

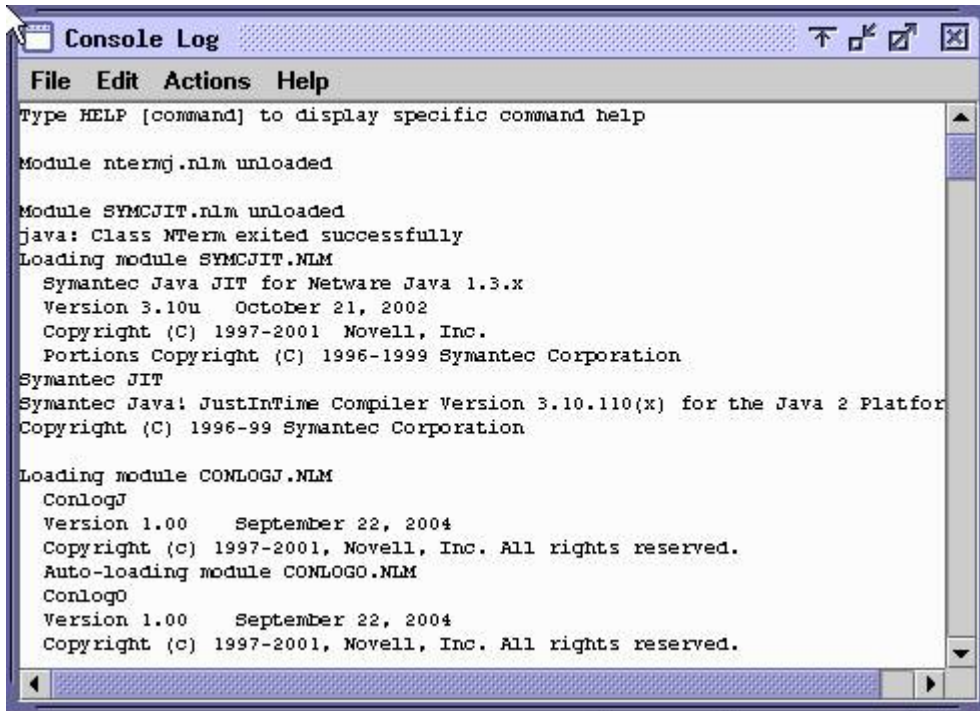
## Novell Netware Console Forensics

### Introduction

For all its features Novell Netware has several problems that make forensics very difficult to manage. One of the most interesting however is the “login less” console, the component of the OS that allows the user to boot the server and enter a root prompt without the need to enter a user name or password. As discussed in the security section of this project there are several ways of making the console more secure, the lock console function as well as BIOS functions preventing the user from executing a physical denial of service attack against the network. However this article will focus on the forensics behind the client, what happens when the user does exploit the system and what happens after? How do we proceed with an investigation? Unfortunately the answer is limited there isn't much forensics work that can be done due largely to the fact that there is no console login command. We can however log what is being done at the console, and the times in which they are done at. This in conjunction with secure locking chassis's and physical server room security cameras should be sufficient to provide a forensics environment.

### Console Log File

Novell by default makes a small log file for troubleshooting purposes this log is accessible through the Novell Netware GUI under the Novell Menu and clicking the Console Log Button

A screenshot of a 'Console Log' window. The window has a title bar with the text 'Console Log' and standard window control buttons (minimize, maximize, close). Below the title bar is a menu bar with 'File', 'Edit', 'Actions', and 'Help'. The main area of the window contains a scrollable text area with the following text:

```
Type HELP [command] to display specific command help

Module ntermj.nlm unloaded

Module SYMCJIT.nlm unloaded
java: Class NTerm exited successfully
Loading module SYMCJIT.NLM
  Symantec Java JIT for Netware Java 1.3.x
  Version 3.10u   October 21, 2002
  Copyright (C) 1997-2001 Novell, Inc.
  Portions Copyright (C) 1996-1999 Symantec Corporation
Symantec JIT
Symantec Java! JustInTime Compiler Version 3.10.110(x) for the Java 2 Platform
Copyright (C) 1996-99 Symantec Corporation

Loading module CONLOGJ.NLM
  ConlogJ
  Version 1.00   September 22, 2004
  Copyright (c) 1997-2001, Novell, Inc. All rights reserved.
  Auto-loading module CONLOGO.NLM
  ConlogO
  Version 1.00   September 22, 2004
  Copyright (c) 1997-2001, Novell, Inc. All rights reserved.
```

The problem with this log is that it is by default trimmed to a very small amount, because for the most part its intended to provide troubleshooting for the server.

### Auditcon

Novell however did build a command into the server called Auditcon, by executing this command at the server prompt it will allow for a more extensive log file to be created. This command will create the log file in the SYS:ETC file, however admin privileges are needed to view this directory.