

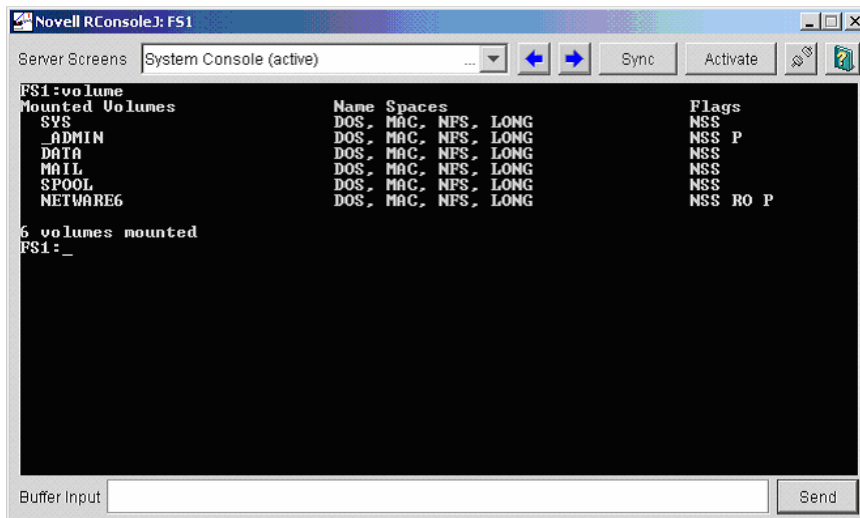
Introduction

Information Gathering and espionage on servers is always a first step in penetration testing, and the developers of Novell make it extremely difficult from the server console to get any kind of information off the server, however there are a number of simple tools bundled with Netware to make extracting information from the server via the client very easy, this section of the article will outline the subtle differences in the console while taking a look at the in-depth tools that will allow the user to extract information from the console.

Server Console Variants

The main difference between each of the server consoles (if one were to look at them in passing) is the appearance of the GUI, the server at first glance appears to have a java look to the GUI, giving the illusion of a older Solaris variant, this is true mainly because the Novell GUI is java based and a major component of Netware is java, however don't let the look of the OS fool you, the look and feel may be similar to Solaris however at the core it is a very different system.

If there is no GUI present and the system has been in place for several years it is safe to assume that the OS is Netware 4 or bellow, this is largely due to the difficulty of disabling the GUI on start, however most competent security administrators will exit the GUI when they get the server setup correctly to prevent "pass by reconnaissance" of the system. The reason that I suggest Netware 4 if a GUI is not present is simple; the GUI was not a major component of the OS until the introduction of Netware 5



The screenshot shows a window titled "Novell RConsole:J: FS1". The window contains a terminal interface with the following text:

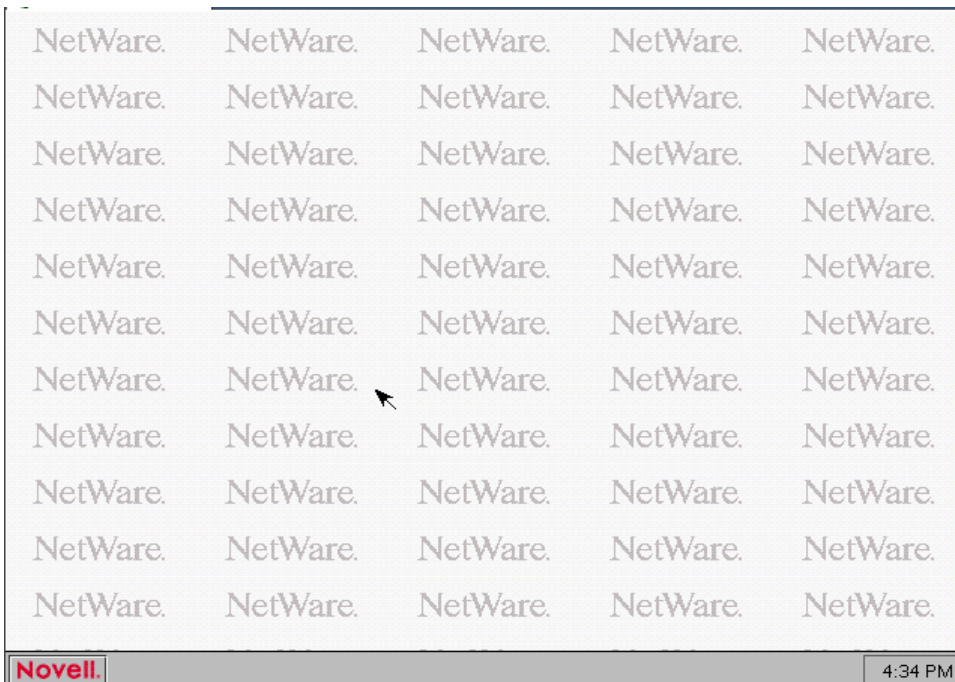
```
Server Screens System Console (active)
FS1:volume
Mounted Volumes
Name Spaces Flags
SYS DOS, MAC, NFS, LONG NSS
_ADMIN DOS, MAC, NFS, LONG NSS P
_DATA DOS, MAC, NFS, LONG NSS
_MAIL DOS, MAC, NFS, LONG NSS
_SPOOL DOS, MAC, NFS, LONG NSS
_NETWARE6 DOS, MAC, NFS, LONG NSS RO P
6 volumes mounted
FS1: _
```

At the bottom of the window, there is a "Buffer Input" field and a "Send" button.

Remote Netware Console: Netware 4

Things get slightly more complicated with the introduction of Netware 5 and 6's GUI's mainly due to the fact that they are mostly identical in nature. The most subtle difference however is the sharpness of the icons and the background picture. Because of the GUI's simple design and the designers put very little development time into it, the features for changing the background are not

exactly evident. Therefore most of the administrators (as I did thought this project) didn't bother changing the default background



The two pictures above illustrate the differences in GUI configuration in the Two OS variants, the top being Netware 6 (significantly sharper image as well as a more visual background) while the bottom being the Netware 5 GUI

Console

If a Netware server is observed from the console and not the GUI it is quite easy to mistake the server for a Linux environment as the consoles look remarkably the same, both start with a simple prompt and use different colored text to illustrate different system components. However there are differences. The most major being the Linux console will display the machine hostname and the path (as illustrated bellow) for example local host root # whereas the Netware console will only display the server hostname (bottom picture) and no directory location due largely to the fact that the console of the Netware workstation was never indented for directory browsing.

```
* Modules built or support compiled into the kernel
* Mouse is ImExPS/2 Generic Explorer Mouse at /dev/input/mice ...
* Starting gpm ...
* Network device eth0 detected, DHCP broadcasting for IP ...
* Creating X Configuration ...
Video is Cirrus LogicIGD 5446, using X(vesa) Server
Monitor is Generic Monitor, H:28.0-96.0KHz, V:50.0-75.0Hz
Using Modes "1024x768" "800x600" "640x480"
* Configuring OpenGL ...
* If you have a card that you know is supported by either the ATI or
* NVIDIA binary drivers, please file a bug with the output of lspci
* on http://bugs.gentoo.org so we can resolve this.
* opengl-update is deprecated and is just a frontend to the opengl
* eselect module. In the future, opengl-update will be removed
* from portage. Please see 'eselect opengl help'
Switching to xorg-x11 OpenGL interface... done
* VideoCard: Cirrus LogicIGD 5446
* Auto-scrambling root password for security ...
* samba -> start: smbd ...
* samba -> start: nmbd ...
* Starting snort ...

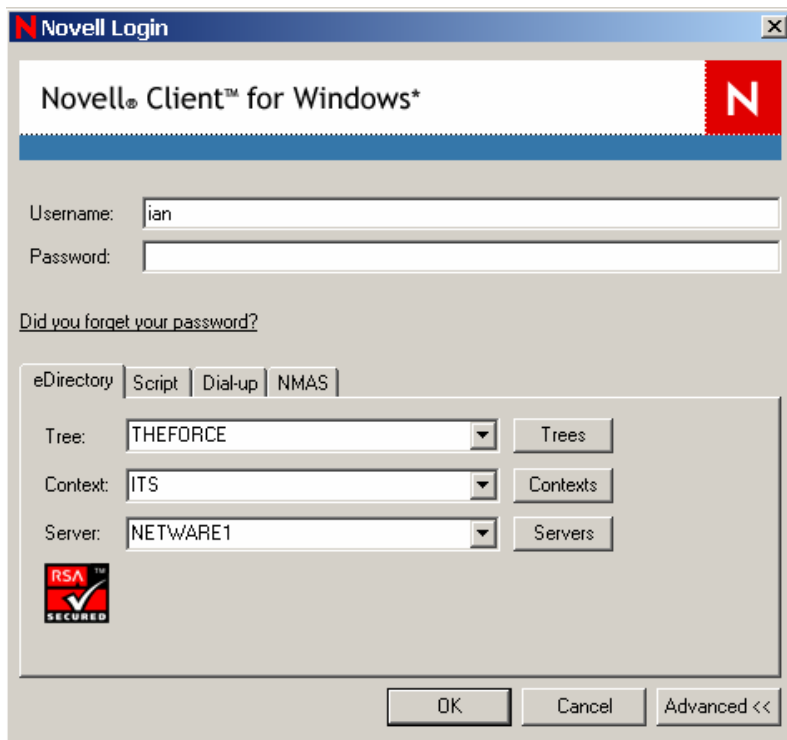
localhost root #
```

```
FS1:cifsstop
Module NFAP4NRM.NLM unloaded
Module CIFSPROX.NLM unloaded
Module CIFS.NLM unloaded
Module CIFS.DNS.NLM unloaded
Module SETMD4.NLM unloaded
FS1:_
```

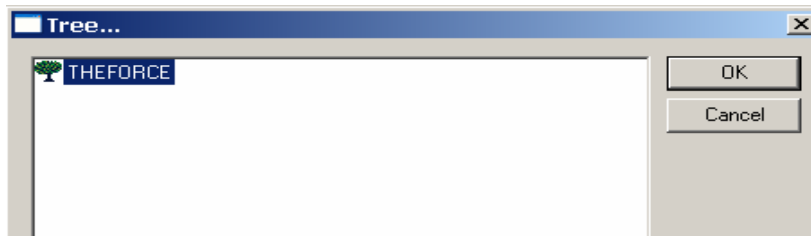
Gathering Information from a Workstation

The first of several tools is oddly enough the Novell client itself, unlike windows which will only tell you a domain name; the Netware client allows the user to view the server name, the tree name and the context. And if the user clicks on the context tree and server buttons allows the user to browse through the directory

looking for objects to connect to, this allows the user an idea at how the directory is broken down and the server hostnames without the need to login



Client with Details



Tree

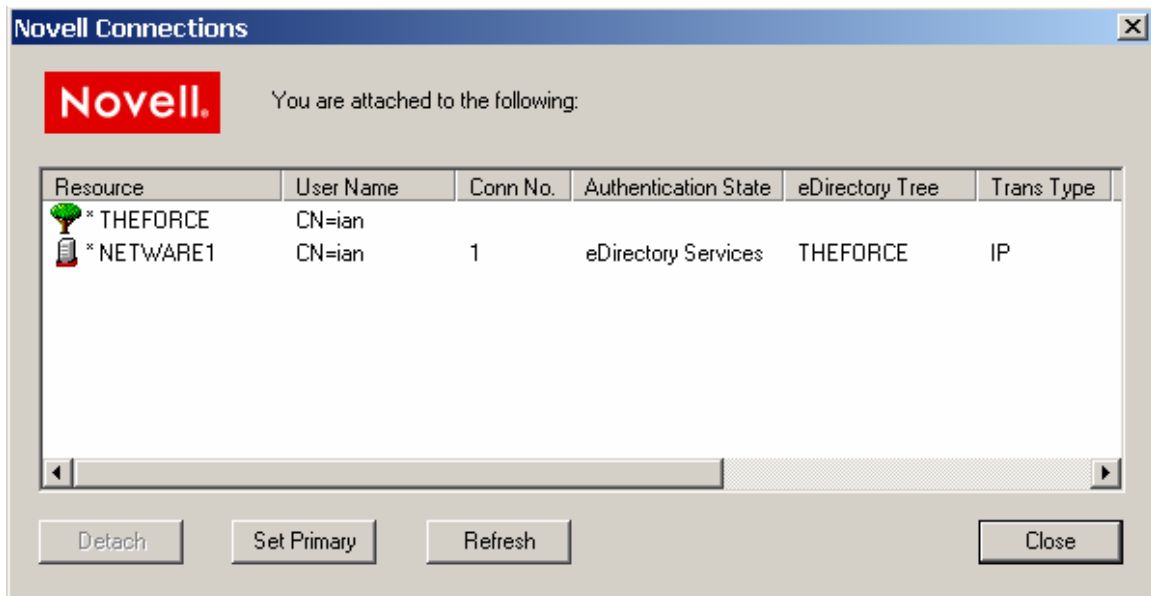


Contexts

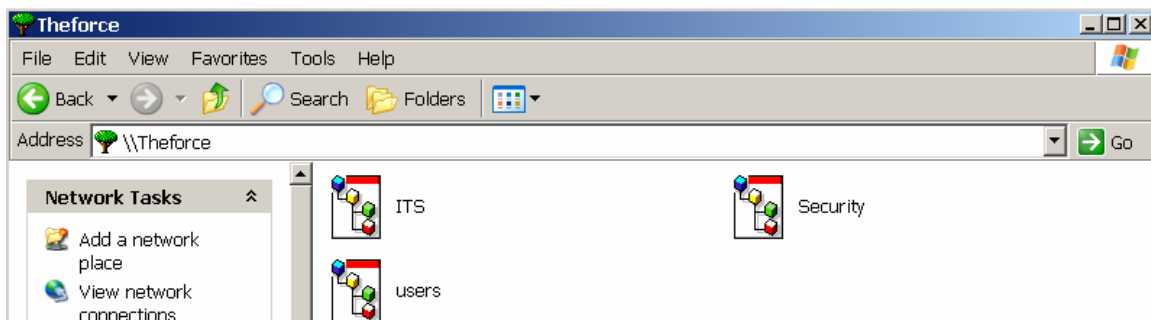


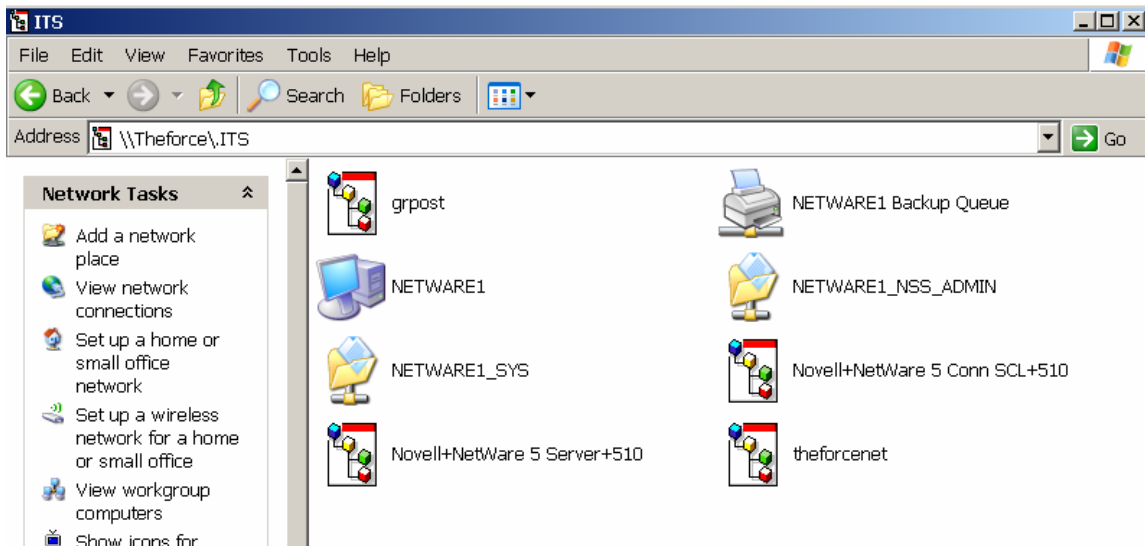
Servers

Also the Novell connections menu item (located under the red “N” icon in the system taskbar) will allow the user to view connection information and the servers they are currently connected to. In a large environment the user could potentially gather critical information about a number of servers on the Netware network

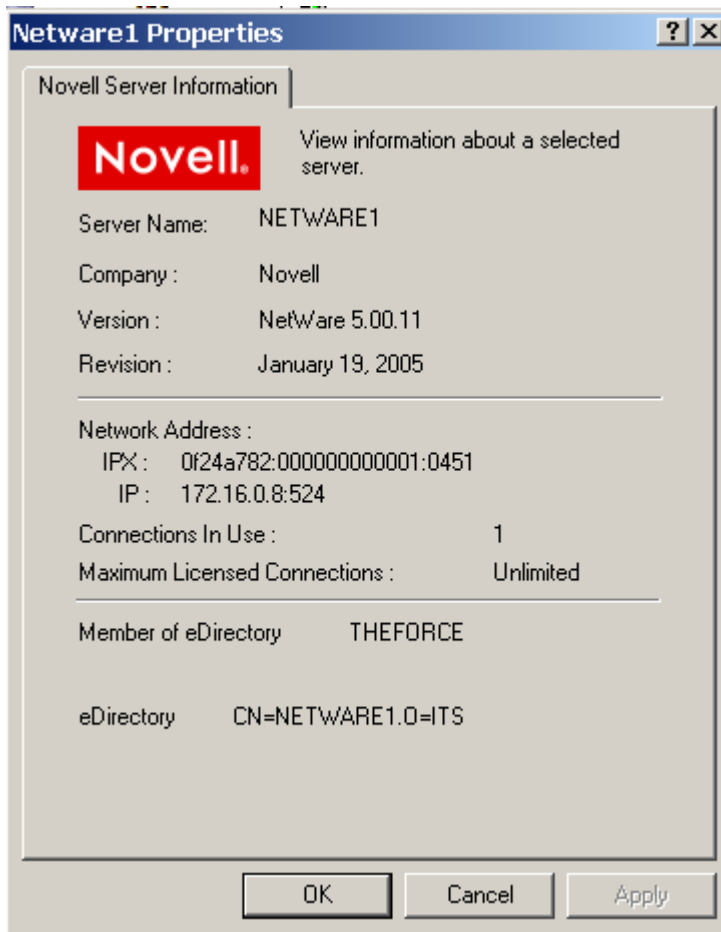


By clicking the Novell connections item in my network places, the user can browse the tree gaining information about contexts and the servers associated in them. All volumes are displayed unless the user doesn't have access to the specific volume





In the above section of a typical Netware context, we can see organization units, printer Queue's Server Names and volumes



By right clicking on a server object and clicking properties the user can view an incredible amount of information, including a LDAP server name, Licensing Information, Reversion of the OS (Indicating service pack) OS Version and server name and IP/IPX information

The next tool that is very useful in gathering information on Netware systems from a client point of view is NWADMIN32. This tool included in Netware 4,5,6, 6.5 and the newest edition open enterprise server was originally intended as a administration tool for adding users, groups, assigning permissions and other simple tasks like that. Even though this program was replaced by Console1 in Netware 6, it is still included in the public access directory of all Netware servers and mapped to a user desktop by default.

This program gives the user detailed information on the directory structure and the usernames of all the users in a specific context or tree (depending on assigned access rights) this is a perfect starting point for social engineering attacks, mainly due to the fact that user information (department, first name, last name phone number) are accessible to virtually every user on the system

It is however worth noting that the more complicated the e-directory (especially when the newer features of Netware 6.5 like iprint and net storage are added) the more likely that NWADMIN will crash. This is also dependent on network utilization.

