GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Michael S. Boyd
GSEC v1.2f
NetWare Auditing and Security
January 16, 2005

Overview

The networking world is very insecure place as of late, and it seems your level of market share has a little (or a lot) to do with your level of vulnerability. NetWare, it seems, is slowly being phased out of the corporate NOS environment. One sign could be the sparse exploit and vulnerability list. The recent GroupWise exploit was the first in a long while that targeted Novell. Novell always tried to make their NOS a little more secure out-of-the-box. They were forward thinking enough to realize security was an issue from the start. Unfortunately their marketing department couldn't paint the picture well enough for the rest of the IT managers.

Realizing Novell's foothold is slipping, there are still plenty of shops out there running NetWare who need to take steps to ensure there servers are more secure. This paper will cover those steps and provide a list of tools that can help make those Novell environments a bit more secure. Enhancing Novell security doesn't take too much work, and it can help you sleep a little better at night.

Enhancing security on a default server install

The first step in securing your server should be to physically secure the machine. One added level would be if you could also lock the rack that the server resides in, and only allow trusted engineers the keys. If an attacker can get to the server, they can get to the console and bring your network to its knees.

You want to keep the console secure at all times. In NetWare 4.x and below you had to go into the **monitor** utility and select the **Lock File Server Console** option to lock the console. In newer, 5.x, versions of NetWare you no longer lock the console. Instead you run the **scrsaver.nlm**, which starts the NetWare snake screen saver. To disable the screensaver, Novell now checks NDS rights, so you must login with the appropriate user.

Here are some additional steps that should be taken to improve your NetWare servers security.

1. Rename and/or hide the Admin account
    1. One of the first things that should be done after creating your server is renaming, and maybe even hiding, the admin account. (*Note: before hiding the account, I would recommend creating another user account with trustee rights to the container, or the* [root]*, and security equal to the admin account. You never know when you may forget the name or the password of the account once you change it.*) Hiding the account is done by placing an IRF (Inherited Rights Filter) on the account and restricting all the rights. All you have to do to view the hidden account is login as the new admin equivalent account you created.
2. Enable intruder lockout on the container

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1. Right-Click on the container and select details
2. Select the Intruder Detection tab from the right hand side
3. Configure settings for:
4. Lockout after failed attempts = 3
5. Reset account after = 15 minutes

3. Create a default user template
    1. Creating a user template will make the administrative tasks of enforcing account security a little easier.
    2. To create a user template
        1. Highlight the container you want the object created in
        2. Right-click on the container and select create
        3. Scroll down and select user template
        4. Name the template, check the box to display object after creation, and select OK
        5. A recommendation for some of the settings is as follows: (*note: These recommendations can be adjusted to fit your organizational needs and policies.)*
            1. Require Password = Yes
            2. Minimum Password Length = 8
            3. Require Password Change = 90 days
            4. Require Unique Passwords = Yes
            5. Limit Connections = 1

Pros and Cons of Secure Console

Secure console is another way to enhance your servers security. If your server has been breached and the attacker gains access to the system console, having secure console enabled will help minimize their attack. Secure console does the following; it removes DOS paths from the search path; it allows only NLMs from the search path to be loaded; it disallows the setting of certain SET parameters; it prevents the server date and time from being changed; and it prevents keyboard entry into the operating system debugger. This command does NOT remove the requirement that the server console be physically secured.

The biggest con is that you can't remotely reboot the server if you're on call.

Rconsole

Rconsole and **Rconj** are great utilities from an administrative standpoint, but not very good when it comes to security. They both give you the ability to remotely control a server, which is extremely useful if your server happens to be in a different building, or state, or country. The problem is they offer only unencrypted connections to the remote servers. The password, as well as other commands are sent in clear text, which can be sniffed off the wire with most any packet capture application.

One way to enhance security is to encrypt the password using the **remote encrypt** command. Follow these steps to encrypt your rconsole password:

1. unload **RSPX**
2. unload **REMOTE**
3. load **REMOTE** *password*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

*4.***REMOTE ENCRYPT** *password*

When you are finished typing in your password, the server will ask if you want the encrypted password put in the **autoexec.ncf**. You also have the option of saving it to another file and then calling that file from your **autoexec.ncf**. This can also be viewed as another layer of security, albeit security through obscurity, it's still one more step an attacker would have to go through to gain access to your server console.

You can hide it in a couple of ways:

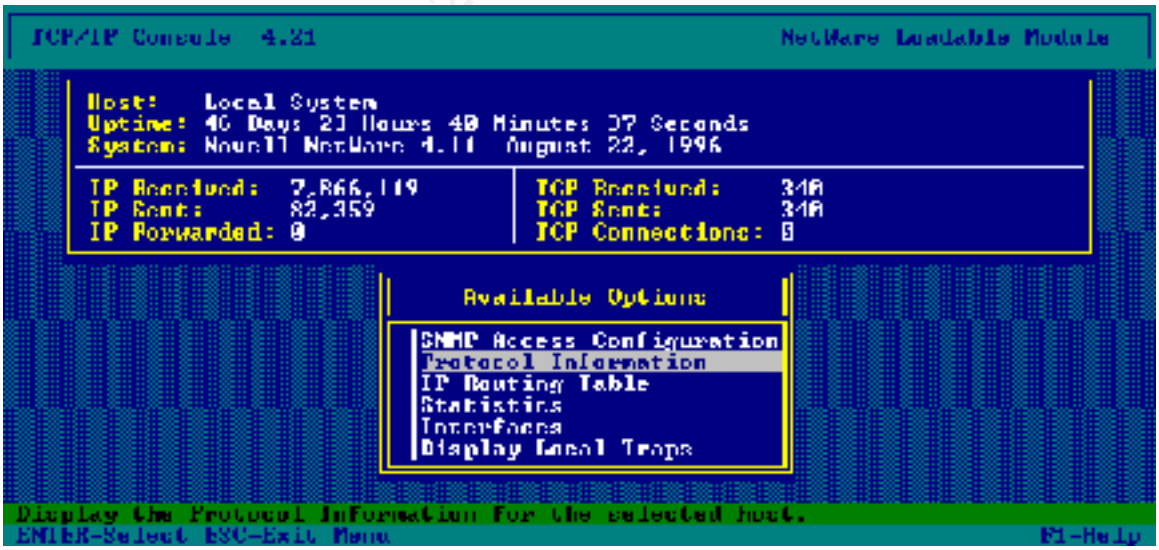
1. Cut the commands out and append them into another .ncf that gets called from the **autoexec.ncf**
2. Create a generic .ncf (which resembles a harmless system ncf or command) and append the rconsole commands into it.

You can also use some third party utilities for secure communications between servers. AdRem Software makes **sfConsole**, which is an rconsole like application that uses an nlm on the server and checks NDS for rights to the server. They make a freeware version of this application that doesn't have as many features, but still uses NDS to authenticate your rights for access to the server.

Inetcfg and Filtering

Out-of-the-box the only way to filter ports is to run **inetcfg** and enable filtering. Novell requires some ports be open for various services, but the rest should be closed down for your protection. You can check for open ports a number of ways, but we'll cover probably two of the more common ones: **tcpcon** and **nmap**.

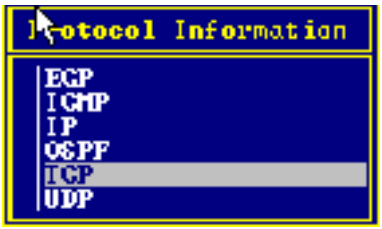
Using **tcpcon** to check for open ports



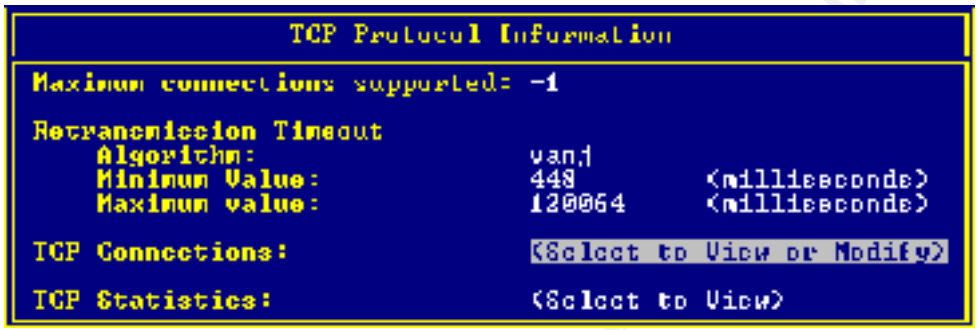
At the server console type: **LOAD TCPCON**

Select **PROTOCOL INFORMATION**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Select **TCP**



Select **TCP CONNECTIONS**



This will allow you to see a list of your open ports using Novell's built-in **TCPCON** utility. As you can see from the screenshot, there are a few ports that need to be closed.

Using **Nmap** to check for open ports

- **Nmap** is a freely available network-mapping tool that you can obtain from www.insecure.org. **Nmap** is available for a number of different platforms, so you should be able to find a version for one that you are currently using in your organization. **Nmap** has a plethora of switches and arguments you can use to fine-tune your scanning. I would highly recommend reading the man pages and documentation to get an understanding of the switch usage.
- The command I use the most is:
  - **nmapnt -sS -oN *filename.txt servername*** (***ip address*** will work instead of ***servername***)
    - **-sS** tells nmap to do a stealth syn scan
    - **-oN** tells nmap to pipe the output in human readable format to ***filename.txt***
    - If you want to scan all the ports you can add the ***-p 1-*** switch.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- When the command is finished you can pull up the text file in any text editor and it should look similar to this:

```
# Nmap (V. nmap) scan initiated 2.53 as: nmapnt -sS -oN file.txt server
Interesting ports on yoursite.com (x.x.x.x):
(The 1520 ports scanned but not shown below are in state: closed)
Port       State       Service
7/tcp      open        echo
9/tcp      open        discard
19/tcp     open        chargen

# Nmap run completed at Mon Sep 10 12:57:49 2001 -- 1 IP address (1 host up)
scanned in 3 seconds
```

- If you have a number of servers at your site, you can write a script to scan all the servers from a list, and write the output to a text file. Here's a copy of the script that I use:

(*Using Windows 2000, I just save this as nmap.cmd and run it with a .lst file that has my server names in it.)*

```
:begin
set cnt_1=
set list=%1
set server=

set list=d:\lists\%list%.lst

for /F %%j in (%list%) do set /a cnt_1=cnt_1+1

for /F %%i in (%list%) do call nmap.cmd part2 %%i %cnt_1%

:Part2

shift
set /a cnt_1=%3
set server=%1
set date=%date%
cls

md %date%

nmapnt -sS -oN d:\nmapnt\%date%\%server%ports.txt %server%

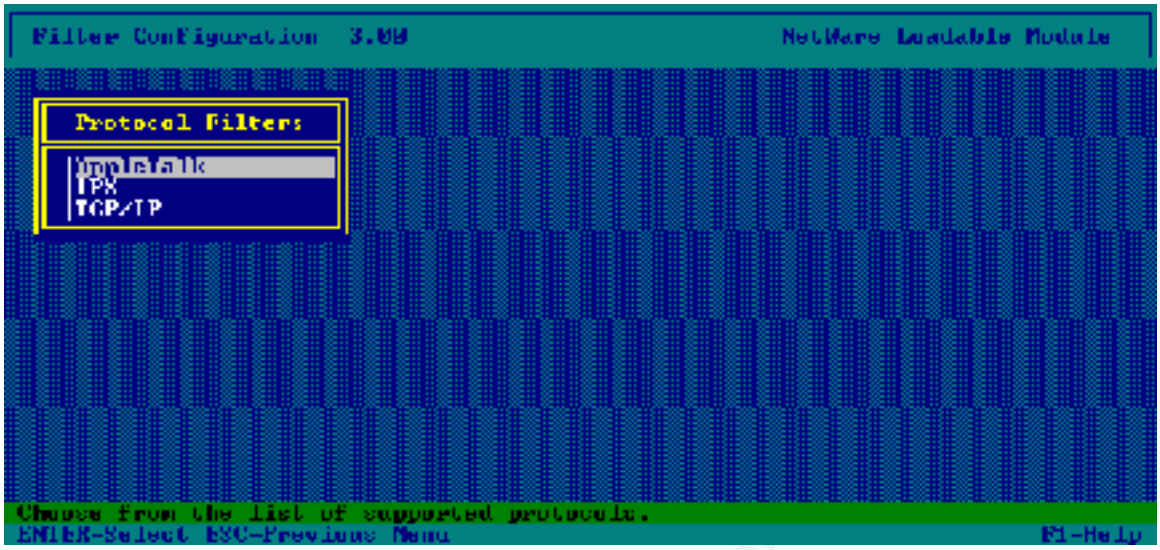
:end
```

© SANS Institute 2000 - 2002, Author retains full rights.

Filtering ports with **filtcfg**

Filtering ports is accomplished using the **filtcfg.nlm.** The following screen shots can be used to help understand the text from **Limiting the Exposure of a NetWare Server in an IP World** by Dana McLaughlin.

When you load **filtcfg**, the following screen appears:
Select **TCP/IP** from this screen.



Select **Define TCP/IP filters** from the next screen:



Select **Packet Forwarding Filters**



Enable the filter, then select which packets(ports) to deny or permit, depending on how you setup the filter, from the **Filters:** submenu.



Auditing out of the box

Enabling Auditing

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Novell's auditing utility allows you to audit DS events or you can audit by user. Once you enable auditing and choose which events to audit, you can start building your audit trail. If you go back and decide there are other events you wish to audit, you can enable them at a later time. The only thing you have to remember is that you won't get any data on an event until you enable that event. So, if you're looking to audit an event, make sure you do it when you enable auditing, otherwise the audit trail won't be there for you if you need it.

You can audit a great number of DS events, some of which I've listed below:

- Add member to group property
- Add partition
- Add replica
- Change password
- Change security equivalence
- Disable user account
- Enable user account
- Intruder lockout change
- Log in user
- Log out user
- Rename object
- Rename tree
- User locked

The first thing that should be done is the creation of an auditor account. The auditor account should not necessarily be used by a network administrator, but more likely someone from a different department. You may even choose to create a separate container to house the auditor account and audit file objects. Either way, the auditor account will need the following to be able to audit:

- Browse right for containers to be audited
- Drive mapped to audit program directory (should be SYS:PUBLIC)
- Search drive mapped to SYS:PUBLIC
- Browse object right and File Scan directory trustee right to SYS:PUBLIC

The utility to enable auditing is called **Auditcon**, and is usually located in SYS:PUBLIC. When you run the **Auditcon** utility, you will have the option to enable volume, container, or external auditing.

Using custom scripts

Administrators on a budget can build their own auditing scripts using the **NLIST** command. The following settings, at a minimum, should be checked:

-no password
-user doesn't have to change password
-require unique password
-accounts with admin equivalency
-last login older than x days (refer to your security policy)
-accounts that are disabled

© SANS Institute 2000 - 2002, Author retains full rights.

I created my own batch file for this, before I found out that Novell actually put out a **TID**, which listed the commands. The document is **TID# 10024879** and I've provided the commands below. All you have to do is cut and paste them into a file then just remove the ones you don't want, change a few server and file names, and change the last login and account expiration dates, and you should be set to do some auditing.

(Don't forget to login with admin rights and to change your context to [root] or wherever you want to start auditing from. You can use the /S switch at the end of any command line to search down the tree.)

One other side note, you may want to group the nlist commands together instead of putting them all in on file. Depending on the size of your tree, the file could be very big. I used my configuration in the following example, but feel free to change it for your needs.

```
MD C:\AUDITNW
CX .top_level
NLIST User SHOW "Date Password Expires" >>C:\AUDITNW\passexp.TXT
NLIST User WHERE "Date Password Expires" LT 09/04/2001
>>C:\AUDITNW\passexp.TXT
NLIST User WHERE "Full Name" NEXISTS >>C:\AUDITNW\fullnm.TXT
NLIST User SHOW "Require a Password" >>C:\AUDITNW\reqpass.TXT
NLIST User WHERE "Require a Password" NEXISTS >>C:\AUDITNW\reqpass.TXT
NLIST User SHOW "Account Disabled" >>C:\AUDITNW\acctdis.TXT
NLIST User WHERE "Account Disabled" NEXISTS >>C:\AUDITNW\acctdis.TXT
NLIST User SHOW "Account Has Expiration Date" >>C:\AUDITNW\acctexp.TXT
NLIST User WHERE "Account Has Expiration Date" LT 09/04/2001
>>C:\AUDITNW\acctexp.TXT
NLIST User WHERE "Last Login Time" NEXISTS >>C:\AUDITNW\lastlogt.TXT
NLIST User WHERE "Last Login Time" LT 09/04/001 >>C:\AUDITNW\lastlogt.TXT
NLIST User WHERE "Security Equal To" EQ .admin.context >>C:\AUDITNW\seceq.TXT
NLIST User WHERE "Security Equal To" EQ .server.context /S
>>C:\AUDITNW\seceq.TXT
NLIST User WHERE "Security Equal To" EQ .server_volume.context /S
>>C:\AUDITNW\seceq.TXT
NLIST Organization SHOW "Object Trustees (ACL)" /S >>C:\AUDITNW\AUDIT.TXT
NLIST "Organizational Unit" SHOW "Object Trustees (ACL)" /S
>>C:\AUDITNW\objtrst.TXT
RIGHTS /T /S >>C:\AUDITNW\rights.TXT
```

Running your audit scripts is one thing, just be sure to go back and fix any discrepancies your audit may have found. It would be a good idea to run the scripts daily so you can so you can keep a good eye on changes. You may just want to create a number of smaller scripts, that way you can choose which ones to run on which days.

Setting Up a Virus Scan Solution for your Server

One thing that needs to be discussed is a virus solution. Using the defense-in-depth strategy, it's important to have a second layer of virus protection on the server. You may already have a solution for the desktop, but it's essential to have the added protection of a server-based solution. You may even want to mix and match, have Norton on your desktop and McAfee on your servers, or vice versa. Novell used to bundle Inoculan with their NOS, but now it is owned by Computer Associates.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

McAfee and Norton both allow you to manage virus updates from a single location. You have a choice of downloading the updates yourself, and then letting your servers deploy them, or letting your servers download the updates and automatically deploy them. Whichever way you choose, it would probably be wise to check for updates daily, especially with the likes of 'Nimda' running around our networks.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

How to delete a hidden object
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2943415.htm

AdRem Free Remote Console
http://www.adremsoft.com/freecon/index.htm

SECURITY.EXE equivalent information in
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10024879.htm

Securing Your NetWare Environment
http://secinf.net/info/nw/novak/1120ws1.html
http://secinf.net/info/nw/novak/1120ws12.html

Basic Novell Netware Security
http://www.sans.org/infosecFAQ/novell/netware_sec.htm

Limiting the Exposure of a NetWare Server in an IP World
http://www.sans.org/infosecFAQ/novell/exposure.htm

How can the RCONSOLE password be encrypted?
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10027169.htm

Configuring Auditing
http://www.novell.com/documentation/lg/nw51/auditenu/data/hwxoeyp3.html

Creating the Auditor Account
http://www.novell.com/documentation/lg/nw51/auditenu/data/hwput700.html

Auditing Procedure
http://www.novell.com/documentation/lg/nw51/auditenu/data/h0wafpf7.html

Enabling Volume Auditing
http://www.novell.com/documentation/lg/nw51/auditenu/data/hvgqz15q.html

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002, Author retains full rights.