Novell Directory Services:
Pandora - Security Hacks
Sanjeev Kumar Sood

Introduction

This document is about a project called Pandora developed by Simple Nomad and sponsored by Nomad Mobile Research Center, and which provides tools for getting into Novell's premier product: Novell Directory Services (NDS). NDS is an X.500 directory-scheme based distributed database for NetWare 4.x and 5.x, which provides access to all network resources. It allows a user to use a single login to a Netware environment. The foundation of the Directory tree is established through container objects and these objects represent organizational and physical structure of the network. Container objects contain other Directory objects and container objects provide a means for logically organizing all other container or leaf objects in the tree. At least one Organization (O) objects exists directly under the [Root] object. It identifies an organization's name and provides a level of administration for the entire tree. The lower layers of tree contain Organizational Unit (OU) objects and Leaf objects. The OU objects typically represent functional groups as container objects. This structure is then divided, or partitioned, into pieces - usually based on geographic location, and usually at the organizational units. For redundancy and efficiency, these partitions are then copied, or replicated, to various servers throughout the network. The goal is that a user will authenticate to a replica on a local server, without having to go across slow WAN links. NDS Manager (NDSMGR32.EXE0 and NetWare Administrator (NWADMN32.EXE) are two tools to manage NDS.

By default all users, whether authenticated or not, have read and file scan access to the SYS:\LOGIN directory. This is where the files needed to authenticate a client reside. Another location, PUBLIC, has default browse rights to NDS itself from [Root] down for all users. A user with no rights can browse NDS and record user names, contexts and other public information, and this information can be very valuable for account cracking and social engineering issues.

Inside NDS

NDS consists of four main files. On Netware 4.x, these files include PARTITIO.NDS, ENTRY.NDS, VALUE.NDS, and BLOCK.NDS. On Netware 5.x, the file names have an extension of DSD instead of NDS, and a new file with an extension of DSB is present: 0.DSD, 1.DSD. 2.DSD and 3.DSD. These files are located on the SYS: volume in a hidden directory, called _NETWARE, and this directory cannot be accessed from any user login including Admin. All objects addressed by server are located within the ENTRY.NDS file. Values associated with ENTRY records are stored in one and sometimes two files. VALUE.NDS will contain up to 16 bytes of data about an ENTRY record. The partition information is contained within PARTITIO.NDS file.

There are two methods by which NDS can be accessed:

The first method is getting direct console access or using RCONSOLE and then loading NLMs (like JCMD.NLM and NETBASIC.NLM) which allows access to SYS:_NETWARE. Loading NETBASIC and typing 'shell' generates a DOS-like environment and you can copy *NDS files to another location on the server. On larger systems, it is recommended that DS.NLM must be unloaded to do this.

The second method uses DSMAINT.NLM or DSREPAIR.NLM (available at http://www.novell.com) DSMAINT creates a file called BACKUP.DS and DSREPAIR creates DSREPAIR.DIB. If the server is compromised, this can be done easily and these files can be generated.

An additional point to mention here is that RCONSOLE is a clear-text utility. By default the RCONSOLE password is recorded in SYS:\SYSTEM\AUTOEXEC.NCF in clear text. In the INETCFG.NLM utility has been invoked, then this is stored, again in clear text, in SYS:\ETC\NETINFO.CFG. Editing an AUTOEXEC file or calling INETCFG is a task that is frequently done in an RCONSOLE session, and thereby exposing the password to the tool itself.

Vulnerabilities in Novell NDS

Nomad Mobile Research Center has discovered flaws in the NetWare Core Protocol (NCP) and IPX protocol that let hackers sniff and capture data during a typical user's login sequence. In so doing, hackers can gain a level of security access equivalent to the Admin account that has full access to the entire Novell Directory Services tree and can do virtually anything from a system and administrative standpoint. The hacks in Pandora v3 rely on "spoofing" NCP calls over the IPX protocol in order to grant Supervisor rights to a guest account or to create a denial-of-service. These hacks work only if client packet signature is set to 1 on the server and 1 on the client (1 is the default setting for both), OR, if you don't have the DS.NLM 595 patch installed on your NetWare server. Signature levels can be set in the NET.CFG on a DOS client or in the Novell NetWare Client Properties on a Windows 95 or NT client.

Pandora

Pandora is a set of tools for hacking, intruding, and testing the security and insecurity of Novell Netware versions 4 and 5. Pandora consists of two distinct sets of programs -- an "online" version and an "offline" version. Pandora is a windows 95/98/NT based freeware GUI program.

Offline features:

- Netware 4 and 5 password auditing tool, and limits extraction of password material from damaged NDS files.
- Importing and sorting of password data from BACKUP.DS, BACKUP.NDS and DSREPAIR.DIB and other files.
- Built-in NDS browser.
- Multiple simultaneous cracking of passwords of different users.

- Includes a C port of The Ruiner's Remote Console Decryption algorithm

Online features:

- Searches for target servers and grab user accounts without logging-in.
- Multiple DOS attacks and dictionary attacks against user account.
- Attach to server with password hashes extracted from Offline program.
- Improved spoofing and hijacking by using real-time sniffing.
- Silently ‘read’ files as they are downloaded from server to client.
- Improved packet drivers for Windows 95/98/NT.

Most of the functionality of the online version is taken from tools like HACK.EXE, NW-HACK.EXE, YANG.EXE, KILL.EXE, BURN.EXE, etc. DS STRIP and PANMOUNT are NMRC's utilities. In version 3.0 of Pandora, there are a number of new exploits. Most involve the NCP protocol, and some are quite sophisticated and new. Several utilities from version 2.0 have been combined, including the old CONVERT has been moved into EXTRACT, and SUPE and INTRUDE have been combined into INTRUDER

The exploit

Pandora can be used by an intruder (or an administrator), in the following fashion to break in (or to determine vulnerability):

- Use Pandora online version to determine common user accounts and use Pandora Online to determine passwords.
- Alternately Pandora Online can be used to determine the password to the special Supervisor object. If Pandora Online and your dictionary list cannot find the password for Supervisor, try using KNOCK.EXE if Intruder Detection was not triggered.
- By exploiting the information collected from Pandora Online try to access SYS:SYSTEM. If BACKUP.DS and/or DSREPAIR.DIB exist, they can be copied off of the server.
- By exploring the NCF files it should be possible to determine the remote console password, or possibly exploit the read/write access to an NCF file to gain console access.
- After gaining console access, using Novell's DSMAINT a fresh BACKUP.DS can be created and copied down. - BACKUP.DS can be converted into the original NDS files using Pandora Offline.
- The NDS files can have Pandora Offline run against them to create the PASSWORD.NDS file. - Pandora Offline can be run against PASSWORD.NDS to do either a brute force attack or a dictionary attack to obtain additional passwords.

The offline version of Pandora is similar to L0pht Crack where an attacker obtains the password hash and the application utilizes the known algorithm and procedure to generate hashes from either a dictionary or brute force attack. The NetWare passwords are entered in clear text and then passed through a one-way hash function in which there is no known algorithm to reverse the process and it is extremely unlikely that 2 passwords would generate the same hash. The result is repeated to generate a 32 bytes string which is XOR'd with the unique user ID, resulting in a unique hash even if two users have the same password. This result is then passed through a nonlinear function to create 16 bytes hash. Pandora will only attempt to crack passwords up to 16 characters.

The attacker can then use either DS Repair utility, or by NETBASIC to gain access to the server. Then the attacker copies SYS:_NETWARE*.* to SYS:\LOGIN. At this point, from any workstation, this directory can be mapped and files copied to workstation. Once DSREPAIR.DIB is copied on local hard disk, the attacker launches offline version of Pandora. Pandora extracts and displays all usernames, contexts, user ID's, length of passwords and password hashes. Users that do not have passwords assigned will display as null passwords. After selecting a user, the attacker cracks the password. This can be done either manually or by dictionary or brute-force attacks.

An administrator should review the SYS:\ETC\CONSOLE.LOG log files to look for suspicious activity recorded on the server console. The most give-away sign to this type of attack would by the existence of a DSREPAIR.DIB file or .NDS files outside of SYS:_NETWARE.

Protection

The best protection against this type of attack is establishing and enforcing a strong password policy. Physical access to all servers should be prevented. Remote management tools like RCONSOLE over SPX or RCONj or TCP/IP should not be used. In NetWare 5.x environment, screen saver also gives good protection, because the screen saver requires an NDS username and NDS password of a user with supervisor rights to the server to log in. All floppy drives and CD drives should be disabled, so that no external programs are copied. Using switches instead of hubs and placing servers and administrators on different LAN segment also increases security against sniffers. NDS version 8 in NetWare 5.x environment has added benefits of Novell Modular Authentication Service (NMAS) package. NMAS can use fingerprint readers, face scanners, magnetic cards or such other devices for authentication. Certificate Server can also be implemented for certificate-based authentication.

You should make copies of the STARTUP.NCF and AUTOEXEC.NCF files. The bindery or NDS files should be backed up and stored offsite. All System Login Scripts, Container Scripts, and any robotic or non-human personal Login Scripts should be copied offline. Use a tool like Bindview or GRPLIST.EXE from the JRB Utilities to get a list of users and groups (including group membership). Once again, keep this updated and check it frequently against the actual list.

If you only load NLMs from the SYS:SYSTEM directory, use the SECURE CONSOLE command to prevent NLMs being loaded from the floppy or other location. Compile a list of NLMs and their version numbers, and a list of files from the SYS:LOGIN, SYS:PUBLIC, and SYS:SYSTEM directories. You should periodically check these files against the originals to ensure none have been altered. Run Security (from the SYS:SYSTEM directory) or GETEQUIV.EXE from the JRB Utilities to determine who has Supervisor access (http://www.jrbsoftware.com/index.htm). Look for odd accounts with Supervisor access like GUEST or PRINTER. Turn on accounting: once Accounting is turned on, you can track every login and logout to the server, including failed attempts. Use the CONLOG.NLM to track the server console activity. This is an excellent diagnostic tool since error messages tend to roll off the screen. It will not track what was typed in at the console, but the system's responses will be put in SYS:ETC\CONSOLE.LOG.

These are some of the recommendations for NDS security:

- Use a very strong password (at least 18 characters) for Admin account and secure it in a safe. Use a NULL character somewhere in the password.
- Instead of letting people log in as Admin, grant their user object security equivalence to Admin. Strictly limit the number of such accounts.
- Keep Admin object in a container with no other users.
- Enable intrusion detection on each OU.
- Use IRF if necessary to prohibit global access to NDS objects and properties. For OUs, groups, or individual users, grant explicit rights to an NDS object by trustee assignments. This will replace any previously inherited rights.
- Remove the inheritance attribute on each OU that you want to be supported separately by other administrators (NetWare 5 only).

Novell's solution

Installing support pack 5B and setting the server signature level to 3 (the highest level) and the client packet signature to 1 (1 is the default setting for both) takes care of all the hacks in Pandora v3. You must set the server packet signature to 3 before DS.NLM loads. To do this, set the server packet signature to 3 as the first line in your AUTOEXEC.NCF and reboot, or, put the line in STARTUP.NCF. In either case, you must reboot the server.

The hacks in Pandora v3 work only if client packet signature is set to 1 on the server and 1 on the client (1 is the default setting for both), OR, if you don't have the DS.NLM 595 patch installed on your NetWare server. (Setting the signature level offers NCP packet signature, which is a message digest that prevents unauthorized access to the network via forged packets. While testing Pandora, Novell's engineers concluded that:

- Dictionary attacks (Crypto, crypto2, intruder, extract, and manipul8) can be dealt with good password policy and IDS.
- After setting the packet signature level correctly, the denial of service attack (Havoc) failed.
- NCP attack to gain admin rights (Game Over) is also taken care of with correct setting of packet signature levels.
- Level1-1, Level3-1 attacks did not work as expected. However after setting packet signatures to 3 both attacks generated messages to the console indicating

"ncp with an invalid security signature." Novell has contacted Simple Nomad for assistance in testing these further.

References

1. Novell, Inc. Security Information:
http://www.novell.com/products/nds/pandora.html

2. Nomad Mobile Research Center (NMRC) Pandora home-page:
http://www.nmrc.org/pandora/index.html

3. Infoworld article on Novell NDS hacking: *Jul 13, 1998*
http://www.infoworld.com/cgi-bin/displayStory.pl?980713.ehnetware.htm

4. LANTimes article on NDS hacking utility:
http://www.lantimes.com/97/97aug/708a014a.html

5. Pandora: Novell NetWare & Vulnerability #8: Douglas Hewes, September 16, 2000:
http://www.sans.org/infosecFAQ/audit/pandora.htm

6. Novell Technical Information Document #2941119 Pandora Hack, document rev. 6
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2941119.htm

7. Novell Security Information:
http://www.infosyssec.org/infosyssec/novsec1.htm

Download

Pandora download site:
http://www.nmrc.org/pandora/download.html

Remote Console Decryptor by The Ruiner is available at:
http://www.nmrc.org/files/netware/remote.zip