Novell NetWare 6: Beyond file and print

GSEC Practical Assignment V1.4b

Author:	Michel Couturier, CNE
File Name:	Michel_Couturier_GSEC.doc
Date:	2003-04-05

TABLE OF CONTENT

Novell NetWare 6: Beyond file and print
Michel Couturier
GSEC Practical Assignment V1.4b option 1
April 5, 2003

Abstract

Novell has built its reputation upon the NetWare file and print services. However, over the years, NetWare has gradually evolved from the original file and print services to an application server providing an increasing number of services, especially web oriented services. With the objective of making the installation easy, many of these new services are pre-configured and installed by default by the installation process. As a result, NetWare 6 is installing much more applications by default than any previous version. Your basic NetWare server might be running services you may not be aware of. With the increasing number of applications and services being delivered with the NetWare server, it is becoming much more difficult to secure a NetWare server.

This document will examine some of the security issues related to the strict minimum installation of a NetWare server. It will expose ways a secure environment can become insecure and how to secure them. It will also list some known vulnerabilities and how to overcome them.

1 Introduction

Prior to NetWare 6, in a "Defense in Depth" strategy, securing the information stored on a NetWare server was basically limited to securing the network operating system and the physical server. Originally a NetWare server was mainly providing file and print services. With the release of NetWare 6, this is no longer true. To properly secure this version, one must look beyond file and print services. The server now supports a much broader range of protocols and services. Even the most basic installation will include a web server and many web based services. A more elaborate installation will include a second web server and also services to make the server accessible through the Internet and natively by workstations running Windows, Unix or Macintosh operating system. In order to protect the information stored on a NetWare server, your "Defense in Depth" strategy will need to include, not only the network services and the host but also a large range of basic services and applications running on the NetWare 6 server. The "Defense in Depth" of a NetWare 6 server is an on going and a complex process. As Novell evolved toward Web oriented services, they also opened the network to more vulnerability.

The NetWare 6 server is a major change of philosophy in information management. A short history on Novell is needed to understand this evolution and what to expect from this philosophy in order to properly secure the NetWare environment. Although, Novell has lost market share over the years, they still represent over 30 % of the market. Their products are still present in most major corporate networks running along with competitor's products. Over 700 million users are accessing network services through Novell Directory Services (NDS).

Novell NetWare was introduced in 1983 and was designed to be a LAN software based on a file server. One computer managed the network and access to files and printers. Over the years, the popularity of NetWare grew to lead the market with a 70 % market share toward the mid 1990's.

In the early 1990's Novell released NetWare 4 with Novell Directory Service (NDS). The features included centralized users and resources management to meet the requirements for distributed enterprises.

By the mid 1990, Internet revolutionizes the network market. Competition was faster than Novell to join the Internet revolution and gradually reduced Novell's market share. The end result is that the corporate network was no longer based on a single network operating system.

Novell started to make its products Internet ready. In 1998 Novell released NetWare 5 with native support for IP, the Internet communication protocol. A new version of NDS supporting IP was also released. Novell started to promote Web based services on NetWare. When installing NetWare 5.x, a Web server is readily available.

The diversity of platform within the corporate network created an interoperability problem. Novell promoted the NDS as solution to solve this problem and released in 1999 Novell eDirectory, a cross-platform directory service based on interoperability, scalability and open standards.

In 2002, Novell released NetWare 6. With this version, Novell is now positioning its products as a solution to unifying all networks within a one Net world where intranets, extranets and the Internet, wired and wireless work together. In a one Net world, individuals must be able to access their own information, the way they want it, any time, anywhere, from any device. This is quite a statement and Novell has put a lot of energy in adding new services and modifying existing services in order to meet this new philosophy. To achieve this, Novell is complying with an increasing number of standards. (1)(2)

As Novell evolved toward Web application servers they also opened the network to more attacks and vulnerabilities. So, it is important to address the known vulnerabilities of the Novell products to properly secure the data while providing a greater accessibility in a heterogeneous network environment.

In this document, I will first look at some basic elements of securing the NetWare environment. I will describe some ways the administration practices might compromise a secure environment and ways to improve security. Finally, I will list some vulnerabilities with the specific services that are installed on a NetWare server when selecting the strict minimum of a default installation. Most of these services are automatically pre-configure with default values. The large number of services that are part of the minimum installation will probably be a surprise to many. Yet this document will not cover all the other services that can be selected as additional services at the installation time. This document should be considered an overview of what is involved in securing the services running on a NetWare minimum installation. An in-depth analysis of most of these additional services would be required to fully secure the installation.

2 Secure the environment

2.1 The challenge

A search on the Internet demonstrates the complexity to find security risks and vulnerabilities about the Novell products. This does not mean the Novell products are not vulnerable. When attacks occur, they are not always openly known. The Novell products are lesser prone to attacks by hackers because of Novell's reduced market share. With time, more attacks will target Novell's products and more vulnerabilities will be discovered.

2.2 Physical security

The first security measure is to restrict physical access to the servers. The servers should be lock inside a server room and the access to that room should be limited. The greatest damages can be caused from physical access to the servers. This is especially true for NetWare server. This statement is repeated over and over in any security assessment and might seem needless to say, but for various reasons, servers are still often seen being installed in unattended areas where access is not controlled, even in large organizations, and especially in branch offices.

Recommendations

- Install the servers in a lock server room.
- Restrict access to the server room to a very limited number of people; any one else should be escorted at all time.

2.3 Server installation

Administrators like their servers to be identical to one another as much as possible and will often create procedures to do so. Their procedures will often install a very generic server with a complete set of applications and services. Beware of default installations of servers and services. This can create security issues. The NetWare 6 installation process can install a large number of services. To make the installation easy, the services may have default configurations that leave the services wide open to attacks. The "Novell's guide to NetWare 6 networks" book (Hughes and Thomas, 2002) (3) and the "NetWare 6" product documentation (4) fully describe the installation process and the related products. These references will be used throughout this research.

2.4 NetWare

The NetWare operating system and services are installed on volume SYS. Limit the use of this volume to that purpose. Users should not have access to this volume except for very limited access to the LOGIN and PUBLIC directories.

Protect this volume from being filled up by attackers. Create at least one more volume to install print queues and store users' data. It is possible to send simultaneous print jobs that could exceed the size of the volume SYS. If the volume SYS gets filled up, NDS will stop functioning and could get severely damaged, resulting in a loss of service. Any user's data should also be stored on a different volume than SYS for the same reason.

Generally speaking, a well-installed NetWare server has the reputation of being very stable. Network administrators managing NetWare servers pride themselves with long uptime periods for their servers. This stability can be a risk by itself because many administrators will have the tendency to apply patches only when a problem occurs. With the increasing number of services being provided by Netware servers and the compliance to more and more standards, the Netware environment is becoming more vulnerable. Attacks toward NetWare servers are not as widely exposed as the more popular platforms. This can give administrators a false impression of security and can become the weakest link in your network. It is important to apply patches and service packs as soon as possible. Novell often releases the information about vulnerabilities only when they have a fix available. Meanwhile, the word has been spread around in the attackers' world.

Recommendations

- Identity the purpose of the server. Only install the services required to meet this purpose.
- Install Service packs and patches as soon as possible.
- Limit access to volume SYS.
- Install print queues and data s on a different volume than SYS.
- Identify default accounts when installing servers and services and review assigned rights.

3 NDS Administration

3.1 Administrator accounts

The installation process of a NetWare 3.x server and prior versions, created a default administrator account with the permanent name of SUPERVISOR. This account has full rights to the file system of the server and the account database called the BINDERIES.

For NetWare 4.x and above, the installation process of the first NetWare server requires the creation of an administrator account and a password must be set. The suggested name is ADMIN but can be renamed. This administration account has supervisor rights to the root of the NDS tree and the file system.

Another administrator account called SUPERVISOR is also created for backward compatibility and cannot be renamed. This account is created with the same password as the ADMIN account at creation time. The password for SUPERVISOR is not synchronized with the ADMIN password when either one is changed. This account is not listed as a directory object and can only be managed under bindery emulation. Generally speaking, this account is never used and is not a concern as long as a bindery context is not set. Unfortunately, the experience shows that at one point or another, there will be an operational need to set a bindery context on one or more servers. At this point on, the account is accessible and can be used to access the server with full rights to the file system. If an attacker could successfully set a bindery context on a server, this account could be used to create and/or administer NDS object under bindery emulation.

Recommendations

- Create a second administration account with a different name than ADMIN and place the object in a different container. Assign specific supervisor trustee assignment for this new object to the ROOT object of the tree. (Do not make the new account an equivalent to the ADMIN object). Remove the supervisor trustee assignment of the original ADMIN account on the ROOT object. (Do not do this before the new administrator account has been created).
- Enforce intruder lockout at the container level (organization units).
- Change the SUPERVISOR account password even if you are not using the account. Disable the account.
- Create a group or a role to manage administrator accounts and rights.

3.2 USER Account

Prior to NetWare 4.x, a user account was created at every server where a user needed to access shared resources. With NetWare 4.x and above, the access to the resources is controlled and managed through NDS. The administrator only needs to create a single account to grant access to any resources managed by NDS. This account is accessible anywhere within the network.

Recommendations

- Set up a template object based on your security policy to create users.
- Assign the least required rights to the accounts.
- Use roles and groups to assign rights and trustees to users.
- Use a Group or role to manage administrator accounts
- Do not create GENERIC account for user access. Avoid using a “Guest” account.
- Create system accounts to be specific to only one system with limited rights.
- Force periodic password change and minimum password length.
- Set expiration date to temporary employees and contractors.
- Enable Intruder lockout at the container level (organization unit).

3.3 Rights to NDS

NDS uses containers to organize objects. The containers in NDS are similar to directories in a file system.

Rights and permissions given on a container to a specific object will flow down to all other objects within that container. This might represent a much easier way of assigning rights to a large number of objects than granting rights to every object within a container. But before doing so, you must be aware of a few side effects you might not have expected.

All rights given on an upper level container can be filtered, including supervisor rights. A user with excessive rights could use this feature to create an additional container and cut off the visibility to central administration, therefore hiding the container and its objects.

Although, NDS is completely independent from the file system rights, the NetWare server objects and the volume objects are special integrated objects that allow rights given on these objects to flow down to the file system. These rights may be specifically given or inherited from the container. In other words, if you grant Supervisor to a user on a server or a specific volume object, the user will also be supervisor of the entire file system or to that specific volume. In fact, the user only needs to get the “Write” permission on the server object to become Supervisor of the entire file system of this server! Be sure you fully understand the impact of such features and side effects. Know who has rights to your server and volume objects. Use tools such as DSSEC.EXE (6) to periodically check and report security issues in NDS. Enable auditing on NDS.

By default, public is made trustee of the ROOT object with ”Browse” rights that flows down to all other containers and objects. This will allow anyone connected to the network to browse the NDS tree without being authenticated in NDS. There is no NDS object to represent this object. It can only be managed through the ROOT object itself or through each individual objects.

Investigate if this right could be removed in your environment. One side effect of removing the right to public is, you no longer can use context less login. The user has to specify its full context to login.

Recommendations

- Enable auditing on NDS.
- Periodically run DSSEC utility to monitor conformance to your security policy.

3.4 Rights to file system

Rights given a directory will flow down to files and directories it contains. It is possible to set an inheritance right filter to block the inheritance of the rights. The supervisor right to the file system cannot be blocked.

On the NetWare file system, by default "Read" and "File scan" are granted to public on the SYS:LOGIN directory. Some of the tools installed by default in this directory could be used to gather information and to attack the network.

Once logged in, any user with minimal rights is granted "Read" and "File scan" to SYS:PUBLIC directory. This directory contains many general network tools and most administration tools. These tools can be used to gather more information than needed to attack the network. Remove or move these tools to a restricted directory. Most users don't need these tools. (7)(8)

Recommendations

- Enable auditing on NDS.
- Periodically run DSSEC utility to monitor conformance to your security policy.
- Use tools to find hidden objects.
- Run utilities to report rights assignments to the file system.
- Remove from SYS:\PUBLIC directory all administration tools and any other network tools not required by users.
- Restrict access to administration tools like NWADMIN.exe, NLIST.exe, CX.exe, and ConsoleOne.

4 Network protocols

NetWare support many network protocols. Prior to version 5, all versions required IPX/SPX to be installed. IPX relies on broadcast to access servers and services. All the servers and services names and addresses are broadcasted every minute throughout the network. An attacker only needs to connect to the network and record the broadcasts to get a full layout of the network services running over IPX. Don't install IPX unless you need it for backward compatibility. If you don't need it, don't install it. Install only the network protocols you really need. IP is fully supported on NetWare and NDS since NetWare 5. IP can be the only protocol installed. Note that IP packet forwarding and IPX routing are enabled by default, unless you intend to use the server as a router, disable packet forwarding and routing to avoid routing through the server. This can be done in INETCFG console.

NetWare has some specific parameters available to improve security and to help protect against specific attacks. They are not all set by default. These parameters can be set in the Monitor server settings or by adding them to the AUTOEXEC.NCF command file.

Parameters	Recommended	Default
Allow Unencrypted Passwords	OFF	OFF
Allow Audit Passwords	OFF	OFF
Automatically Repair Bad Volumes	ON	ON
IPX NetBIOS Replication Option	0	2
Additional Security Checks (Be careful with this one if you have mixed NDS version in your tree. It is not backward compatible with previous version of NDS**)**	ON	OFF
TCP Defend Land Attacks	ON	ON
TCP Defend SYN Attacks	ON	OFF
Reject NCP Packets with bad components	ON	OFF
Reject NCP Packets with bad lengths	ON	OFF

It is possible to make a "Man in the Middle" attack against Novell NetWare. (9) Novell has released the patch TCP605o.EXE that contains a fix against a "Man in the Middle" attack over TCP/IP. (10)

Recommendations

- Install only the required protocols.
- Review and adjust the settings for the listed parameters.
- Install latest network protocol patches.

5 Default Services

This section covers only the minimal NetWare installation by not selecting any of the additional services available at the installation time.

5.1 Remote Server Management

Many server management tools are accessed at the server itself. These are relatively safe as long as the server is physically kept secured. But this can be annoying and many administrators will use remote access tool to connect to and manage the NetWare servers. The previous remote management tool offered weak security. The password is either saved in clear text or with an encryption code that can easily be broken. (11)

As NetWare evolved toward Web services, Novell has developed new Web based management tools. These new tools now use SSL to provide a more secure communication between the server and the administration workstation. These management tools now use NDS for user authentication.

Novell Remote Manager is one of these tools. This manager is installed by default on every NetWare 5.x and 6.x servers. There are still some security issues you should address before running this service. The NetWare 5.x remote manager displays excessive information without requiring the user to authenticate. The remote manager will display information like the server name, software versions for the operating system and all loaded modules. This is enough information to satisfy an attacker who wants to exploit vulnerabilities of unpatched systems. Use address filtering to limit access to port 8008 and 8009. In NetWare 6, the information is only available once the user is authenticated. You can and you should configure the Remote manager to restrict access only to specific IP addresses or range of addresses.

The Netware remote manager has recently been patched to fix a buffer overflow issue for both NetWare 5.x and 6.0. The updated version is 1.10b for NetWare 5.1 and 2.00 for NetWare 6.0. (12)(13)

There is a potential security issue where a user could login using an expired account. (14) This situation may occur on a NetWare 5.1 server running NDS 8.5. The problem was fixed with Service pack Netware 5 SP5 and NDS85.30.

Another security issue exists with RconsoleJ, the Java remote console. After applying NetWare 6.0 service pack 2, and when running RconsoleJ in secure mode, a user could gain access to the server without a password. (15) This issue was fixed with the remote console agent RCONJ6.NLM Version 6.10a dated 2002-08-20. (16)

Recommendations

- Do not use rconsole.
- Use Novell Remote manager, running only with the latest updates.
- Configure Netware Remote Manager to be accessed only by specific IP addresses or subnet range of addresses.

5.2 SNMP

This service is loaded automatically at startup. The default installation will enable the Monitor Community and the Control Community to PUBLIC. Change the community names to a different name. Disable Control community if you don’t need it. You can manage SNMP using INETCFG server utility. Select Manage configuration then SNMP Parameters. Modify the States to Specified Community May Read and Specified community May Write. Change the community strings. You may also set the trap community not to send traps or to send with specified community. The configuration is stored in SYS:\ETC\NETINFO.CFG and the trap destination address must be specified in the file SYS:\ETC\TRAPTARG.CFG.

There are multiple vulnerabilities reported on SNMP. (17) The vulnerabilities have been fixed with SNMP.NLM version 4.16b dated 2002-02-15. The fixes are included NetWare 5 SP4 and Netware 6 SP1. (18)

5.3 SLP

The Service Location Protocol is an Internet standard protocol. It is a method of discovering infrastructure services in the TCP/IP environment. It provides basically the same service in an IP environment, as SAP would do in an IPX environment. With the default configuration, the agents will use multicast for the discovery of services. The client will also use multicast to query for services. Any client is allowed to query the database to find these services using multicast and an agent will reply. Attackers could use SLP to gather information about your network. Avoid the default dynamic configuration and set SLP to use a static configuration. Define your own name, don't use the default scope name "Unscoped". Configure SLP to store the services in NDS using a single scope. Create a partition of SLP scope container. Replicate this partition to every server running the Directory Agent (DA). Every server except the DA servers should have the address of a DA server in the file SYS:\ETC\SLP.CFG. In monitor, set the SLP DA Discovery Options to 4. This will disable the dynamic discovery. The server will use the address in the file to send information to the DA. Enter the name of the scope in the SLP Static Scope List. Use your DHCP server to send the SLP DA address and scope name to the workstations. You can also set static information yourself in the workstation NetWare client configuration.

Recommendations

- Block port 417 to the outside world at the firewall.
- Set SLP to use static service discovery.
- Register the services in a named scope.
- Use NDS to replicate the information to all DA's.
- Configure your workstation to query a specific Directory Agent, set manually or by the DHCP.

5.4 NTP - Timesync

Network Time protocol. (NTP) is used to synchronize time on Network devices. NetWare supports this protocol. The functionalities have been included in the TIMESYNC.NLM. There are no known vulnerabilities with this service on NetWare.

5.5 LDAP

Novell supports the Lightweight Directory Access Protocol v3 (LDAP) in its implementation of NDS. It is possible at the installation time to set this protocol to accept clear text password. This should be avoided.

A denial of service attack has been reported in NetWare 5 and NDS 8.5. It was possible to create a buffer overflow condition that would Abend the server by entering a very long user name and password. The problem was fixed with the NDS patch ds8520c.exe. (19)

A security issue exists with LDAP when a GroupWise 6 post office is configured to uses LDAP to authenticate the users. A user could try to authenticate using the last user identification in the login interface without a password. After a few trials, LDAP would eventually authenticate the user as anonymous and access would be granted to the user's mailbox. (20) An easy workaround is to use only NDS for authentication in GroupWise. If you need to use LDAP then specify the NDS account and password in the LDAP user field in the post office configuration details. The post office agent will use this account to log into LDAP and authenticate GroupWise users. The problem was fixed with the patch FGW62N5.EXE now included in GroupWise6 SP2. (21) A fix is also available to disable anonymous login in LDAP. (22)

Recommendations

- Use only NDS for GroupWise client access.
- If you must use LDAP for GroupWise, specify which user and password the post office will use to log into LDAP.
- Apply the patches and latest service pack as soon as possible.

5.6 Novell Certificate server

The early releases of the Novell Certificate server were called Novell PKI service. The Novell Certificate server provides a set of services that enables the use of public key cryptography and digital certificates in an NDS environment. Some of the services related to the Certificate server are the Public Key Infrastructure service (PKI) to generate private and public keys, the Novell International Cryptographic Infrastructure (NICI) and the secure Authentication Services. The installation of the first NetWare server will also create your own Organizational Certificate Authority (CA) within NDS and install the Novell Certificate Server on this server. This service will be used to issue Server certificates and User certificates. Every server added to the tree will need to access the certificate server to obtain a server certificate. The PKI service will use these certificates to generate Public and Private Keys. The NICI service will use the keys along with some mathematical algorithm for encryption to provide secure communication. The Secure Authentication Service (SAS) will also use them to provide secure user authentication. You can act as your own Certificate Authority and issue an unlimited number of server and end-user certificates at no charge. You can also use the services of trusted certificate authority external to your organization for a fee. This may be required if you provide services outside your organization through Internet using secured communication. Other organizations or users may not trust your certificate if they are not certified by a trusted certificate authority. (23) (24)

The major concern about the certificate server is that it is extremely important in the NDS environment. It is the basis of your secure communication. If you need to remove the first server installed in your tree, be sure the certificate server is moved to another NetWare server. Otherwise, you will not be able to install a new server into your NDS tree since you would no longer be able to issue new certificates. All the certificates already issued will be invalidated, although the service relying on the certificate will continue to work until the certificate expires. If you install a new certificate authority, all certificates issued will need to be replaced.

There is a compatibility issue between the early PKI service version 1.x and the Certificate server 2.x. If the Certificate authority is running on a NetWare 4.x or NetWare 5.0 server, you will not be able to add a NetWare 5.1 or NetWare 6.x server because the CA must be running on Certificate server 2.x. You will have to upgrade the server hosting the CA first and then install the additional NetWare 5.1 or NetWare 6.0 server. (25)

Some people may have concerns about a security issue regarding SSL vulnerability. The NetWare implementation is not affected by this vulnerability since SSL is implemented differently. (26)

5.7 Storage Management Service

The Novell Storage Management Service is a collection of services that provides backup, restore and data migration. It is platform independent and can be use to backup eDirectory, file systems and workstations. A Target Service agent (TSA) is installed on the target system and a backup utility will use the SMDR component to communicate with the TSA.

The SMS also include the basic backup utility SBCON.NLM. There is a security issue with SBCon in NetWare 5.1. After submitting a backup job using SBCon a queue file is created (i.e.: SYS:\QUEUES\xxxxxxxx.QDR\xxxxxxx.Q). If the xxxxxxx.Q is viewed through any text viewer (i.e. NOTEPAD.EXE) both the backup job submitter name and their password are displayed in clear text. This has been corrected and there will be encryption of the username and password in the SYS:\QUEUES\xxxxxxxx.QDR\xxxxxxx.Q file when using SBCon. (27)

There is a denial of service vulnerability when running with IPX compatibility enabled on NetWare. Novell SDMR DoS. (28) To fix the problem disable IPX compatibility and install the update TSA5up11.exe 2002-11-21. (29)

5.8 NetWare Web Manager

NetWare Web Manager is a browser-based management tool. It is the front door used to access the NetWare browser-based management tools, such as NetWare Enterprise Web server, NetWare Remote Manager, iMonitor, FTP server, etc. Other management tools will be integrated as you install more services to the NetWare server. It is accessed via the NetWare server IP address and IP port 2200.

It is important to note that NetWare Web manager relies on the Apache Web server not the NetWare Enterprise Web server. Even if you choose to install the NetWare Enterprise server, the NetWare Web Manager will be installed along with Apache Web server as a basic service.

5.9 NDS iMonitor

NDS iMonitor is a web based management tool for managing eDirectory. It provides monitoring and diagnostic tools similar to the server based tools DSBROWSE, DSTRACE, DSDIAG. It can be accessed with a web browser using HTTPS with the server IP address on port 8009. It Integrates into NetWare Web Manager and Remote server manager. The information is displayed based on the identity of the user. The default value does not restrict the use of the tool. The version 1.0 grants access based on rights. This implies that anyone can access without authentication and view anything Public as rights in eDirectory.

In versions 1.5 and 2.x, the user must be authenticated as a valid user to access. This is a very powerful tool and can provide quite a lot of information. The access to this tool should be restricted to the administrators.

Setting the value of the LockMask parameter to 2 in the configuration file SYS:\SYSTEM\NDSIMON.INI can restrict the access. It will require that a user be authenticated as a supervisor to gain access. Make a copy of the NDSMON.INI file as it might be overwritten when you apply your next NetWare 6 service packs and reapply the changes after the service pack. (30)

There is a denial of service vulnerability that can be generated by entering a long username and password at login. This has been fixed with patches NW51SP5 and NW6SP2. (31)

There is another Denial of service issue with iMonitor delivered with eDirectory 8.6.2. This is fixed in iMonitor version 1.5.5. (32)

Recommendations

- Limit access to iMonitor to Administrators only by modifying the NDSIMON.INI file.
- Make a copy of the configuration file NDSIMON.INI.

5.10 Novell iManager

Novell iManager is a browser-based tool used for administering, managing, and configuring Novell eDirectory objects. Novell iManager is design to manage services based on roles. You basically assign specific tasks or responsibilities to users by adding groups or users to specific role based objects. When accessing iManager, the users will be presented with only the tools they are allowed to access. In NetWare 6, you can use Novell iManager to administer Novell iPrint, DNS/DHCP, and Novell Licensing Services. You can create your own role based service objects to manage other services. To simplify your management, you should assign the roles for managing services to groups and make the users members of the specific groups.

There is a buffer overflow vulnerability if you're running a version prior to iManager 1.2. (33) The problem will happen if more than 256 characters are passed in the username field. The problem is fixed in iManager 1.22 patch emfrm122.exe. (34)

Recommendations

- Create groups to manage your services and add the groups to the specific role based service objects.
- Apply latest patches.

5.11 Apache Web Server

Apache Web server is an open-source Web server. It is an integral part of the Web infrastructure of NetWare 6. Apache is installed by default during the

NetWare 6 installation and is the main component of NetWare's Web based services. NetWare Web Manager, Novell iManager, iFolder, NetWare Web Access, NetWare Web Search Manager, all use it.

Apache is a very high profile web server and is used by more than 60% of all web sites. Being open source, the hackers have full access to the source code and can scrutinize every line of code for vulnerabilities. When vulnerabilities are found, the information is quickly distributed. Therefore, it is very important to apply security related patches as soon as possible.

There are several security issues that were discovered since the release of NetWare 6.0. The NetWare 6 service pack 2 includes Apache version 1.3.26 and fixes some of the security issues. (35)

The current version of Apache is version 1.3.27 and corrects more security issues. (36)(37). It is basically a security related release. It can be downloaded directly from the Apache web at the following link. http://nagoya.apache.org/mirror/httpd/binaries/netware/apache_1.3.27_netware-mp.zip (38)

More security issues are currently under investigation. (39)

There were some concerns about a security issue regarding OpenSSL vulnerability on Apache. The NetWare version is not affected by this vulnerability since SSL is implemented differently. The MOD_SSL and OpenSSL do not exist on NetWare. SSL is handled by NILE through Winsock.(40)

Recommendation

- Apply Apache updates as soon as possible.

5.12 Tomcat 33

Tomcat is a servlet engine used to serve up Web applications and is also developed by the Apache Group. Tomcat is installed by default on the NetWare 6 server. It runs Java servlets and is used by several NetWare 6 components like the NetWare Web Search Server. Tomcat is proposed as an alternative to IBM Websphere, which is also available on the NetWare CD with the additional product bundle.

NetWare 6 comes with several Tomcat example accounts with default passwords. These accounts give access to several example directories and scripts. These account names and passwords are specified in the following files:

- Sys:\tomcat\33\conf\users\admin-users.xml
- Sys:\tomcat\33\conf\users\example-users.xml
- Sys:\tomcat\33\conf\users\global-users.xml
- Sys:\tomcat\33\conf\users\tomcat-users.xml

The example directories are located under SYS:\tomcat\webapps\examples.

These example accounts, files and directories should be removed. (41)

There are several security issues currently under investigation. Apply patches as soon as these issues are resolved. (42)

Recommendations

- Remove example accounts, files and directories.
- Apply Tomcat updates as soon as possible

5.13 JAVA

The NetWare installation will also install several Java based components. This will include the Java Virtual Machine (JVM) modules from Sun Microsystems and the Java just in time compiler (SYMJIT) from Symantec. ConsoleOne on the NetWare server is one application using these components. The Java installation includes some samples installed in the SYS:\JAVA\SAMPLE directory that allows browsing in the NDS tree. This directory should be removed.

The current Java version is 1.31 contains some vulnerabilities. (43) Novell has corrected these vulnerabilities and is currently testing the version JVM 1.41. (44)

Recommendations

- Remove sample accounts, files and directories.
- Apply patches as soon as available.

5.14 PERL

PERL is a scripting language that is especially useful for working with text files, generating reports, dynamic Web pages and automating server tasks. PERL is an open source programming language with a very wide distribution and is available for most platforms.

PERL installation contains a sample directory under SYS:\PERL\WEBDEMO. The default installation of Apache does not include extensions to execute these sample scripts but the extension module MOD_PERL for Apache is available and is included in the updated PERL version 5.8. If you chose to install Novell Enterprise Web Server, then the PERL extension is already installed with this web server. These samples allow disclosure of valuable information. The sample directory should be removed. (45)

There are several vulnerabilities that have been fixed in patch perl5002.exe. (46)(47) This patch is included in NW6SP2 service pack. This PERL version also forces authentication when users try to access restricted files on the server. The control parameter is located in the file SYS:\SYSTEM\NWSEC.INI and is enable to ON by default.

Recommendations

- Remove sample directory
- Install latest updates.

5.15 NetBasic / NSN

NetBasic is an interpreter that allows running Basic-like programs on NetWare. The current version is 6.0 and is installed by default under SYS:\NETBASIC. It is the predecessor to the Novell Scripts for NetWare (NSN).

NSN is an interpreter compatible to ANSI basic and VBScript. It can be used to build dynamic Web pages or server application. This interpreter is installed under SYS:\NSN.

Both NETBASIC and NSN directories contains sample scripts and utilities that can be used to attack the network. Remove any sample scripts and any utility that could disclose information. (45)

Vulnerability in NetBasic Scripting Handler could allow a remote attacker to traverse directories on the Web server. (48)

A patch is available to fix directory traversal and the buffer overflow vulnerabilities. (49)

Recommendations

- Remove sample scripts and utility scripts that pose a threat to security.
- Apply patches as soon as possible.

5.16 UCS

The Universal Component System (UCS) is an interface to different components systems and different programming and scripting languages. This makes the components reusable between the different programming and scripting languages. Under NetWare these languages are generally Java, NSN, PERL, C, C++. There is no known vulnerability specific to this service.

5.17 Pervasive SQL 2000i

Pervasive SQL 2000i is in fact Btrieve SQL database. NetWare 6 installs Brief 7.9x version. It is used mainly for NetWare system databases. Some additional NetWare products will also use Btrieve for managing local databases.

No security issues could be found for this product on NetWare.

6 Additional Novell products

The NetWare installation process offers the possibility of installing, along with the NetWare server, a set of additional Novell products. Although they are optional, some were already selected and had to be deselected in order to get the minimal installation. They are not be analyzed of this research. If you intend to install any of these products, you should be aware that there are some security issues that need be addressed.

The following Novell products are available with the NetWare installation.

- NetWare Enterprise Web Server.
- NetWare FTP server.
- NetWare Web Search.
- Novell DNS/DHCP Services.
- Native file access protocols for Windows, Macintosh, and Unix.
- Wan Traffic Manager Services.
- NetWare Web Access Interface to NetWare 6 using portal services.
- Novell IFolder Services.
- Novell NetStorage.

7 Conclusion

The evolution of the NetWare server toward Web based services has brought a lot more capabilities to the server. At the same time, it also brought a lot more vulnerabilities. Securing a NetWare server now represents a greater challenge. Beware of the default installation. You might get more than what you wish for. The default installation can leave the server wide open to attackers.

Maintain servers up to date with patches and service packs. Control and secure the basic services before adding any additional services. Find your vulnerabilities before someone else does. There are solutions to these vulnerabilities. Be alert to new vulnerabilities and apply fixes as soon as they are released. Regularly check conformance to your security policies. Most attackers are more interested in exploiting known vulnerabilities in systems than finding new ones.

References

1 Novell. “Novell History” Pressroom
URL: http://www.novell.com/news/press/pressroom/history.html (02 Feb 2003).

2 Novell. “Novell execution of “one net” – Critical corporate Milestone”. 2002. URL: http://www.novell.com/news/press/pressroom/milestones2002.pdf (02 Feb 2003).

3 Hughes, Jeffrey F. and Thomas, Blair W. Novell’s Guide to NetWare 6 Networks. San Jose, Novell Press, 2002.

4 Novell. “NetWare 6” Product documentation. Aug. 2002.
URL: http://www.novell.com/documentation/lg/nw6p/index.html (Mar. 2003).

5 Securiteam.com “Novell Netware Default settings expose sensitive system information” (11 Dec.2000).
URL: http://www.securiteam.com/securitynews/6L00C0K0AE.html (2 Mar. 2003).

6 Novell. “DSSec.exe: Report NDS Security Issues”. 6 Mar.2003.
URL: http://www.novell.com/coolsolutions/tools/1637.html (2 Apr. 2003).

7 Novell. “Miscellaneous Security Tips” Appnotes June 2000. 28 Jun. 2000
URL: http://developer.novell.com/research/appnotes/2000/june/03/a0006012.htm (2 Mar 2003).

8 Foust, Mark. “NetWare security: closing doors to hackers” Appnotes June 2000. 07Jun. 2000. URL: http://developer.novell.com/research/appnotes/2000/june/03/apv.htm (2 Mar. 2003).

9. Securiteam.com. “MITM Attacks Against Novell NetWare” 19 Feb. 2001
http://www.securiteam.com/securitynews/5CP0D2K3GK.html (02 Mar. 2003).

10. Novell. “TCP update 6.05o for NetWare 6 - TID2964249” 04 Dec. 2002
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2964249.htm
(03 Feb. 2003).

11. Securityfocus. “Netware Remote.NLM Weak Encryption Vulnerability”. 01 Jun1999. URL: http://www.securityfocus.com/bid/482/info. (15 Feb. 2003).

12. Securiteam.com. “Netware Remote Manager Found to Contain a Buffer Overflow” 04 Apr. 2002. URL: http://www.securiteam.com/securitynews/5EP01156VW.html (15 Feb. 2003).

13. Novell. “Portal.nlm to address code red worm attack TID296847” 30Jan. 2003. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2964847.htm (15 Feb. 2003).

14. Securityfocus. “Novell eDirectory Expired Password Vulnerability” 12 Nov. 2002. URL: http://www.securityfocus.com/bid/6163/discussion (15 Feb. 2003).

15. Securityfocus. “Novell NetWare 6.0 SP2 RConsoleJ Authentication Bypass Vulnerability” 21 Aug. 2002. URL: http://www.securityfocus.com/bid/5541 (15 Feb. 2003).

16. Novell. “RCONAG6.NLM for servers running NW6SP2 - TID2963349”. 21JAN2003. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2963349.htm (15Feb. 2003).

17. CERT.ORG. “CERT Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)”. 12 Feb. 2002). URL: http://www.cert.org/advisories/CA-2002-03.html (23 Feb. 2003).

18. Novell. “SNMP vulnerability fix for NW 4.x, 5.x, 6.x”. 07 Mar. 2002. URL: http://support.novell.com/servlet/tidfinder/2961546 (23 Feb. 2003).

19. Novell. “Denial of Service attack in NLDAP.NLM - TID10066712”. 13 Sep. 2002. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10066712.htm (23 Feb. 2003).

20. Securiteam.com. “Security Issue with GroupWise and LDAP Authentication in Post Office (Anonymous bind)”. 2002-03-03. URL: http://www.securiteam.com/securitynews/5EP000A6LK.html (23 Feb. 2003).

21. Novell. “GroupWise with LDAP Authentication Security Details. - TID1006792” 10 Feb. 2003). URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10067921.htm (23 Feb 2003).

22. Novell. “How to disable anonymous binds in LDAP - TID10077872”. 12 Feb. 2003. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10077872.htm (23 Feb. 2003).

23. Novell. “Novell Certificate Server v2.0 FAQ - TID10023843”. 14Feb. 2003. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10023843.htm (25 Feb. 2003).

24. Novell. “Understanding how NICI/PKI/CS works - TID10064202”. 23JAN2003. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10064202.htm (25 Feb.2003).

25. Novell. “How do I upgrade from PKI Services 1.x-TID10055253”. 09 Jan 2002. URL: http://support.novell.com/cgi-in/search/searchtid.cgi?/10055253.htm (25 Feb.2003).

26. Novell. “How does Novell implement SSL? - TID10074700”. 20 Sep. 2002. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10074700.htm (25 Feb. 2003).

27. Novell. “Encryption of username and password in SBCON - TID2959357” 07 Jun. 2001. URL: http://support.novell.de/cgi-bin/search/searchtid.cgi?/2959357.htm (28 Feb. 2003).

28. Novell. “ Novell Netware SMDR.NLM Denial of Service Vulnerability”. 08 May 2002URL: http://www.securityfocus.com/bid/1467 (28 Feb.2003).

29. Novell. “Latest sms updates for nw4, nw5 and nw6 - TID2964311’. 21 Nov. 2002). URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2964311.htm (28 Feb. 2003).

30. Novell. “Securing access to your iMonitor environment - TID10075969”. 07 Nov. 2002. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10075969.htm.(28 Feb.2003).

31. Novell. “Consolidated Support Pack 8 Changes since last support pack. - TID10073558” 30 Dec.2002. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10073558.htm (28 Feb. 2003).

32. Novell. “iMonitor update for eDirectory 8.6.2”. 22 Oct. 2002. URL: http://support.novell.com/servlet/tidfinder/2964032. (28 Feb. 2003).

33. Securityfocus.com. “Novell Netware eMFrame iManage Buffer Overflow Vulnerability” 11 Nov. 2002. URL: http://www.securityfocus.com/bid/6154 (04 Mar. 2003).

34. Novell. “iManager 1.22 - TID2963651”.08 Oct. 2002. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2963651.htm (04 Mar. 2003)

35. Novell. “Apache Chunked encoding vulnerability CAN-2002-0392 - TID10072204”. 09 Aug. 2002. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10072204.htm (20 Mar. 2003).

36. Mitre.org. “Can-2002-840 (Under review) 17 Mar. 2003. URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0840 (21 Mar.2003).

37. Mitre.org. “Can-2002-843 (Under review) 17 Mar. 2003. URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0843 (21 Mar.2003).

38.Apache.org. "Apache 1.3.x for NetWare binaries". 03 Oct. 2002. URL: http://nagoya.apache.org/mirror/httpd/binaries/netware/apache_1.3.27_netware-mp.zip (21 Mar. 2003).

39. Novell. "Potential Security Vulnerability with Apache Web Server on NetWare - TID10080124" 10 Feb. 2003. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10080124.htm (21 Mar. 2003).

40. Novell. "How does Novell implement SSL? - TID10074700". 20 Sep. 2002. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10074700.htm (21Mar. 2003).

41. Novell. "Potential Security Vulnerability with Tomcat on NetWare 6 - TID10073346". 10 Oct. 2002. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10073346.htm (25 Mar. 2003).

42. Novell. "Potential security vulnerability with Tomcat 4.x on NetWare 6 - TID10078117". 25 Jan. 2003. http://support.novell.com/cgi-bin/search/searchtid.cgi?/10078117.htm (25 Mar. 2003).

43. Cert.org. "CA-2002-07 Double free bug in zlib compression library". 20 Jul. 2002. URL: http://www.cert.org/advisories/CA-2002-07.html (25 Mar.2003).

44. Novell. "BETA 2 Novell JVM 1.4.1 for NetWare - TID2965154" 12 Mar. 2003. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2965154.htm (25 Mar.2003).

45. Novell. "How to restrict access to NDS information through the NetWare Enterprise Web - TID10064452". 12 Dec. 2002. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10064452.htm (28 Mar. 2003).

46. Novell. "Perl Vulnerability Patch - TID2963307". 16 Aug. 2002. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2963307.htm (28 Mar. 2003).

47. Novell. "Potential security vulnerability in Perl handler-TID10073338".24 Jan. 2003. URL: http://support.novell.com/cgi-in/search/searchtid.cgi?/10073338.htm (28 Mar. 2003).

48. Securityfocus.com "Novell NetBasic Scripting Server Directory Traversal Vulnerability". 20 Aug. 2002. URL: http://www.securityfocus.com/bid/5523/info/ (28 Mar. 2003).

49. Novell. "NetBasic buffer/scripting vulnerability patch - TID2963297".16 Aug. 2002. URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2963297.htm (28 Mar. 2003).