want unneeded ports open as they can provide an intruder with unmonitored access to the system. Novell requires the following ports to be open. [8]

  - UDP (123): NTP Time Synchronization.
  - TCP/UDP (427): SLP Requests.
  - TCP/UDP (524): NCP Requests.
  - TCP (2302): CMD (Compatibility Mode Driver)
  - UDP (2645): CMD (Compatibility Mode Driver)
  - TCP (1677): Novell GroupWise (If running this service)

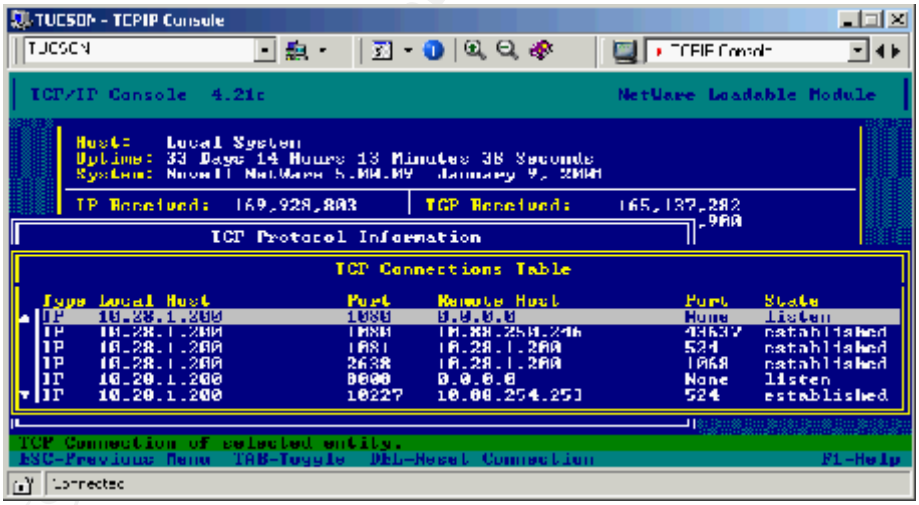
  For more information on required ports, see TID 10013531

  You can utilize TCPCON.NLM to look for open ports and current TCP connections. TCPCON is similar to the dos-based utility netstat. To use TCPCON, type "LOAD TCPCON.NLM" at the server console.

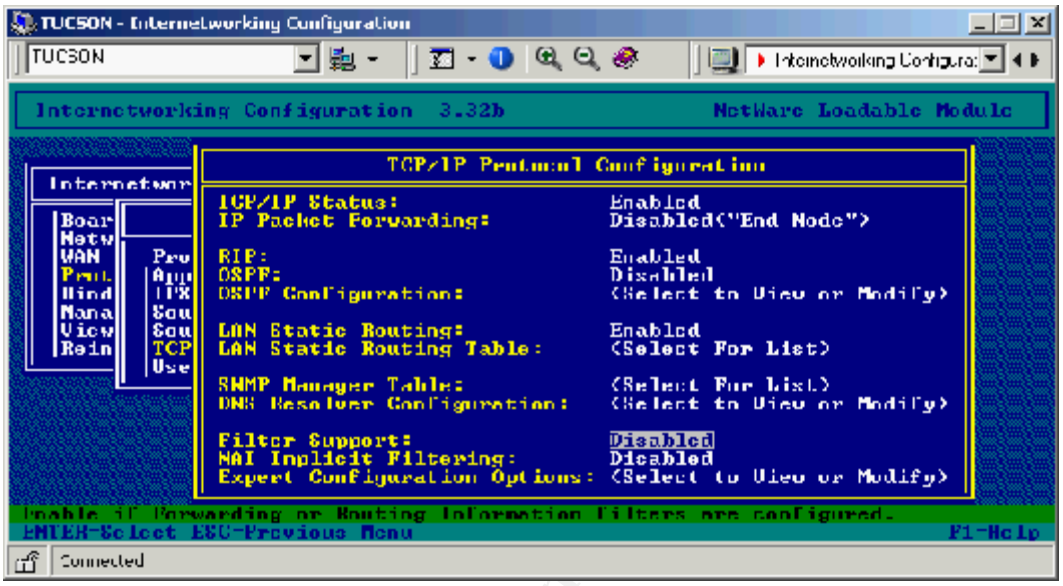
(8) "Ports and Protocols used by Netware 5.x IP (TID 10013531)"
(17) "Inside NDS"
(22) "The Hack FAQ"



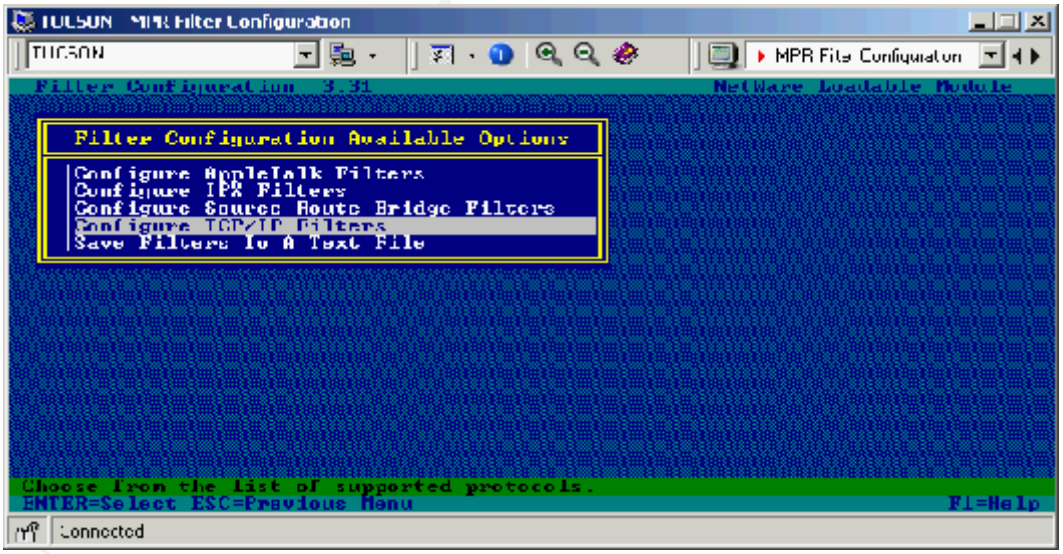
Select Protocol Information and choose the protocol, in this case TCP. Then choose TCP Connections: Select to view or modify. You will then be presented with a list of open ports and all TCP connections.



- Using FILTCFG.NLM to filter ports
  In order to filter ports in Netware, you need to use FILTCFG.NLM. Filtering ports is done to limit the services offered by the operating system. Any services that are not used and remain open on a system will most likely not be audited and, therefore, provide an open window for attacks and limited ways of tracking an intruder. Before you can filter ports, you need to enable filtering in INETCFG.NLM. Once you have loaded INETCFG.NLM, choose Protocols, then the protocol you want to filter, in this case, TCP/IP. From that screen, you can enable filtering.



To load FILTCFG.NLM, at the server console type, “LOAD FILTCFG”.



You can then choose the protocol; in this case, TCP/IP, then “Define TCP/IP Filters.” From the following screen, you can choose a filter and modify it to your needs, allowing/disallowing inbound or outbound packets on TCP/IP ports.

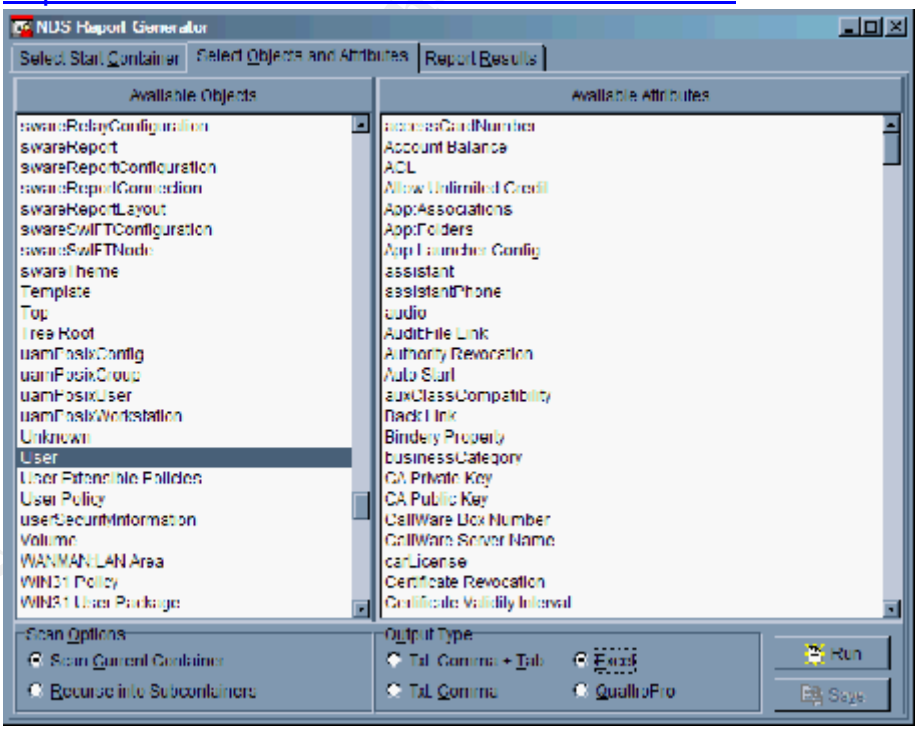
- Auditing and Log Files

  In order to be aware of events on your system, you need to audit and monitor them on a regular basis. There are various tools needed to audit and monitor events on your system. Most of these tools create logs; these logs should be kept for a minimum of three months and reviewed at least on a weekly basis, most daily.

- AUDITCON
  AUDITCON is Novell's built-in auditing program. You can utilize AUDITCON to audit various information on both NDS container information and volume information. AUDITCON is a dos based application and tends to be very cumbersome to utilize. There are other utilities that can provide the same information in a friendlier format.

For more information on AUDITCON see:
http://www.novell.com/documentation/lg/nw51/auditenu/data/a2q3x2v.html

DSReport.exe
DSReporter is a free utility available on Novell's web site. This tool extracts more information from NDS than you will probably need. DSReporter can be used to extract and compare properties and settings from various NDS objects. Probably the most useful object you can use this tool for is user objects. It gives you the ability to compare security settings, etc. from various user accounts and export the data into text or excel files. The utility can be found at:
http://www.novell.com/coolsolutions/tools/1448.html



LT Auditor For Netware
LT Auditor is a product that provides real time monitoring of NDS. This may be a good tool for larger enterprise networks as it provides advanced auditing of multiple servers across a wide area

network. More information on LT Auditor can be found at: http://www.bluelance.com

CRON.NLM
CRON is a utility that uses a script file to execute scheduled tasks for the Novell operating system. CRON.NLM runs in the background on the server and checks the script file once a minute (SYS:ETC\CRONTAB) for commands that need to be executed. Once CRON.NLM is loaded, it will keep a log of any actions it performs. The log file is SYS:ETC\CRONLOG. In order for commands to execute via CRON, you need to place the commands in the crontab file with the following syntax: [9]
"minute, hour, day-of-month, day-of-week command".
Minute = 0-59
Hour = 0-23
Day-Of-Month = 1-31
Day-Of-Week = 0-6 (The week starts with 0=Sunday)
You can use an * to specify "any" for any of the properties.

For more information on CRON.NLM, see TID 2939440.

Log Files
Below are default locations of various log files generated by the operating system.

✓	Console Log	SYS:ETC\CONSOLE.LOG
✓	System Error Log	SYS:SYSTEM\SYS$LOG.ERR
✓	Volume Log	SYS:VOL$LOG.ERR
✓	Abend Log	SYS:SYSTEM\ABEND.LOG
✓	DHCP 2.0g and below	SYS:ETC\DHCP.LOG
	DHCP Above 2.0g	SYS:ETC\DHIO.LOG contains debugging output from DHCPIO.NLM SYS:ETC\DHCPMAIN.LOG contains output from DHCPSRVR.NLM SYS:ETC\ADDRVALD.LOG contains information about IP lease expiration For more information on DHCP logging see TID 2924836 [10][14]
✓	Border Manager Proxy	SYS:\ETC\PROXY\LOG\HTTP\COMMON SYS:\ETC\PROXY\LOG\HTTP\EXTENDED
✓	Web Server	SYS:\WEB\LOGGS\ERROR.LOG SYS:\WEB\LOGGS\ACCESS.LOG
✓	FTP Server	FTP log files are specified in the config file.
✓	CRON.NLM	SYS:\ETC\CRONLOG
✓	Backup	Backup logs are specific to the application.

(9) "CRON.NLM Server Utility V1.7 (TID 2939440)"
(10) "DHCP Server Log Files for version 2.0i (TID 2924836)
(14) Dudenhoeffer, Patti. "Critical Security Skills / Novell"

- Anti-Virus
  To date, there have been very few viruses directed towards Novell. Some may question, "Why do I need Anti-Virus software on a server that may rarely receive a virus?" The answer is because most likely that Netware server is servicing operating systems that have a tendency to have viruses, and could store a virus on a server volume causing the virus to spread to unprotected computers. There are several different anti-virus applications for Netware servers; the two most popular are Netshield from Network Associates and InoculateIT from Computer Associates. Included in your Information Security policy, you should have a virus policy. Virus policies should not be an annoyance to the system administrator and end-users. A virus policy should be in place to prevent the introduction of a virus to a network.

  These policies should be tailored to your organization's needs, but consider the following guidelines when creating virus policies: [15]

  - ✓ Limit user intervention
  - ✓ Transparent operation
  - ✓ Automatic updates
  - ✓ Central reporting
  - ✓ Immediate notification
  - ✓ Tamper detection or prevention

- Patches
  As a part of ensuring your system is secure; you need to keep up to date on software patches for all products listed. There are free and payable services available that will inform you of patch releases for specific software applications and operating systems. For Novell products, there is a simple listing on their web site listing all Novell applications and current patch releases. Novell's list is available at: http://support.novell.com/produpdate/patchlist.html

- Display Login Banner
  Login banners are used for legal disclaimers when accessing Information Systems. They should be in place to notify both authorized and unauthorized users of several things. When creating login banners you may want to consider the following:

  - ✓ A short summary of what is considered proper use of the system.
  - ✓ That the system may be monitored to detect improper use.

- ✓ That there is no expectation of privacy while using the system.

If you do not have a login banner at any entry point into your network, an intruder that caused damage to the system could then use that as a defense saying they did not know what system they were accessing and did not know the appropriate use of the system. (16)

- Default user templates
  For easier administration and standardization of your user accounts, you may consider using user templates. You can specify all security settings in the user template so that you do not need to specify the settings on each individual account that you create.

- Backup procedures
  Backup policies will vary for every organization. Routine backups must be apart of any organization. A backup policy should be included as apart of the organization's Information Security policies. This part of the policy should be configured to your organization's specific needs. Backups can be made on various types of media at various speeds. There are various backup applications to perform backups of your system. Several third-party applications are available that provide advanced backup features. Some third party tools are; Backup Exec from Veritas or ArcServe from Computer Associates. Some things to consider when creating a backup policy:

  - ✓ Full daily backups (if possible).
  - ✓ Keep a recent, full system backup off site at all times.
  - ✓ Keep monthly backups for as long as possible. (Some organizations are required by law to keep backup's of data for 7 – 10 years.)

  Keep in mind the purpose of backups is to restore functionality of data to a computer system. Backup logs should be checked daily, and backups should be tested on a regular basis to ensure their integrity. One thing your company may want to consider is to have a BCP (Business Continuity Plan). The purpose of a BCP is to relocate a restore operation of a company in the event of a disaster. An example of this is the companies that were affected in the 9/11 attacks to the World Financial Center in New York City. The companies that survived those attacks had a BCP in place and utilized it. There are many tools and third-party companies that can provide assistance in creating a BCP.

(16) "Creating Login Banners"

Securing the Workstation

Securing workstations tends to be one of the last security issues addressed when securing a network. If a workstation should become compromised, it could easily be used to compromise network servers. Because of the variety of management utilities and workstation operating systems, I will focus on the most popular in a Novell environment Microsoft Windows 2000 Professional and ZenWorks for desktops.

Windows 2000

Windows 2000 is again like any operating system. It has security issues that need to be addressed. I will only cover several issues with Windows 2000 but there are links below that can provide you with assistance in securing your Windows 2000 desktops.

Windows 2000 has a database called SAM (Security Accounts Manager). This file can be compared to NDS. The SAM database contains user name and password hashes in either an encrypted or in some cases, unencrypted state for Windows 2000. If this file is compromised, the password hashes can then be cracked, thus possibly allowing an intruder to gain access to a Novell Administrator's password through Windows 2000 and have full administrative control of the Novell Network! Below are some things you can do to help prevent this type of attack.

- ✓ Format all Windows 2000 partitions in NTFS.
  (NTFS partitions are only accessible from Windows 2000)

- ✓ Configure a CMOS password and disable booting from floppy and CD.
  (There are utilities available to boot from floppy and access an NTFS partition from dos, allowing an intruder to copy the SAM database to floppy!)

- ✓ Ensure SYSKey protection is enabled. SYSKey encrypts the SAM database with 128bit encryption. NOTE: SYSKey is implemented with all of the latest Operating System Serivce Packs.
  (See Microsoft article Q143475 for more information on SYSKey.
  http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q143475&)

- ✓ SAM Cleanup:
  Every time an ERD (Emergency Repair Disk) is created a copy of the SAM database is copied to "%systemroot%\repair." After creating an ERD, make sure this directory is clear of all files. An intruder could gain access to this directory and again copy the SAM database.

- ✓ DLU (Dynamic Local User):
  Netware ships with the ZenWorks starter pack software. This is not the full version of ZenWorks, but it does have some useful features like the DLU. The purpose of DLU is to manage Windows desktops from a Novell network. The DLU will pull policies from the NetWare server to the local desktop and apply them. An added feature from this is that when a user logs out of the workstation, the user account is then removed, leaving no accounts for an intruder to gain access to.

References:

(1) Chase, Philip. “Securing Netware Systems.” 5 March 1996.
URL: http://grove.ufl.edu/~pbc/securing-nw.html (October 2002)

(2) Moffat, Iain, Chase, Philip, Sallot, Ken. “Best Practices for Netware Security.” 20 October 1999.
URL: http://grove.ufl.edu/~pbc/itsa/netware-security-slides.ppt (October 2002)

(3) Novak, Kevin. “Securing Your Netware Environment.” 16 October 2000.
URL: http://secinf.net/info/nw/novak/1120ws12.html (October 2002)

(4) Higginbotham, Peter. “Netware Security”
URL: http://www.itssg.ox.ac.uk/training/securityweek2001/NovSec.ppt (October 2002)

(5) Boyd, Michael. “NetWare Auditing and Security”
URL: http://www.giac.org/practical/michael_boyd_gsec.doc (October 2002)

(6) Ziemba, Joe, Waters, Steve. “HALON The Search for Alternatives” 24 September 1995.
URL: http://www.halcyon.com/NAFED/HTML/Halonalt.html (October 2002)

(7) “C2 Security Under Novell 4.11” July 1999
URL: http://www.bsi.bund.de/gshb/english/s/s4102.htm (October 2002)

(8) “Ports and Protocols used by Netware 5.x IP (TID 10013531)”
URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10013531.htm (October 2002)

(9) “CRON.NLM Server Utility V1.7 (TID 2939440)”
URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2939440.htm (October 2002)

(10) “DHCP Server Log Files for version 2.0i (TID 2924836)
URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2924836.htm (October 2002)

(11) “Using NCP Packet Signature”
URL:
http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/sos__enu/data/hc66y4qi.html (November (2002)

(12) “About Strong Authentication & One-Time Passwords” 25 October 2002
URL: http://www.bnl.gov/cybersecurity/strong_auth.asp (October 2002)

(13) “Options for Enforcing Strong Passwords”
URL:
http://developer.novell.com/research/appnotes/2000/august/02/a0008023.htm
(October 2002)

(14) Dudenhoeffer, Patti. “Critical Security Skills / Novell” 21 March, 2002
URL:
http://developer.novell.com/research/appnotes/2000/august/02/a0008023.htm
(October 2002)

(15) “Establishing Virus Prevention Policies”
URL: http://www.cai.com/virusinfo/policies.htm (October 2002)

(16) “Creating Login Banners”
URL: http://www.ciac.org/ciac/bulletins/j-043.shtml (October 2002)

(17) “Inside NDS” 12 May 1999
URL: http://www.nmrc.org/pandora/inside.txt (November 2002)

(18) Anonymous. Maximum Security Second Edition.
SAMS Publishing, 1998. 417 - 435

(19) McClure, Stuart, Scambray, Joel, Kurtz, George. Hacking Exposed.
Osborne/McGraw Hill, 1999. 169 - 205

(20) McClure, Stuart, Scambray, Joel, Kurtz, George. Hacking Exposed Second Edition.
Osborne/McGraw Hill, 2001. 265 - 303

(21) Chirillo, John. Hack Attacks REVEALED.
Wiley Computer Publishing, 2001. 649 - 667

(22) “The Hack FAQ” 6 September 1999
URL: http://www.nmrc.org/faqs/hackfaq/ (November 2002)

Last Updated: May 23rd, 2017

Upcoming SANS Training

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

SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Thailand 2017	Bangkok, TH	Jun 12, 2017 - Jun 30, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MNUS	Jun 19, 2017 - Jun 24, 2017	Live Event
DFIR Summit & Training 2017	Austin, TXUS	Jun 22, 2017 - Jun 29, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, FR	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Stockholm 2017	OnlineSE	May 29, 2017 - Jun 03, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced