

## Novell Netware Console Security

### Introduction

One of the main problems with servers is their simple ability to be compromised by turning it off. In many cases the problem is solved with physical security, and in several of the other sections of this project I have noted that Novell is extremely versatile in the area of remote management making it an ideal operating system for high physical security, however let's focus for a moment on the concept of console security, in the case of physical security failing and the user having immediate access to the console, what is to stop the user from simply typing the "DOWN SERVER" command at a Netware console and effectively causing a denial of service attack for your network (even if the results are short-lived)

Many hardware manufacturers make system BIOS controls that disable the on/off button on many servers, and as Dell and IBM have done effectively in the past the front of the Chassis is locked to prevent physical access to the server's on/off button

The same holds true for operating system security virtually every version of professional Windows since Windows NT4 have included a screen or workstation lockout feature and the software is adapted in the Novell client. This program on the servers effectively solves the problem for Windows Servers but it is important to note the same feature on a Novell server.

If presented with the console (which in a typical running environment is the running mode a Netware server should be operating in the GUI should be disabled to save resources) the following should keep the console secure.

## Screensaver NLM

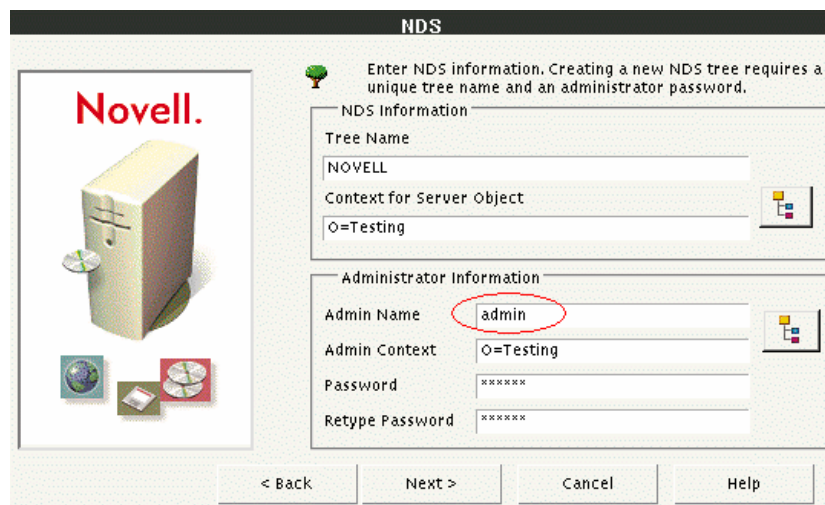
At the console execute the command Scrsaver.NLM (Netware 5.0 and above) this program will allow the administrators to control access to the console.

When the console is intended to be used the module presents the user with a login window, it then checks the user's database to insure that the user has read and write access to the Access control list, if the property is true the console is unlocked, if false an error message is displayed

## Admin Security

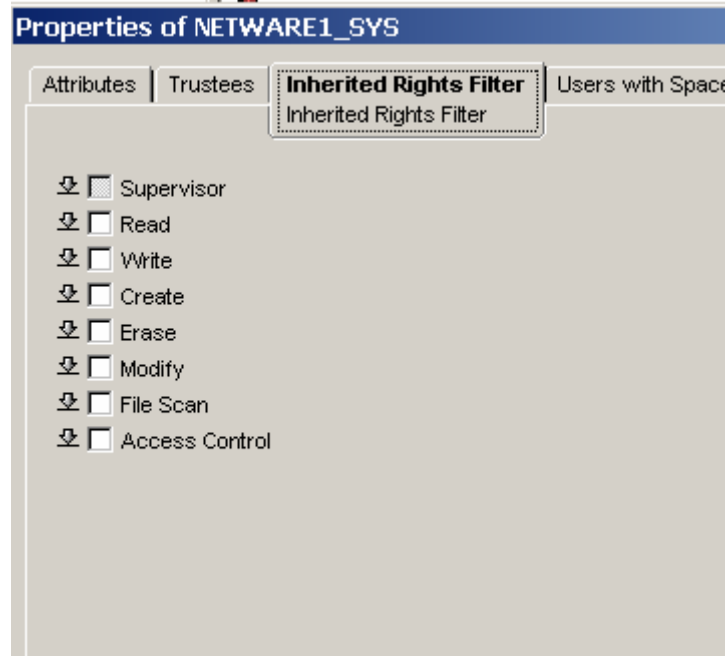
The admin user is by far the most critical user in the entire Netware directory, so therefore this account must be protected to combat the problems illustrated in the Penetrating Testing section. The following are effective solutions for admin user security

- Rename the Admin user on startup – Novell by default during setup will prompt the user to name the first user admin, however this can be changed simply by changing the value in the textbox during the GUI setup



The screenshot shows the 'NDS' setup window. On the left is a 'Novell.' logo and an illustration of a server tower. On the right, there are two sections: 'NDS Information' and 'Administrator Information'. The 'Administrator Information' section has four fields: 'Admin Name' (containing 'admin', circled in red), 'Admin Context' (containing 'O=Testing'), 'Password' (containing '\*\*\*\*\*'), and 'Retype Password' (containing '\*\*\*\*\*'). At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

- Once Renaming the admin object, create another user named admin (with minimal permissions and lock it out completely, then audit the user using the system logs
- Be careful when setting inherent rights to volumes- These rights are set to every user in the context where the volume is located so it's a good idea to carefully examine the rights that you are assigning in this property



- Assign one computer or workstation to be the admin computer and control access to it. Then login the admin user to this workstation and set the simultaneous connection of the admin object to 1, if any other user tries to login with the admin account on another workstation they will be unsuccessful

