

Escalation of Privileges (Netware 6)

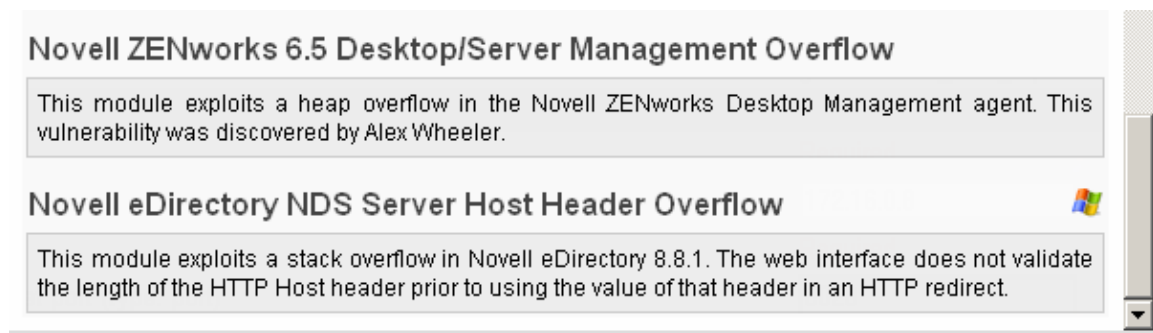
Introduction

Although the operating variable files used to attack passwords in the previous section are a critical part of the Netware 6 operating system (and all other versions of Netware) the Pandora vulnerability is widely publicized and Novell developed and introduced an effective workaround in their implementation of Netware 6 and Netware 6.5. To develop the workaround the Novell design team focused on the problem: Users access the console and gain access to the files. Their solution was simple: re-write the Novell imanager and RconsoleJ programs to deny everyone but Admin and security equal to admin the rights to the programs.

This solution does an effective job at addressing the vulnerability therefore in order to escalate privilege level on Netware 6; a large amount of hacking is involved.

In order to launch our remote console we must first locate information about the server in question more specifically which version of the NLM files are running on it. However this information is evident on most of the client programs and console1.

The next step in our procedure is to locate vulnerability for Netware 6, or one of the programs that are installed on it, several of the vulnerability's are available through internet newsgroups and some are bundled with the metasploit framework



Upon Selecting your vulnerabilities target the Novell Server for attack and launch a generic remote shell

Novell ZENworks 6.5 Desktop/Server Management Overflow (6)

Novell ZENworks 6.5 Desktop/Server Management Overflow

Please enter all of the required options and press 'Launch Exploit' to continue.

CURRENT CONFIGURATION - [CHANGE PAYLOAD](#)

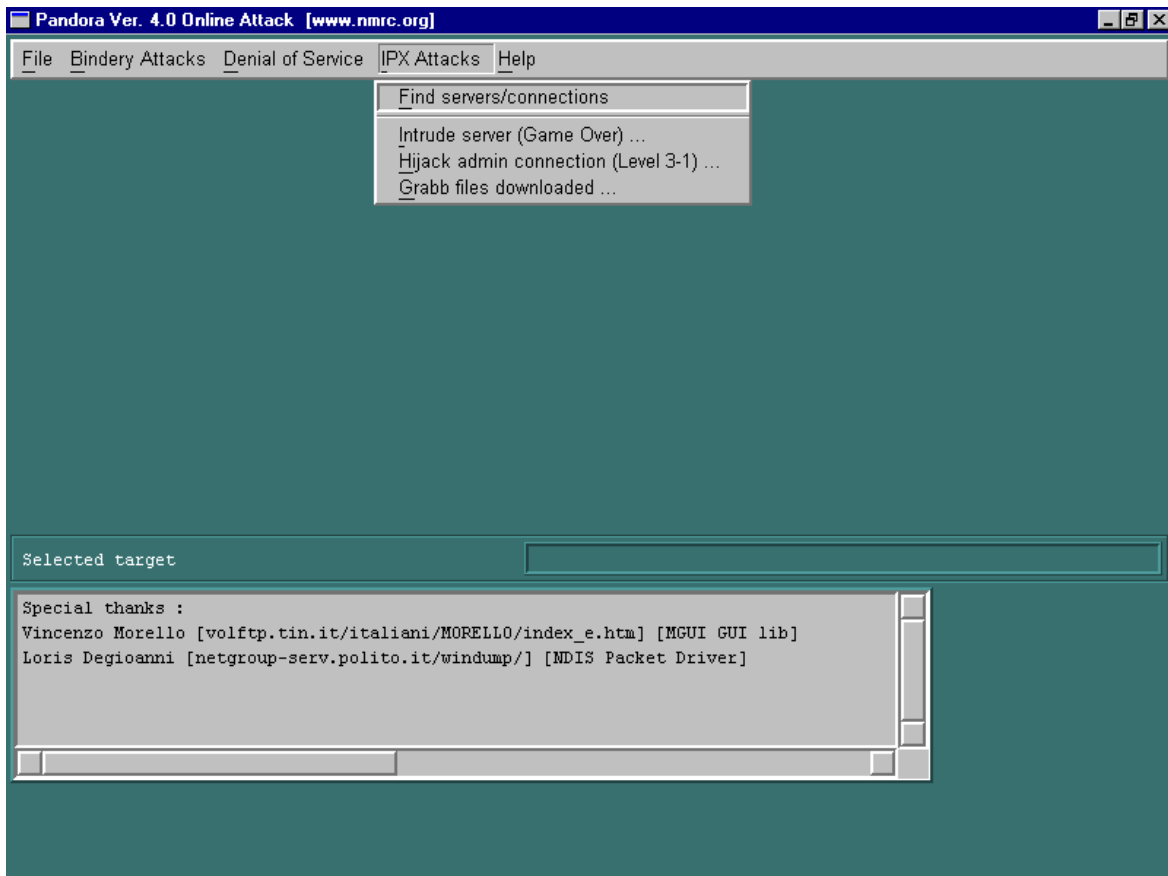
EXPLOIT	windows/novell/zenworks_desktop_agent
TARGET	Windows XP/2000/2003- ZENworks 6.5 Desktop/Server Agent
PAYLOAD	generic/shell_bind_tcp

STANDARD OPTIONS

RHOST	Required
The target address (type: address)	<input type="text"/>
RPORT	Required
The target port (type: port)	<input type="text"/>
LPORT	Required
The local port (type: port)	4444

Once launched the attacker will have access to the command shell at root access and can copy the files out of the SYS:_NETWARE directory and crack them using Pandora

Another Alternative is to use Pandora Online attack, this program executes a vulnerability in Netware 4,5,6 (not 6.5) and will attack the server and decode the passwords all without ever needing to execute a remote console by the user.



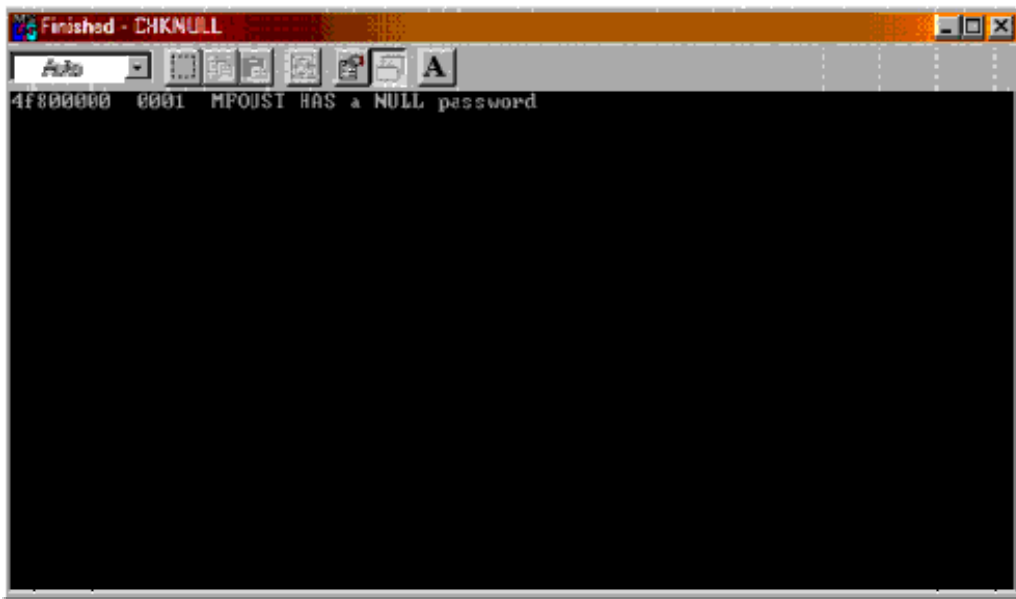
Pandora security research continues to evolve and more attacks for the Netware 6 and 6.5 environments are being developed

Non Users

Like any other network operating system Novell is bound to TCP/IP rules and like the laws of physics, the laws of TCP/IP must be followed regardless of security. And one rule that works in our favor is "everything that TCP/IP needs to connect to has to have a IP address" meaning that even though we are not connected to the server through the client the server can be contacted via a TCP/IP connection, leaving the server vulnerable

To exploit this problem we will use another tool from the Pandora toolkit called checknull.exe this program will take a string from a user (the full LDAP

username) and check the server to see if the usernames password is NULL then report back to the user.



Above: Checknull scanning the user MFOUST

NLIST

In most versions of Netware there is a product called NLIST, this program is DOS based and it scans contexts for usernames. This program can be used in connection with Checknull or social engineering tactics to execute a unauthorized entry into a Netware server.

***** NLIST *****

Object Class: User

Access control: LSE

User name: The name of the user

Min = Login disabled

Log exp = The login expiration date, # if no expiration date

Min = Yes if passwords are required

Pwd exp = The password expiration date, # if no expiration date

Min = Yes if unique passwords are required

Min = The minimum password length, 0 if no minimum

User Name	Min	Log Exp	Pwd Exp	Min	Min
-----------	-----	---------	---------	-----	-----

admin	No	##/##/##	No	##/##/##	0
-------	----	----------	----	----------	---

nslist	No	##/##/##	No	##/##/##	0
--------	----	----------	----	----------	---

A total of 2 User objects was found in this subtree.

A total of 2 User objects was found.

ABOVE: NLIST OUTPUT