Securing a NetWare 6.5 Installation and Server Environment

(Know thy system)

GIAC Security Essentials Certification
Practical Assignment v1.4b Option 1

Bob Clarke
February 5, 2004

Table of Contents

Abstract

Even though NetWare still supports the more secure IPX/SPX protocol, over the past 6 years Novell has increasingly focused more on NetWare running on the less secure TCP/IP protocol. NetWare 6.5 is the latest OS release from Novell Inc. [1] Novell is actively participating in the Open Source movement and has integrated open source applications such as Apache, Tomcat, MySQL, PERL, PHP and OpenSSH into NetWare 6.5. [2] This paper will focus on how to secure the installation of NetWare 6.5 and a number of applications and services that run on it, including Apache, MySQL, PHP and PERL and OpenSSH. In addition, steps for making a more secure server environment will be reviewed. All of this will create a more secure server environment that enables you to “know thy system.”

Overview

A layered approach to network security is explained in the SANS Security Essentials II: Defense in Depth [3] section. An essential component of Defense in Depth is to have a secure OS installation procedure. Security measures typically are not a part of a vendor’s OS installation procedure. It is up to system administrators to build this security or “hardening” into the installation process. Closing unnecessary system services as well as patching is a must when installing a new OS and applications with known vulnerabilities. Vulnerability scanners help to expose these open services and vulnerabilities. There are a number of vulnerability scanners available today including Nessus, eEye Digital Security, and Foundstone. The Foundstone Enterprise v3.1 vulnerability scanner was used in this process. NetWare security practices are also employed. These steps are followed to secure the NetWare 6.5 installation:

- OS installation including service packs, security updates and patches
- Vulnerability scan
- Vulnerability remediation
- Verification scan
- Service lockdown
- Remote management security
- Application security
- Service security
- AntiVirus, backup and physical security

Additional general NetWare and NDS/eDirectory security topics will be reviewed as well.

Authorization to Scan, Sniff, Probe and Hack

Most organizations have policies regarding the scanning, sniffing, probing and hacking of their networks and systems. Make sure that you have authorization to perform such tasks in your organization before you use a vulnerability-scanning tool.

OS and Product Installation information

The most current NetWare 6.5 installation documentation can be found at http://www.novell.com/documentation/lg/nw65. Always review the read me files before installing the OS, service packs, patches and additional products for information on any issues discovered with the initial release. Also review the minimum and recommended server requirements. If possible accept what Novell recommends for processor, memory, disk space, and partition sizes for scalability. Today's server hardware is more affordable than ever so it is a good practice is to use real server hardware made by the major manufacturers. This will typically insure that the OS will be supported to run on the hardware and that drivers will be written as well. Know the media source for the OS installation and only use reliable media from the vendor. The correct admin rights to the location in the tree where the server is to be installed are required. A NetWare 6.5 server can provide many roles based on the wide choice of products that can be installed. There are currently 19 different installation choices for NetWare 6.5. The installation process allows many options on the type of server you want to install, from the common file and print server to specialized servers for hosting Web services and applications, LDAP authentication, mass storage, clustering and auditing to name a few. A Customized NetWare Server installation was chosen in this example to allow for selecting the products to install. This installation provides file and print, DNS/DHCP, LDAP, web and database services. Novell commonly refers to an installation of Apache, MySQL and PHP/PERL on NetWare, as AMP. [4] The installed products:

- Apache/Tomcat Server
- NWFTP
- DNS/DHCP
- MySQL
- OpenSSH
- iManager
- iPrint
- Nsure Audit Starter Kit

Additional products that are installed by default and by selecting the above products:

- eDirectory 8.7 Directory Services
- ConsoleOne 1.3.6
- eMBox
- Java Virtual Machine (JVM)
- LDAP Service
- NetWare Remote Manager
- Novell NDS iMonitor
- NetWare Storage Management Services (SMS)
- Novell Certificate Server 2.4.0
- Novell International Cryptographic Infrastructure (NICI)
- Novell Licensing Services

- Novell Modular Authentication Service (NMAS)
- Novell Script for NetWare (for PHP and PERL support)
- Novell Native File Access (MAC, CIF and UNIX file access)

A feature of NetWare is that services must be selected for installation and are not installed by default. A good security practice is not to install services if they aren't required. However, depending on the environment it might be a good practice to install basic services like FTP, DNS/DHCP and printing, and remove them from the startup files so they do not run. You may need to enable one of these services say if another server goes down. As service packs and security updates are applied to the OS, these services will be also be updated even if the service is not running. This will avoid having to install a particular service later on if needed and then reapplying the service pack again to update the service.

Patches, Fixes, Security updates and Knowledge Base

NetWare 6.5 needs "hardened" once the OS and applications are installed. The first step after any OS installation is to put on the latest tested service pack, patches, fixes and security updates. The link to Novell's v6.5 patch list is:
http://support.novell.com/filefinder/18197/index.html
At the time of this writing these OS updates were available:

- NetWare 6.5 Support Pack 1.1
- Corrected PERL scripts for NFS exports
- TCP Update for NetWare 6.5
- NW 6.5 Tomcat 4 .keystore Utility

The link to Novell's security alert site is:
http://support.novell.com/filefinder/security/index.html
At the time of this writing these security updates were available:

- XNFS-NESSUS abend fix
- NWFTPD.NLM August 2003 Enhancements and fixes
- Security updates to Novell's OpenSSH CVE CAN-2003-0190
- Security Update 3 CVE CAN-2003-5543 and CAN-2003-5544

Novell's extensive knowledge base containing Technical Information Documents or TID'S can be found at http://support.novell.com/.
In order to download some files from Novell's web site a portal login is required. It's easy to set up an account.
All of these updates except for Security Update3 were applied. SP 1.1 upgrades eDirectory to version 8.7.3 that has the fix for the SSL/TLS ASN.1 decoder DoS vulnerability. Additional information on this vulnerability can be found in this TID http://support.novell.com/cgi-bin/search/searchtid.cgi?/10087450.htm.

Scanning and Remediation

Vulnerability Scan

Our organization uses a vulnerability scanner from Foundstone. Once the OS installation and patching was complete a scan was run on the server using Foundstone's general assessment and web application assessment modules. The general assessment module included trojan, rogue app, UNIX, web and miscellaneous non-intrusive scripts and brute force, UNIX, web and miscellaneous intrusive scripts. Most Foundstone scripts are based on Common Vulnerabilities and Exposures. CVE is a list of standardized names for vulnerabilities and other information security exposures. Be careful if you run intrusive scans with any scanning tool on production systems. If the system has a vulnerability that the scanning tool knows about it will run the exploit and you risk the chance of crashing the system. It is recommended to only run intrusive scans on new systems before they are placed into production or during a maintenance window. Several good sources for vulnerability and threat information are Talisker, SecurityFocus, Secunia, CERT and Symantec. The web assessment module looks through Web applications for data that attackers might find. It looks for source code, backup files, and application information. It also searches for SQL Server access points and attempts to gain access to Web applications.

The vulnerability scan turned up 1 high-risk vulnerability:

- OpenSSH buffer_append_space Buffer Overflow CVE CAN-2003-0693

The vulnerability scan turned up 2 medium risk vulnerabilities:

- SSHv1 Protocol Enabled CVE CAN-2001-0572
- SNMP Default Community Name CVE CAN-1999-0517

The Web assessment scan information:

- Source Code Disclosure was enabled. No vulnerabilities were discovered by the Source Code Disclosure feature during this scan.
- SQL Security Analysis was enabled. No vulnerabilities were discovered by the SQL Security Analysis feature during this scan.
- Source Sifting Analysis was enabled. No vulnerabilities were discovered by the Source Sifting Analysis feature during this scan.

Remediation

Fixing the reported vulnerabilities from the scan was done as follows:

OpenSSH buffer_append_space Buffer Overflow CVE CAN-2003-0693.
The OpenSSH patch was applied to the server to address the OpenSSH vulnerability before the scan. This should have been fixed. This turned out to be what is called a "false positive". The Technical Information Document, TID 2967067 on the OpenSSH fix on Novell's site, http://support.novell.com/cgi-bin/search/searchtid.cgi?/2967067.htm, indicated that the v3.7.1 buffer changes were incorporated into Novell's OpenSSH

SSHD.NLM 3.6.1. I checked the banner that the scan pulled from port 22 and it was listed SSH-2.0-OpenSSH_3.6.1p1. The scan listed this vulnerability based on the banner it grabbed. This is known as a false positive. Foundstone and Novell tech support were called to verify this. It was suggested to Novell that Novell change the banner and code to reflect the true version to prevent this type of false positive from occurring.

SSHv1 Protocol Enabled CVE CAN-2001-0572.

The fix for this is to edit the SYS:\ETC\SSH\SSHD.CONF SSH configuration file.
At the server prompt type EDIT SYS:ETC\SSH\SSHD.CONF <CR>
Change the Protocol 2, 1 line to remove the 1 and to look like this:
Protocol 2
ESC and Save to exit.

SNMP Default Community Name CVE CAN-1999-0517.

In order to fix the SNMP Default Community Name, the INETCFG utility was run to configure the Community name to something other than public or default. Or it can be set to no community can read. The utility enables the change to be made on the fly. The reference for the INETCFG utility can be found at http://www.novell.com/documentation/lg/nw65/utlrfenu/data/hv7lr8sz.html.
So in effect Novell had a fix for all three of these vulnerabilities.

Foundstone Enterprise has a remediation feature that allows for verification of the fixed vulnerability. A ticket is issued for each vulnerability discovered. After the fix is applied to a vulnerability a verify button in the ticket is clicked and the system with the vulnerability is checked to verify that the fix is in place and works. If the verification is good the ticket is marked “passed” and can be closed by the administrator. This process was used to check each vulnerability.

Verification Scan

Once the fixes were verified the same vulnerability scan was run against the server. According to the verification scan results 2 of the 3 vulnerabilities were removed. The exception in this scan report was the OpenSSH Buffer Overflow vulnerability, which is the false positive.

Securing Services

A number of services were discovered running during the vulnerability scan. There are some that deserve mentioning from a security perspective either because the service is a security threat or the service enables security methods that take away security threats. TCPCON is a utility that can be run from the server console to view UDP and TCP ports running on the server.

FTP

File Transfer Protocol is started by running NWFTP.NLM. If the FTP service is not necessary then it should be removed the SYS:\SYSTEM\AUTOEXEC.NCF file and not run at all. FTP is configured from the SYS:ETC\FTPSERV.CFG file. Don’t enable the anonymous user account. FTP authentication is through eDirectory with a valid Novell user account. Access restrictions and rights are assigned in the SYS:ETC\FTPREST.CFG file. Make sure that intrusion detection is enabled. Also make sure that all FTP log files are enabled. FTP documentation can be found at Novell's web site. http://www.novell.com/documentation/lg/nw65/ftp_enu/data/a2fbytg.html.

SNMP

Simple Network Management Protocol is an application that enables the exchange of management information between devices on a network. There are no authentication methods for SNMP and it is a security threat if enabled. A number of exploits exist for SNMP if it is not configured properly. Disable SNMP if it is not required. Two good references for SNMP information can be found at http://www.cert.org/advisories/CA-2002-03.html
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm - xtocid17

HTTP

Hyper Text Transfer Protocol uses an unsecured connection to retrieve data from a Uniform Resource Locator and needs to be trusted.

HTTPS

HTTP over Secure Socket Layer, SSL. Ensures secured connection using HTTP. Used by Apache and Tomcat.

LDAP

Lightweight DirectoryAccess Protocol is used to authenticate to eDirectory with web enabled applications like iManager. LDAP uses port 636 for SSL encryption over the wire. Disable TCP port 389 so as not to allow clear text on the wire.

SSH

Secure SHell establishes an encrypted session from the server to a SSH client. A note here, telnet is not supported on NetWare 6.5.

Authentication Services

Certificate Server

Novell provides a Certificate Authority with Novell Certificate Server. Using Novell International Cryptographic Infrastructure, NICI, for encryption and Public Key Infrastructure, Novell's public key cryptography technologies, private and public key certificates (X.509) are issued and managed and encrypted. The CA issues certificates for all SSL enabled applications for session data encryption. Detailed information on Certificate Server is available at the following link. http://www.novell.com/documentation/lg/crt27/index.html

SSL

SSL, Secure Sockets Layer is the standard for encrypting a session between a web server and web browser. It is based on X.509 certificates. You will see a padlock somewhere on your browser when you have established an SSL session. Visit WhichSSL for some good information explaining SSL. http://www.whichssl.com/

Secure Console and Remote Access Administration

There are several methods available to remotely manage NetWare 6.5 servers. RconsoleJ, OpenSSH client utilities and web enabled applications are the most common methods for remotely accessing and managing NetWare 6.5 servers. Secure sessions for these access methods are essential. It is highly desirable to have both eDirectory authentication and encryption for remote sessions.

Remote Server Management – RconsoleJ
Novell RconsoleJ client is a Java based remote access program. RCONAG6.NLM is loaded on the server in order to initialize RconsoleJ client. The secure way of running RconsoleJ is to load RCONAG6 ENCRYPT from the server console. This will set the default secure IP port (SSL) information, port 2036, and the encrypted password used to login at the RconsoleJ screen. In addition you are prompted if you want to create the LDRCONAG.NCF file that will contain this information, including the encrypted password. Rconag6 can then be started during bootup with out answering the prompts by running LDRCONAG.NCF. The Secure IP method is selected from the RconsoleJ login screen and a certificate will be issued and the session will be encrypted. While the session data is secure it must be understood that the authentication is based on trusting the user is a legitimate administrator.
http://www.novell.com/documentation/lg/nw65/sman_enu/data/hw63v9ob.html

SCRSAVER
Run SCRSAVER.NLM to lock the server console. This will run a screen saver on the console that can only be unlocked by logging in with an eDirectory username and password. The utility can be run with a number of command line options for setting length of time to enable, password, etc. One thing to be careful about with this utility. If the SCRSAVER kicks in while the eDirectory database is locked, say running DSREPAIR to repair the local database, SCRSAVER will remain locked as a login cannot occur until the database becomes unlocked. Disable SCRSAVER temporarily when running DSREPAIR.
http://www.novell.com/documentation/lg/nw65/utlrfenu/data/hv7lr8sz.html

OpenSSH
With OpenSSH, SSHD.NLM loaded on the server, client utilities like Putty (freeware) can be used to establish a more secure remote console session than RconsoleJ. With Putty, the SSH session requires that the user login with a valid Novell account that is authenticated in eDirectory. The session data is also encrypted. This provides a great method for remotely managing a NetWare 6.5 server as both authentication and data encryption occur making it more secure then RconsoleJ.
http://www.novell.com/documentation/lg/nw65/openssh/data/front.html

NetWare Remote Manager
Web based management of NetWare 6.5 servers is becoming Novell's standard for managing servers and eDirectory. Using a browser such as Netscape 4.5 or later, Internet Explorer 5 or later or Mozilla Firebird, NetWare Remote Manager is used for administration and troubleshooting of the server and some of the

services running on it. Using port 8009, authentication to eDirectory with a valid Novell account is required to login and use this administration tool. Of course the proper rights to mange the server are required. PORTAL and HTTPSTK.NLM need are loaded in order to use NetWare Remote Manager.
http://www.novell.com/documentation/lg/nw65/index.html?page=/documentation/lg/nw65/remotemgr/data/a7hjvxo.html

iManager
iManager is a web based alternative to the java based ConsoleOne and the Win32 NWAdmin utilities for managing Directory Services. Novell is moving away from these legacy management tools and moving toward web based management. eDirectory authentication is required for accessing iManager. SSL is enabled by default in the Tomcat configuration file
SYS:TOMCAT\WEBAPPS\NPS\WEB-INF\PORTALSERVLET.PROPERTIES
System.DirectorySSL=true
http://www.novell.com/documentation/lg/imanager20/index.html

iMonitor
iMonitor, NDSIMON.NLM, is a web based alternative to eDirectory management tools like DSREPAIR, DSTRACE and DSBROWSE. Authentication to eDirectory is necessary to access iMonitor. iMonitor authentication is through eDirectory and is controlled in the SYS:SYSTEM\NDSIMON.INI configuration file. This setting (default) must be configured:
LockMask: 1 = Must be authenticated as a valid user
http://www.novell.com/documentation/lg/edir873/edir873/data/agwkqvb.html

Open Source Application Security

Apache
Apache is a widely used web server that runs on a number of platforms including NetWare. Apache version 4.0.45 is installed with NetWare 6.5 right out of the box. Versions previous to 4.046 have a number of high and medium risk vulnerabilities. Applying SP1.1 upgraded v4.0.45 to v4.0.48 and closed those vulnerabilities. For more information on Apache on Netware visit the Apache web site. [5]
http://www.novell.com/documentation/lg/nw65/web_apache/data/a7hjvxo.html

Tomcat
Tomcat v4.1 is an Open Source Java servlet application that also runs on several platforms including NetWare. Tomcat administration is done by authentication to eDirectory. Rights for admins and users are maintained through eDirectory as well. Make sure that the ***NW 6.5 Tomcat 4 .keystore Utility*** is applied to prevent problems with LDAP SSL connections and certificates.
http://www.novell.com/documentation/lg/nw65/web_tomcat/data/a7hjvxo.html

MySQL
MySQL is an Open Source relational database management system. MySQL also runs on a number of platforms including NetWare. Applying SP 1.1 upgraded MySQL to version 4.0.16 from 4.0 and closed any vulnerabilities associated with previous versions. phpMyAdmin is used to manage MySQL.

Care must be taken to protect the MySQL password. Typing “mysqladmin -u root password” and pressing Enter will set the root password. Replace *password* with your own password. For more information on MySQL on NetWare read Novell AppNotes, October 2002 [6] http://www.novell.com/documentation/lg/nw65/web_mysql/data/a7hjvxo.html

Server Auditing and Logging

Log Files and Reports

There are a number of log files and reports created by the NetWare 6.5 OS. All of these files contain information about events taking place on the server. In addition these log files could be extremely valuable in the event of a security threat or incident. These logs should be reviewed regularly. All of these log files should be backed up during the daily backup.

- Running the CONLOG.NLM records all events coming from the console and writes them to the Console Log file, SYS:\ ETC\CONSOLE.LOG. CONLOG should be run from the SYS:\SYSTEM\AUTOEXEC.NCF startup file to capture all console commands being executed from AUTOEXEC.NCF. This file can be set for a certain size and is automatically saved in an archive file once the file size limitation is met.
- System alerts, security violations and system messages are written to the System Error Log file SYS:\SYSTEM\SYS$LOG.ERR. This file is configured by running the SET SERVER LOG with options from the C:\NWSERVER\STARTUP.NCF file.
- Server health information is written into the Server Health Log file, SYS:\SYSTEM\HEALTH.LOG. Email notifications can be sent for critical health issues.
- The Abend Log file has server abend information and is stored in SYS:\SYSTEM\ABEND.LOG.
- There is a Server Personal Log Book file, SYS:\SYSTEM\NRMUSERS.LOG, that can be written to by the server administrator. This log is intended for making any kind of remarks based on changes made to the server by the administrator.
- Once the server is configured, running CONFIG.NLM from the server console or from the NetWare Remote Manager, creates a file called SYS:\SYSTEM\CONFIG.TXT. This file contains a complete listing of server settings, NLMS running on the server, configuration files, startup files, drivers and much more. This file is typically used by Novell tech support for diagnosing server problems. The file can also be used to compare server configurations.
- The server SET command settings can be save in SYS:\SYSTEM\SETTINGS.TXT.
- A web based Server Security Report can be generated and viewed from the NetWare Remote Manager. This report contains server security related information on IP protocols, open ports and programs using them, user connections, volume trustees assignments and admin equivalents.

- The Server Inventory Report is a web based report generated and viewed from NetWare Remote Manager. It contains information on volumes, directories, subdirectories, file types and sizes, space usage and usage trends.
- Two FTP log files, SYS:\ETC\FPTAUDIT.LOG and SYS:\ETC\FPTINTR.LOG contain information on login events and intrusion detection.

There a number of Novell YES approved auditing products for auditing NetWare and eDirectory. These products can be found by visiting Novell's web site.
http://www.novell.com/partnerguide/s100012.html

Novell Nsure Audit 1.0

Novell Nsure Audit 1.0 is a cross platform auditing service used to effectively monitor and track system activity. Compliance with company security policies can be enforced with Nsure Audit. For example Nsure Audit can be set to monitor and log a certain administration event. If the policy is violated two things can now occur. A message can be sent notifying management that the event has taken place. The task that was just performed will automatically be reset. This product can be set up to work with MySQL and can run on Netware, Windows, Linux and Solaris.
http://www.novell.com/documentation/lg/nsureaudit/nsureaudit/data/front.html

AntiVirus, Backup and Additional Server Security

AntiVirus

AntiVirus software needs to be installed on the server and set to scan incoming files. Virus definitions need updated as they become available. Regular virus scans should be scheduled to run on the servers file system. A regular review of the log files is recommended. There are several antivirus solutions that are supported on NetWare. Supported Novell partners for antivirus solutions can be found on Novell's web site.
http://www.novell.com/products/netware/partners/virus.html

Server Backup

Backup and recovery procedures are essential components that need to be incorporated into a NetWare 6.5 server environment. Data recovery is protection against disasters (Business Continuity), server crashes, virus infection and could play a part in incident forensics. Backup logs should be reviewed daily to ensure the backup is working correctly. Lock up backup media and have a system for rotating and removing media from the location for disaster recovery purposes. Supported Novell partners for backup solutions can be found on Novell's web site.
http://www.novell.com/products/netware/partners/backup.html

Additional Server Security Tips

- Always keep the SYS volume for the OS only so that is remains static. This will help prevent the SYS volume filling up and crashing the server. Create additional volumes for data and print queues.

- Disable the Bindery Context on each server if it is not required. This will help prevent the use of hacker tools and save CPU cycles.
- Physically secure your servers in a locked room with air conditioning or good air circulation.
- Connect the server to a UPS and install the UPS monitoring software on the server. If the UPS software has the capability configure the software to shutdown the server if on battery power for a fixed length of time.

General NetWare and NDS/eDirectory Security information

Novell's NetWare was introduced in the early 1980's as a LAN based server centric OS. Server centric meant that all user rights to file and print services on a server were administered from that server. In 1993 Novell Directory Services, NDS, was introduced. NDS gave administrators a much better way of administering users, printers and file systems. NDS has matured into eDirectory and it is now an LDAP v3 compliant Directory. eDirectory is a loosely consistant distributed database and it is the central point of administration in a Novell Tree. In order to have a secure NetWare and NDS/eDirectory environment here are some additional suggested practices administrators must know about and need to perform.

Role Based Services

Through iManager, Role Based Services enable specific administration tasks be placed into a role. A defined set of role based administration tasks is included with iManager. New roles can be created and RBS is very granular. Role based administration is having only the necessary rights needed to perform the job. No more no less. This also fits right into "defense in depth" practice mentioned earlier.

Admin account

- Rename the Admin account and move it in the tree.
- Don't create Admin equivalent accounts. If Admin gets deleted Admin equivalent accounts will no longer have admin privileges.
- Use real user accounts with supervisor privileges to enable good auditing. To many administrators using the Admin account will create an audit trail problem.

Password and account security

- Require real user name accounts. No shared accounts.
- No guest accounts or "everyone" groups.
- Use strong passwords. A minimum of 8 characters, mixing letters, numbers and special characters. An easy to remember passphrase is recommended.
- Set passwords to expire every 90 days.
- Require unique passwords. Novell keeps a history of 8 before reuse is allowed.
- Turn on intrusion detection to refuse a connection after 3 bad attempts.

Summary

Securing the installation of NetWare 6.5, services, applications and server environment is part of defense in depth. It involves installing service packs, patches and security updates. Vulnerability scanning is also a key in discovering and fixing vulnerabilities found in the out of the box installation. Knowing the services that are running and how to secure them closes holes that can be exploited. It is important to how to secure remote access methods and sessions. All of these steps will produce an installation procedure that helps to secure a system. It is also important to keep up with new threats and vulnerabilities. This layered approach to securing the NetWare 6.5 server environment clearly helps to "know thy system".

Appendix - NetWare 6.5 vulnerabilities out of the box

Here are a list of vulnerabilities that the Foundstone scanner found on NetWare 6.5 with Apache, MySQL and Perl/PHP right out of the box with no patches or security updates.

1. OpenSSH buffer_append_space Buffer Overflow CVE CAN-2003-0693

A buffer overflow vulnerability exists OpenSSH allows remote attackers to cause a denial-of-service condition or execute arbitrary code on targeted hosts.

Vulnerable Systems:

OpenSSH prior to 3.7.1

Recommendation:

Download the latest version of OpenSSH for your particular platform.

2. MySQL COM_CHANGE_USER Buffer Overflow CVE CAN-2002-1375

A buffer overflow vulnerability in MySQL allows attackers to execute arbitrary code or crash the MySQL daemon on the targeted host.

Vulnerable Systems:

MySQL 3.23.53 and earlier MySQL 4.0 - 4.0.5 a

Recommendation:

Update to MySQL version 3.23.54 or 4.0.6 and later, available from http://www.mysql.com, or apply SP1.1.

3. Apache mod_alias/mod_rewrite Buffer Overflow CVE CAN-2003-0542

A buffer overflow vulnerability in Apache allows local attackers to execute arbitrary commands on targeted hosts.

Vulnerable systems:

Apache 1.3 - 1.3.28 Apache 2.0 - 2.0.47

Recommendation:

Update to the latest version of Apache, available from http://httpd.apache.org or apply SP 1.1.

The Foundstone scan turned up these 7 medium risk vulnerabilities, descriptions and recommendations:

1. Apache apr_psprintf() Denial-of-Service CVE CAN-2003-0245

A vulnerability in the Apache Web server allows remote attackers to cause a denial-of-service condition on the targeted host.

Vulnerable systems:

Apache Software Foundation HTTP Server 2.0.37 - 2.0.45

Recommendation:

Download and install Apache 2.0.46 or later from http://httpd.apache.org/download.cgi or apply SP 1.1.

2. Apache HTTP Server 'type-map' File Denial-of-Service

A vulnerability in the Apache HTTP server allows attackers to cause a denial-of-service condition on the targeted host.

Vulnerable systems:

Apache HTTP server 2.0 - 2.0.46

Recommendation:

Update Apache to version 2.0.47 or later from http://httpd.apache.org/download.cgi or apply SP 1.1.

3. Apache HTTP Server prefork MPM denial of service vulnerability CVE CAN-2003-0253

A vulnerability in the Apache HTTP server allows attackers to cause a denial-of-service condition on the targeted host.

Vulnerable systems:

Apache 2.0 - 2.0.46 with the Multi-Processing Module

Recommendation:

Update Apache to version 2.0.47 or later from http://httpd.apache.org/download.cgi or apply SP 1.1.

4. Apache HTTP Server FTP proxy server denial of service

A denial-of-service vulnerability in the Apache HTTP Web server allows remote attackers to cause the host to stop responding.

Vulnerable systems:

Apache 2.0 through 2.0.46

Recommendation:

Update Apache to version 2.0.47 or later from http://httpd.apache.org/download.cgi or apply SP 1.1.

5. Apache Redirects and Subrequests Denial of Service

A vulnerability in Apache HTTP Server allows remote attackers to cause a denial-of-service condition on the targeted system.

Vulnerable systems:

Apache HTTP Server 1.3.1 - 1.3.27, Apache HTTP Server 2.0 - 2.0.46

Recommendation:

Upgrade to Apache HTTP Server version 1.3.28, 2.0.47, or greater from http://httpd.apache.org/download.cgi or apply SP 1.1.

6. SSHv1 Protocol Enabled CVE CAN-2001-0572

The SSH daemon has SSH version 1 protocol support enabled.

Recommendation:

Configure the SSH server to disallow SSHv1 protocol support or upgrade it to the most recent release available.

7. SNMP Default Community Name CVE CAN-1999-0517

A SNMP community name is set to the default value e.g. public or private.
Recommendation:
Disable the SNMP service

There was one additional problem encountered not listed as a vulnerability or threat. Running the initial scan soft abended the server 5 times. A soft abend means that the OS recovered from the abend. The server console prompt had (5) after it meaning it soft abended 5 times. If a server is in an unstable state the abends caused by the scan could have caused the server to crash. This could be classified as a Denial Of Service. A review of the SYS:SYSTEM\ABEND.LOG showed that the offending process was XNFS.NLM, which is the NFS daemon. Novell had a patch on their security alert site for fixing this issue, which was a new XNFS.NLM. The verification scan with the XNFS-NESSUS abend fix showed that this resolved the problem as the server did not abend.

References

[1] Ken Neff , “What’s New in NetWare 6.5” , Novell AppNotes, August 2003
http://developer.novell.com/research/appnotes/2003/a0308.htm

[2] NetWare 6.5 Open Source white paper
http://www.novell.com/collateral/4621353/4621353.html

[3] Eric Cole, Jason Fossen, Stephen Northcutt, Hal Pomeranz, “SANS Security Essentials with CISSP 10 Domains - SANS Security Essentials II: Defense in Depth”

[4] Rob Lyon, “Installing and Configuring NetWare AMP(NetWare 6, Apache, MySQL and PHP/Perl)”, Novell AppNotes, December 2002
http://developer.novell.com/research/appnotes/2002/december/05/a021205.htm

[5] Using Apache with Novell NetWare,
http://httpd.apache.org/docs-2.0/platform/netware.htm

[6] Rob Lyon, “An Introduction to MySQL for NetWare”, Novell AppNotes, October 2002
http://developer.novell.com/research/appnotes/2002/october/05/a021005.htm

Apache Software Foundation http://www.apache.org

CERT http://www.cert.org

CVE http://www.cve.mitre.org

eEye Digital Security http://www.eeye.com

Foundstone Inc. http://www.foundstone.com

MySQL http://www.mysql.com

Nessus http://www.nessus.com

Novell Inc. http://www.novell.com

OpenSSH http://www.openssh.com

Putty http://www.chiark.greenend.org.uk/~sgtatham/putty

Secunia http://www.secunia.co.uk

SecurityFocus http://www.securityfocus.com

Symantec Inc. http://www.symantec.com

Talisker http://www.securitywizardry.com/radar.htm

WhichSSL http://www.whichssl.com/