

## **INTRO**

Hello Everyone!

I am Michael Houst.

I know you were all expecting Mike Wiggin to be giving this presentation. However, due to a grave family illness, he wasn't able to make it. Mike asked if I could deliver this for him. So you have a Mike, just not the one you were expecting.

For those of you who don't know me, I fill the position of Database Administrator at the Northeast Health Care Quality Foundation; the QIO for Maine, New Hampshire, and Vermont.

Although DBA is my position; my duties and responsibilities are considerably more varied. I also perform tasks as a Novell NetWare Administrator, IS troubleshooter, PC and network modification, repair, and upgrade technician. And I also advise on security measures as relates to Computer Information Management Systems within the Foundation.

As the title of the presentation states, I am here to talk about ways to secure your database using tools in Novell Netware and Microsoft Access.

Let's start on the outside with

### **SLIDE 1**

Novell NetWare Security.

I'm going to walk through setting up most of the security options available in Novell NetWare. For most of you I hope this is just a refresher. For the rest, I hope you come away with a few more ideas on how to better protect our beneficiaries' personal information.

### **LEAD IN**

First, a quick check on everyone's background.

How many of you have actually hacked a Novell system? I mean sit down and gain access, administrative or even user-level on a system you weren't authorized to use/or had accidentally lost all access to? This includes sitting down at a person's system while they are logged in, but not there, and don't know you're using their station. Raise your hands. Keep you hands up.

How many of you know HOW to hack a Novell system? Raise your hands.

How many of you know a Novell System CAN be hacked? Raise your hands.

Novell systems can be hacked. You can make it hard for hackers, or you can hand them the keys to your system.

## **SLIDE 2**

What is a security risk?

Simple definition: A security risk is the potential for un-authorized data access, corruption, or loss.

## **BODY**

First of all, I want to make sure that you all remember that there is no such thing as perfect security. The concept of security is to add enough layers of difficulty such that the cost (in time, money, or processing power) of getting the information through unauthorized means exceeds its value, or your liability costs. It does a drug company absolutely no good to steal a copy of your beneficiary's data if by the time they break the encryption on a file, all the bennies are dead.

## **SLIDE 3**

There are two halves of the Information Security package; and you need to have both halves: Operational Security, and Physical Security.

## **SLIDE 4**

Operational Security is what you and your people do. It encompasses policies regarding how things are going to be done. The use of no lone zones (employees not being allowed to work on something without supervision oversight), no outside personal floppy disk/CDs in the office, no paper records outside the work area, shredding of all employee information before disposal, the policy of no discussion of security measures in either public locations or with unnecessary personnel, these are all examples of Operational Security. They all serve to reduce temptation and opportunities for people to make unauthorized use of data and information.

## **SLIDE 5**

Physical Security is what your company has. Physical security has one objective: slow down and discourage thieves and saboteurs. Time is the major factor. You have physical security measures to slow up intruders, and raise the alarm to law enforcement and management. You have software and operating system security to slow up intruders, raise the alarm, or at least track possible intrusion attempts. Door and window locks, alarm systems, guards, software and operating system security all serve to slow the crooks down and give you a chance to either move/better secure your data, and catch the crooks in the act.

Without good physical and operational security measures in place, it doesn't matter what operating system you use; it can and will be cracked. This includes Microsoft OS's, AIX, Unix/Linux, and Novell Netware.

## SLIDE 6

Novell Netware does a pretty good job of giving you good operating system security. Account Security, Access Rights, Workstation security, Server Console security, Accounting, and Backup.

## SLIDE 7

### Account Security:

- **Intruder Detection**
  - **Login Restrictions**
  - **Password Restrictions**
  - **Login Time Restrictions**
  - **Workstation Security**
- 

Lets take the first one,

- **Intruder Detection**

Using NW Admin and starting from the root,

## SLIDE 8

Select the Organization Container.

## SLIDE 9

And right button click on the Organization container, then select, Intruder Detection.

## SLIDE 10

You can set an intruder detection option to alert you to when someone has a suspicious number of logins: anywhere from 0 to 999. **I don't suggest you set this number any higher than the number of grace logins.** We'll get to grace logins in a minute.

You can also set a time frame for these attempts to be made; from 0 up to 104 days, 7 hours, and 39 minutes. **I suggest setting this to 1 hour. When I start seeing 5 bad attempts every hour, I'm going to wonder what's going on.**

And you can set the system to lock that account out for 0 up to 104 days, 7 hours, and 39 minutes if they exceed the number of login attempts. **I have ours set to 1 day. Obviously this gives them a couple of attempts over weekends or holidays. However, this lets me catch it that day, if a person really forgets their password, and slows any intrusion attempts, hopefully enough for the person to get discouraged and leave.**

Intruder detection can be set at both the Organizational level, and at the Organizational Unit level.

---

### - **Login Restrictions**

Setting login restrictions,  
starting at root, select organization,

#### **SLIDE 11**

then organizational unit

#### **SLIDE 12**

And then right click on the individual account.

#### **SLIDE 13**

And right button click on the individual account

#### **SLIDE 14**

And select the Login Restriction button, which brings us here.

#### **SLIDE 15**

User Accounts can be enabled and disabled here.  
User accounts can be given expiration dates and times.  
And User Accounts can be limited in the number of workstations they can be logged in at and connected to the network.

---

Now lets select,

### - **Password Restrictions**

#### **SLIDE 16**

You can set the account to allow the user to change their own passwords. **This is a good idea as it reduces work for the administrators, removes the possibility of accusing an admin of logging in as that person and causing trouble, and allows the user to know when an admin has had to reset their account. This is a bad idea because most users are complete incompetents when it comes to making good passwords.**

You can set user accounts to require a password. I'm not sure why Novell even makes this an option, it ought to be required no matter what.

Passwords can be aged to require a new one between 1 and 365 days.

They can be required to be unique passwords. I recall one Novell instructor saying that NetWare remembers the last eight passwords used; so I suppose if someone were foolish enough to do so, they could change their password eight times in a row to get the old one back. **I recommend having the Require Unique Passwords be checked.**

You can limit the number of grace logins to between 1 and 200. **Most people set it to 3 to 5.** 1 is too little; and a limit of 200 is ridiculous.

Who knows how to make a good, strong password?

A good strong password is going to be hard to guess, easy to remember, at least 8 characters (mixed alphabetic, numeric, & symbol) in length.

Novell Passwords must be at least 1 character in length; and a mandatory minimum length can be assigned. **A length of 5 is okay, 6 good, 8 is better**, and you can go as high as 128; however, I don't suggest using the first 128 characters of the Gettysburg Address, as "Four score and seven years ago our fathers brought forth, upon this continent, a new nation, conceived in Liberty, and dedicated to the proposition that" is way too long to type every time you want to log in.

---

Now select the button

- **Login Time Restrictions**

### **SLIDE 17**

Users can also be limited to certain days and times of the week that they can use the system; and are locked out of the system at all other times. Generally the best setting is to allow people to log in an hour earlier than they normally start work, and work up to 2 hours later than the normal end of the work day. With weekends completely blocked out. You just have to toggle each of the boxes on or off, and you can use the mouse to select multiple boxes at once.

---

Users can also be limited in the actual hardware systems they can log in on. And this falls into the

- **Workstation Security Restrictions**

But in order to do that, we need to know which workstation we're talking about. Here's one way you can find a system's network address.

In NW Admin, under root, organization, open the ZENWORKS Organization Unit container. You should see the Win95-98 Workstation Package.

### **SLIDE 18**

Right click and select details and this is what you get.

### **SLIDE 19**

If it's not on, select the Workstation Import Policy block.

#### **A word of warning:**

**Only leave this on for as long as is necessary to import new workstations, then toggle it back off.**

**If you leave it on, you will start seeing your server Utilization rates hitting 50 to 100%, and you will notice a drastic slowdown on all network processes.**

Click on the Details button and you'll see this bit of information.

### **SLIDE 20**

What this does is captures the Workstation and its network address and brings it into NW Admin for you.

And now you can go back to the ZENWORKS container

### **SLIDE 21**

and you'll see a whole bunch of your systems that are attached to the network, listing the computer's name that you assigned it when you set the network identification, and the network card number that the network operating system uses.

Select the system you want to restrict the person to, right button click on it.

### **SLIDE 22**

Select the Network Address Button.

### **SLIDE 23**

and jot down the number. Don't use the IP number because SDPS systems are set to dynamically assign those. It usually changes each time the person logs in.

Now jump back to the User Account, and select the Network Address Restrictions button.

## **SLIDE 24**

Click on the Add button

## **SLIDE 25**

and put in the network number (the part in front of the colon) and the node number (the part following the colon). And click Okay. The person is now restricted to that one machine only for login.

## **SLIDE 26**

### **- Access Rights Security:**

Each user account or group can be assigned rights at individual **file, directory, and volume** levels.

Let's look a file's rights.

## **SLIDE 27**

In NW Admin, go to the Organizational Unit container

## **SLIDE 28**

Select the Volume, directory, subdirectory, and the file you want to restrict access to.

## **SLIDE 29**

Right button click on it. Select Details.

## **SLIDE 30**

That tells us a little about the file. But not what we are really looking for.

So select the facts button.

## **SLIDE 31**

Lot more about the file. This area lets us change file owners, modifiers, access, modification, and archive dates and times. This is a **KEY** area to check if you believe someone has been tampering with a file. Unless the person has the rights to get into NWAdmin and change these settings, this can provide you with a strong lead on who's been in your system and when.

Now select the trustees of this file.

## **SLIDE 32**

And here are the file's rights granted to trustees of the file. They are: Supervisor, Read, Write, Create, Erase, Modify, File Scan, and Access control. I think we all know what each of the rights means; so I won't go into each of them.

Let's select the Attributes button.

## **SLIDE 33**

And here is where you can set file attributes within Novell NetWare. In addition to the familiar ones from Microsoft (Archive, Read Only, Hidden, and System), there are also several others which you can use to slow people down from stealing old copies (Purge Immediate), changing file names on you (Rename Inhibit), or stopping them from deleting the file (Delete Inhibit).

## **SLIDE 34**

And you can do almost the exact same thing via Windows Explorer.

## **SLIDE 35**

Select the file, right click on it, select properties.

## **SLIDE 36**

See the Microsoft file attributes: Archive, Read Only, Hidden, and System.

Click on the NetWare Info Tab

## **SLIDE 37**

And there are our NetWare file attributes.

Click on the NetWare Rights tab.

## **SLIDE 38**

And we can see the users who are trustees for the file, and what they are allowed to do with the file.

Click on the Inherited Rights and Filters button.

## **SLIDE 39**

And we can see a whole list of everyone who has rights of any kind to this file.

**SIDE NOTE:** Always assign rights to groups, not to individuals; even in positions with unique role sets, and only one person assigned. By assigning the rights to a role, it becomes much easier to move or replace this individual's role in the company. Should you ever lose that person for any reason, his or her replacement can be loaded into the system, immediately made a member of that unique group, and you don't have to try finding all the individual files, directories, and volumes the original person had access to.

---

#### **SLIDE 40**

##### **- Workstation Security:**

Consists of a combination of NetWare Account security, physical security, and the use of Windows Screen saver passwords.

#### **SLIDE 41**

Here you see your standard Novell Login box, with the Advanced Option expanded to show tree, context, and server you're logging into.

#### **SLIDE 42**

Your hopefully familiar Windows screensaver.

#### **SLIDE 43**

And one of the several locations you can setup your Windows screensaver. Notice the Password protected option, and the short wait time in minutes. Couple of notes here: Science, The 60's USA, and Windows98 screensavers distort information, but they do not make your screen unreadable – DON'T USE THEM.

#### **SLIDE 44**

##### **Console Security:**

Console security's biggest portion is physical security. Physically lock the server and console up in a location that only the Information Systems Manager and one assistant can get to. That's part of the SDPS/CMS requirements. If a hacker can get physical access to your server and the console, you've lost the game. Use Secure Console and the screen saver NLM. And choose a good strong password for your console. This can slow them up a little bit if they gain access during lunch hour; but won't help much if they have all night to work on it.

#### **SLIDE 45**

Here's some of the options you can set with your screen saver nlm.

A note about the Screen Saver NLM. Make sure that the Norton Antivirus NLM is in the current path or it won't load properly.

A side note here on the NetWare Management Portal. I understand that SDPS is planning on implementing this option in the near future. This is a Web-based option for remote server management. It lets you do almost everything you can do at the console and with NW Admin from anywhere in the world, preferably from your easy chair in the living room. What becomes absolutely mission critical is the use of a good, strong, frequently changed passwords for everyone with this kind of access (and there really should only be two people in each QIO with this access.) If you can access it from anywhere in the world, then so can 6 billion other people, and a lot of them will be trying.

---

## **SLIDE 46**

### **Accounting**

What is Accounting?

By the manual, Accounting is Novell's way to control and manage access to the server in a way that is "accountable". The account "pays" for the service by being given some number, and the accounting server deduces for these items. How the account actually pays for these items (departmental billing, cash, whatever) you may or may not want to know about, but the fact that it could be installed could leave a footprint that you've been there. Accounts can be set for the server, or for the user.

## **SLIDE 47**

To set accounting for the server, navigate to the server object in NW Admin, and right click it, and select details.

## **SLIDE 48**

Select the Accounting Button.

## **SLIDE 49**

And select Yes.

The admin set up allows you to charge rates for

## **SLIDE 50**

Blocks Read, written, connect time, service requests, and disk storage.

## **SLIDE 51**

For the user, you access the user account, details, and select account balance where it allows you to select unlimited credit, or so assign a specific account balance.

Any valid account, including non-supervisor accounts, can check to see if Accounting is turned on. Simply run SYSCON and try to access Accounting, if you get a message that Accounting is not installed, then guess what?

Since it is a pain to administer, many sys admins will turn it on simply to time-stamp each login and logout, track intruders, and include the node address and account name of each of these items.

---

## **SLIDE 52**

### **Backups**

SDPS mandates our use of the Backup Exec for Netware by Veritas (currently version 8.5). As far as Netware backup applications go, this is just as good as any of the others on the market according to several other admins and instructors I've spoken to in the Boston area.

Some of the things to consider:

- A good backup strategy needs to be in place.  
(SDPS guidelines say nightly tapes should be kept for 1 week, weekly tapes for four weeks, and last weekly tape of the month should be kept for a full year.) Nightly tapes can be incremental, but weekly tapes need to be full backups. My recommendation, if possible, do complete backups every night. Obviously large QIO's don't have this as a viable option.
- Off-site storage and rotation strategies should be used.
- If you store your tapes outside of your organization's control, you should have a good, strong password on every tape.
- Make sure the verify option is used on the tapes every day.
- Test your tapes frequently by actually doing a file restoration. This will keep you familiar with the process and let you know the condition of your tape cartridge.
- Destroy defective tapes. We typically give a tape cartridge one freebie in case a backup error was due to a dirty drive head, power fluctuation, or some other problem (and make the cartridge so we know we've had a problem with it before. Second failure results in destruction.

Speaking of destruction; you can use a licensed, bonded company that specializes in record destruction (specifically of tapes); but it can be costly. You can also do them in-house with shredders, acid baths, or burning; provided you have the permits and safety equipment for the last two. My low-tech solution, although a bit messy and time consuming, is to remove the tape from the cartridge, and neck it and break it into small (1 to 2 foot long) pieces. Once a tape has been necked, even though the information is still there, nobody has a reader that can scan the surface. And breaking it into small pieces destroys whatever order the information was in.

Possible to recover, but far too time and money consuming to even make the attempt. Not even Bristol-Meyers wants your beneficiary data that bad.

To set the password option on a backup tape, open Backup Exec either from NW Admin, or start it from Windows Explorer, or from an icon you've made (lots of options). Which ever way you use, you should end up here.

### **SLIDE 53**

Select Job.

### **SLIDE 54**

Now either double click on the job, or highlight it and click on Edit.

### **SLIDE 55**

And you can set your good, strong password here. Just don't forget what it is.

### **CONCLUSION**

There are holes that can be exploited in Novell NetWare. However, they are easily fixed. As long as you take all these steps, then you are extremely unlikely to get hacked. Hackers look for these options to not be used, and sadly, there are a lot of networks out there where people don't use these options.