





Introduction

The Novell operating systems like most of the other major network operating systems have a critical problem with Denial of service vulnerabilities. As stated in the sections in this document the Netware operating system will allow any user regardless of authentication to the server, executing a vulnerability on a Netware server is not difficult if the vulnerability deliverable is specifically geared toward Netware servers, or are generic enough in nature to pass as a regular console on the Netware environment.

Because of the heavy reliance on Linux on Netware 6 and 6.5 and the reliance on Netware 3 and Netware 4 in the Netware 5 Platform this section will be divided along those guidelines

Vulnerabilities but Not Catalysts

As Netware 5 is essentially its own breed of operating system there are several operating system vulnerabilities especially with the module components of Netware 5 (NDPS – Novell Distributed Print Services, iManager) the vulnerability database at secunia contains several different vulnerabilities associated with the Netware loadable modules (NLM)

 <u>Novell NetWare CIFS Denial of Service Vulnerability</u> Vendor Patch. Secunia Advisory 1 of 2 in 2005		
Release Date: 2005-08-31	Secunia Advisory ID: SA16640	Solution Status: Vendor Patch
Criticality: 	Impact: DoS	Where: From local network
Short Description: A vulnerability has been reported in NetWare, which can be exploited by malicious people to cause a DoS (Denial of Service). [Read More]		
 <u>Novell Netware CIFS Denial of Service Vulnerability</u> Vendor Patch. Secunia Advisory 2 of 2 in 2005		
Release Date: 2005-01-10	Secunia Advisory ID: SA13766	Solution Status: Vendor Patch
Criticality: 	Impact: DoS	Where: From local network
Short Description: A vulnerability has been reported in NetWare 5.1 and 6.0, which can be exploited by malicious people to cause a DoS (Denial of Service). [Read More]		

The problem however is the catalyst for vulnerability delivery.

In the following section of a metasploit vulnerability delivery agent



As you can see from the section above the majority of the payloads are for windows /add user and some generic reverse bind and reverse shell. All research indicates that a reverse shell generic payload may succeed in getting into the console of the Netware server from time to time, however the failure rate is well above 50% of the time.

For accurate penetration testing it is recommended that a Netware specific payload for metasploit be developed


Netware Denial of Service

One of the major disadvantages of the Novell imanager system is that it offers a unprecedented level of system administration via a web browser window, if a user initiates a escalation of privilege attack they could have a clear administration window to your server from anywhere in the world, via a web browser.

Also the imanager login does not count on the simultaneous connection restriction that was recommended to be implemented in the security section of this guide. If a user has escalated there privileges to admin level they will have a clear way of disabling the server via imanager, and if they are very thoroughly familiar with Netware they could alter the DOS partition (available through imanager) and remove the server exe file from the autoexec, making the server unbootable, or simply remove the sever exe file altogether.

Screenshot of the Novell Imanager accessing the DOS partition, an attacker could upload a blank autoexec file then down the server rendering it unbootable

C:



[Upload](#)

	Name	Size	Attributes	Date and time	
📁	NWSERVER	[dir]	-----	27 Mar 2007 10:20 AM	
📄	AUTOEXEC.BAT	26	---A-Rw--	27 Mar 2007 11:38 AM	Delete
📄	COMMAND.COM	66,657	---A-R0--	27 Feb 1998 07:02 AM	
📄	CONFIG.SYS	36	---A-Rw--	27 Mar 2007 11:38 AM	Delete
📄	IBMBIO.COM	29,626	---A-R0--	19 Aug 1998 11:04 AM	
📄	IBMDOS.COM	30,720	---A-R0--	27 Feb 1998 07:02 AM	

Down Server Options

Press:



To take the server Down.

Press:



To down the server and then restart it.

Press:



To down the server and then warm boot the machine.

Imanager comes standard with several features allowing the imanager "administrator" to restart or down the server.