GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

Novell NetWare & Vulnerability #8

"User IDs, especially root/administrator with no passwords or weak passwords"

A SANS/GIAC Advanced Incident Handling and Hacker Exploits Certification Practical Assignment

By:

Douglas C. Hewes

© SANS Institute 2000 - 2002, Author retains full rights.

EXPLOIT DETAILS

PANDORA
…The SATAN of NetWare

Name: Pandora from Nomad Mobile Research Centre

Variants: Panmount by Jitsu-Disk, DS Strip by Simple Nomad, Remote Console Decryptor by The Ruiner, Imp by Shade

Operating System: Novell NetWare 3.1x (all versions), NetWare 4.x (up through and including at least Service Pack 5) and NetWare 5.0 (up through and including at least Service Pack 2) for Online versions. All NDS capable versions are supported in the Offline version. (NetWare 4.11 and up)

Protocols / Services: NCP (NetWare Core Protocol) over TCP/IP or IPX, NDS Authentication Services and Remote Console Services

Brief Description: As with all operating systems, Novell's NetWare and in particular the Novell Directory Services are subject to password cracking. Pandora, the self-described "SATAN of NetWare," takes advantage of this to successfully crack passwords from hashes on a server or off the wire. Pandora is actually a freeware suite of tools comprised from both original works by NMRC, as well as the incorporation of other tools listed below. This paper describes a chain of events in a typical attack on an NDS server using Pandora, a packet capturing sniffer and some general Novell knowledge.

Additional Information: Pandora (http://www.nmrc.org/pandora/index.html) is actually available in both an "on-line" and "off-line" version. Despite similar look and feel, these two applications have an entirely different set of features. Hashes derived from the off-line version can be utilized in the on-line version. The on-line version incorporates many denial-of-service attacks, session hijacking attacks, file snarfing, sniffing, on-line cracking and even a utility to authenticate with an *un-cracked password hash*! The off-line version, by comparison, focuses strictly on taking NDS files and cracking passwords. It has been the author's experience that obtaining those NDS files is often not very difficult. These files represent the "mother-load." Once the NDS files are obtained and cracking can commence, the functionality in the on-line version of Pandora is not needed, unless an attacker is focusing in on denial-of-service or needs to authenticate via a hash, in cases where the password is too long to crack. The off-line examples described in this paper were confirmed to work on several systems including NetWare 4.11 SP8a, NetWare 5, SP5 and NetWare 5.1 (No service pack). The on-line features were tested as well, but with varying degrees of success.

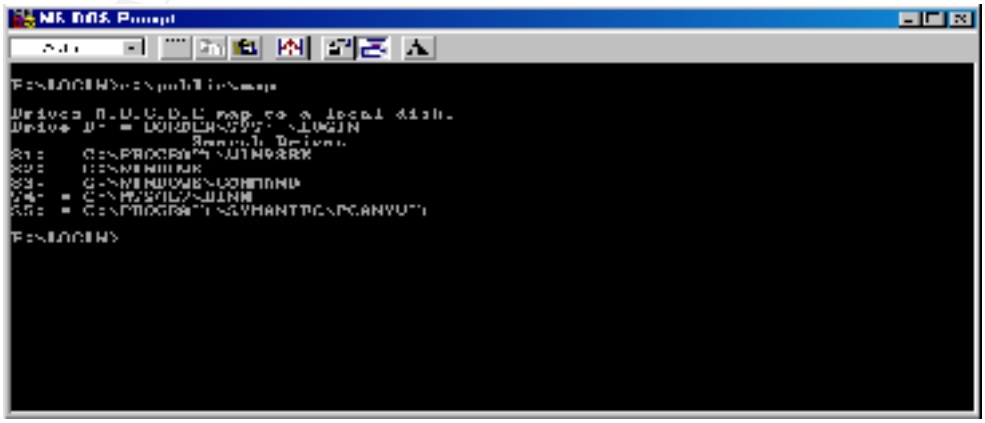
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

PROTOCOL / NDS DESCRIPTION

Novell utilizes a proprietary refined implementation of an X.500 directory scheme known as Novell Directory Services. All ACL's, user information, servers, policies, printers, groups, etc. are contained within NDS. NDS itself is a distributed, synchronized database. NDS is arranged as an inverted tree, with the [ROOT] at the top, flowing down to an Organization, Organizational Units and finally to leaf objects such as users. 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 cross WAN links. Not all servers contain replicas, but most do. Many servers in a network will contain more then just the local replica, as part of the inherent redundancy features of NDS. In NDS terms, a user's context is where that user's NDS object physically resides in the NDS tree. In an effort to maintain backward compatibility, a NetWare server can have up to 16 bindery contexts set, providing that the server holds the NDS replicas for those contexts. This is important to note since several of the Pandora on-line features rely upon a user and either the admin or the server all existing in the same context. With the advent of eDirectory (NDS version 8), the server holding the replica may not even be a NetWare server – it could in fact be NT, Linux, Solaris or others.

On a NetWare server containing a replica, the NDS files are stored in a hidden directory that is not visible from a workstation. This is the SYS:_NETWARE directory. There are several files in this directory that vary depending on the OS version and installed services. The primary files that contain the information related to what an attacker would need are ENTRY.NDS, VALUE.NDS, BLOCK.NDS and PARTITIO.NDS. (In NetWare 5 these are renamed to 0.DSD, 1.DSD, 2.DSD and 3.DSD accordingly.) Together, all user names and password hashes residing in any NDS replicas on a particular server can be obtained.

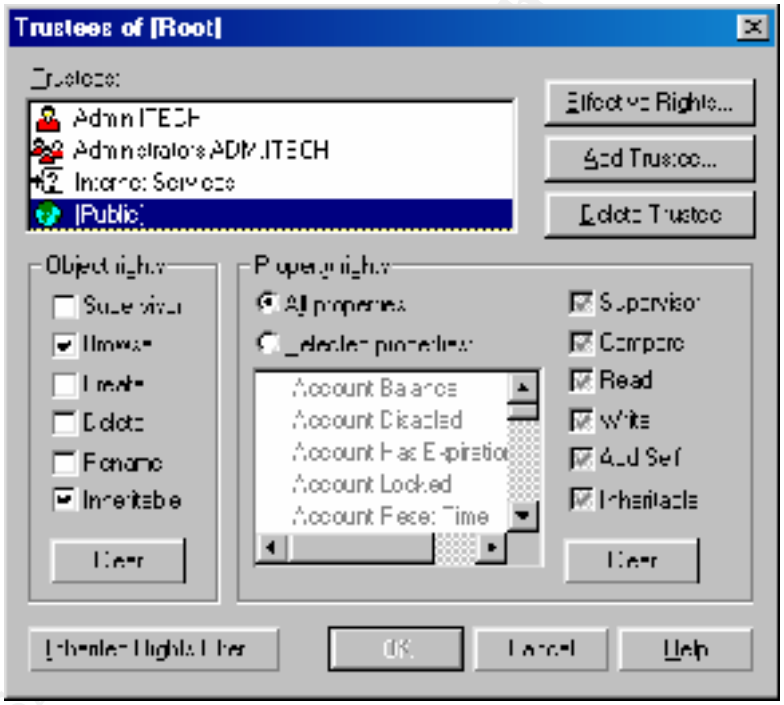
By default all users, whether authenticated or not, have read and file scan access to the SYS:\LOGIN directory. This is where the files needed to authenticate a client reside. Note that when not authenticated to the server



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the first network drive is mapped to SYS:\LOGIN, or F: in the above example. It should also be noted that a client authenticates with a hash, not a password. The workstation client handles the MD5 hashing of the password, and then transmits this password to the server. Therefore passwords cannot simply be sniffed off the wire. This does, however, open up the possibility (as exploited in the on-line version of Pandora) to simply passing the hash to the server instead of going through the process of cracking the password.

Another location open to all users, or PUBLIC, by default is the browse rights to NDS itself from the [ROOT] down. This means that with either Novell's NetWare Administrator, which is found on every server in SYS:\PUBLIC\WIN95, WINNT and WIN32 directories, or any one of numerous other tools available on the Internet, any user has the ability to see every object in the tree. A user with no rights can browse NDS and record all user names, contexts and other public information such as phone numbers, addresses, departments, etc. This information can be very valuable in determining which accounts to focus in on cracking – or even in social engineering activities.



NWAdmin "Trustees or This Object" taken at [ROOT] in a default installation.

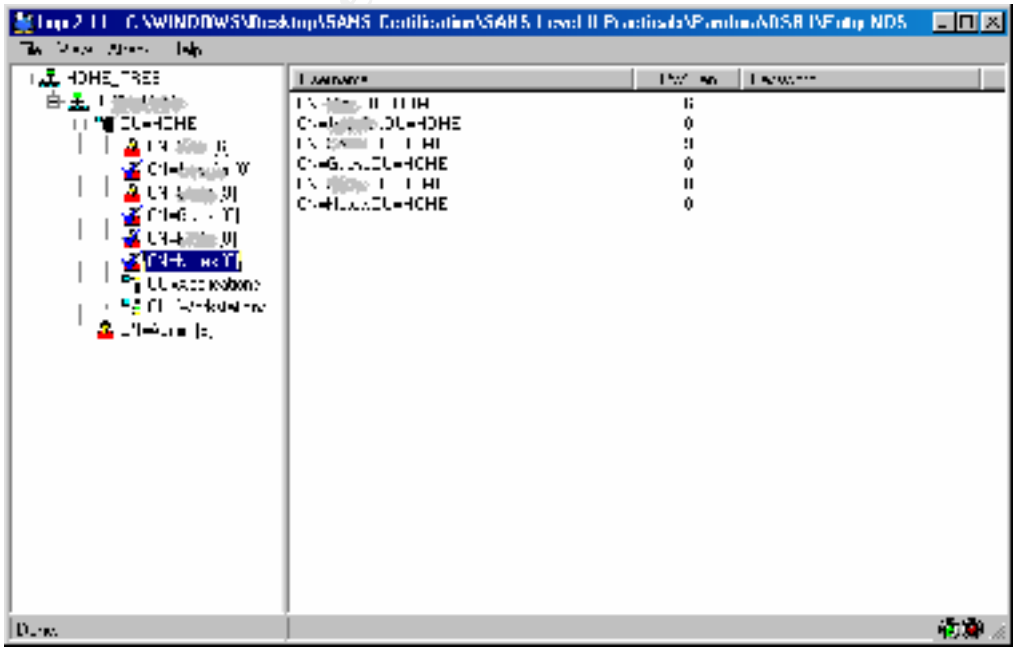
Finally, it should be pointed out that every NetWare administrator's favorite tool, Remote Console (or RCONj in NetWare 5.x) is a completely clear text utility. These utilities are the equivalent of PC Anywhere for a NetWare server, but are built in to all version of NetWare. Most administrators have a bad habit of simply managing all servers through RCONSOLE instead of walking over to the server. This is a key starting point for an attacker, since he can simply sniff an RCONSOLE session and record everything. By default the RCONSOLE password is recorded in SYS:\SYSTEM\AUTOEXEC.NCF in clear text. In the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

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. Novell does have an option to call REMOTE.NLM with an ENCRYPT option, which prompts for a password and generates a hash. From that point on the utility is invoked in AUTOEXEC.NCF (or any other batch file) as LOAD REMOTE E {hash}. This is deceptive, however, since the RCONSOLE algorithm is extremely weak and easily cracked.

DESCRIPTION OF VARIANTS

Pandora is not unique in its abilities. Most of the functionality of the on-line version is taken from utilities such as HACK.EXE, NW-HACK.EXE, YANG.EXE, BURN.EXE, KILL.EXE and other underground utilities. DS STRIP and PANMOUNT are NMRC utilities that include single functions of Pandora. All of these utilities are available at the NMRC web site at http://www.nmrc.org/files/index.html. Ironically, many of the on-line version's discovery utilities are developed from office Novell utilities, such as On-Site Admin. Jitsu-Disk and Simple Nomad, the authors of Pandora, freely give credit to these other applications and their authors. Some of the functionality of the off-line version discussed here is available in other packages as well. Remote Console Decryptor by The Ruiner available at http://www.nmrc.org/files/netware/remote.zip is the original utility used to decrypt the RCONSOLE passwords. Imp by Shade available at http://www.wastelands.gen.nz/projects/imp/index.html utilizes the Pandora functionality but repackages it in a more traditional Windows look, complete with icons from the NWAdmin utility itself.



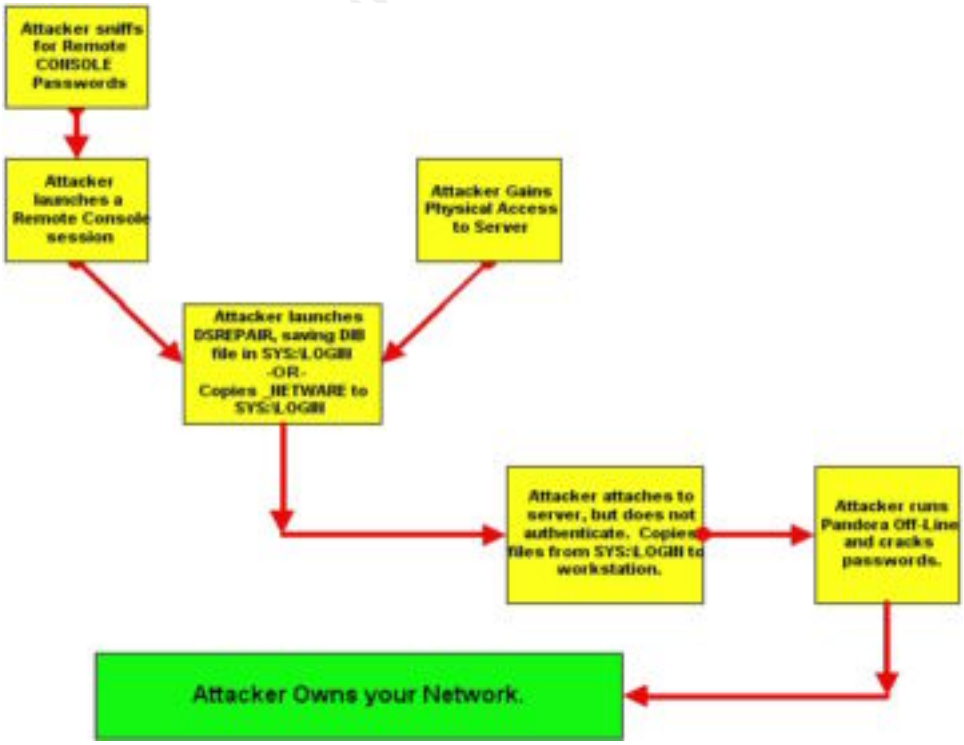
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

HOW THE EXPLOIT WORKS

The off-line version of Pandora is very similar in function to L0pht Crack on NT or Crack on UNIX. An attacker obtains the password hash. The application utilizes the known algorithm and procedure to generate hashes from either a dictionary or brute force process. These hashes are then compared to the stolen hash. If there is a match, then he has the password, otherwise the process continues.

Essentially 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 then repeated enough times to create a 32 Byte length string. This is then 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. The end result is a 16 Bytes hash. Note that a NetWare password can be up to 128 characters, but is broken down in to 32 character chunks. If the password is greater then 32 characters then these chunks are XOR'd against each other. Pandora will only attempt to crack passwords up to 16 characters in length, which in and of itself would require a tremendous amount of processing power to finish in a lifetime with today's technology. This is a great over-simplification of the process, but will suffice for the purposes of this paper. For a more in-depth discussion please refer to the paper written by Jitsu-Disk sited below. (1)

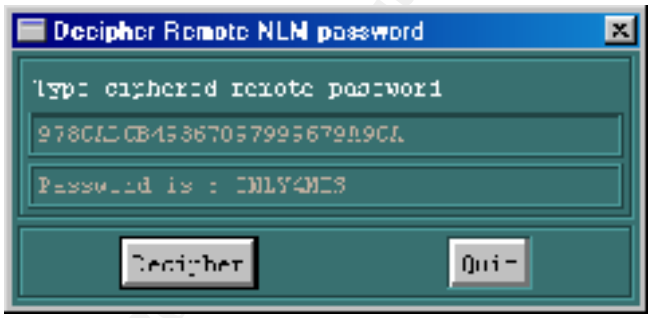
DIAGRAM



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

HOW TO USE IT?

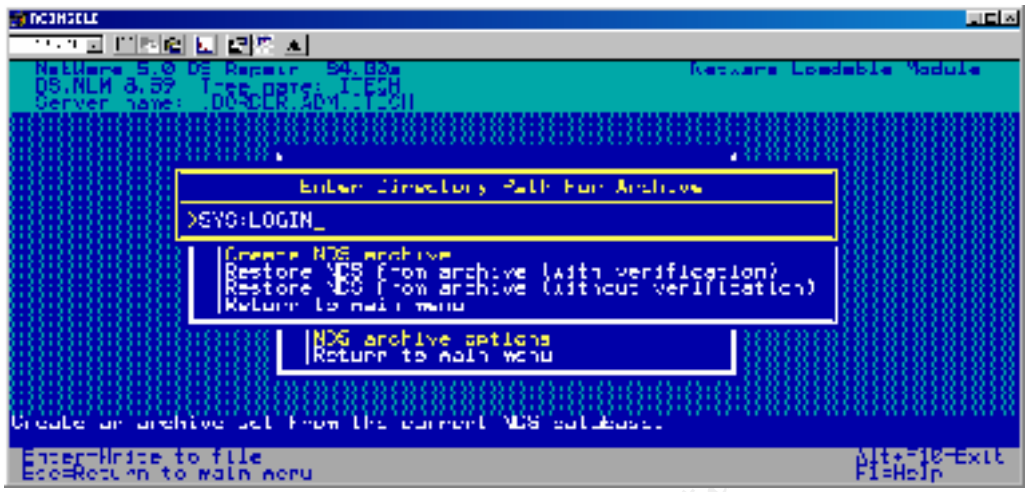
The first step in using Pandora off-line is to gain access to the server. In the simplest form this is facilitated by lax physical security of the server. Recall that a NetWare server does not have to be your most heavily guarded server in order to hold an NDS replica. A simple print server stuck out in a corner somewhere may contain a copy of an NDS partition if an administrator used this server for redundancy. Print servers that serve legacy network printing devices often must contain NDS data in order to have a bindery context set, so this is not a far fetched concept. Another alternative is a rogue sniffer waiting for an administrator or other user to open an RCONSOLE session. Since RCONSOLE has a single password and does not authenticate against NDS, any user – whether he has an NDS account or not, can log in to an RCONSOLE session. Once that session has been opened, or even if the packet capture occurs after the RCONSOLE session began, it often does not take long to watch an administrator open AUTOEXEC and grab the RCONSOLE password itself. If the RCONSOLE password in AUTOEXEC is encrypted, then Pandora comes in to play now.



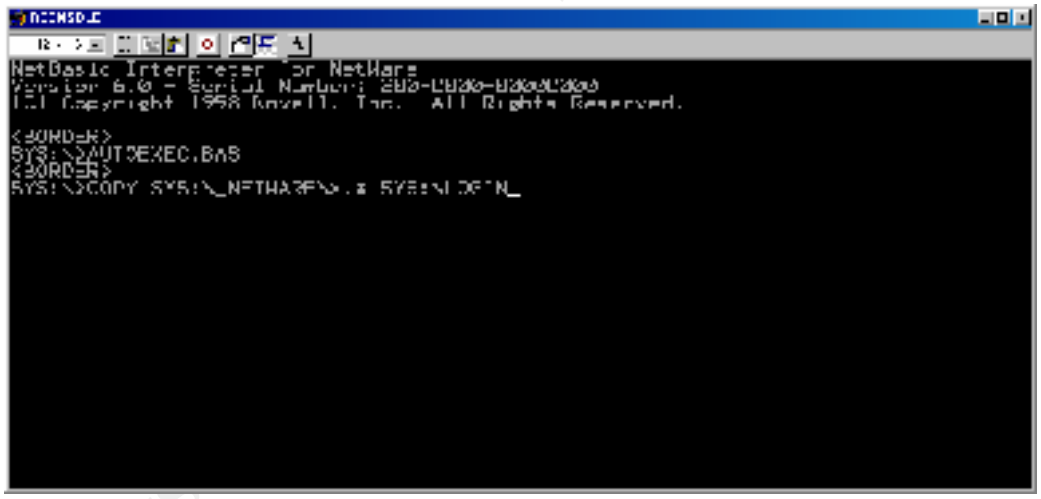
Note that all examples for this paper were run on a Pentium II 266MHz laptop running Windows 98. In the above example the encrypted RCONSOLE hash was input into Pandora and ***instantly*** the correct password was presented. This is due to a much weaker algorithm used for the RCONSOLE utility then for NDS. Also note that the password is in all caps. NetWare passwords are not case sensitive like UNIX and NT passwords. This can greatly increase the speed of password cracking; necessitating a longer password for NDS then would be required for UNIX.

Once the attacker has access to the server then one of two methods can be utilized. The first is to launch the NDS Repair Utility with, DSREPAIR.NLM with a -a option, and create an NDS Archive. To do this, go to the Advanced Options, NDS Archive Options, Create NDS Archive. When prompted, enter SYS:LOGIN as the save directory. This will create either a DSREPAIR.DIB file, or a folder named DSR_DIM with a single file in it. That file will need to be renamed to DSREPAIR.DIB in order to work in Pandora. Note that depending on the version of NetWare and the patch level, this procedure may change slightly but should still be available unless a very early patch is in place. Either way, there is still a second method…

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



A second method to get the files to SYS:LOGIN (recall that all users, whether they have an NDS account or not, have read and file scan rights to SYS:LOGIN) is to just copy them there. There are several methods to do this. The easiest is to LOAD NETBASIC, then type SHELL. This puts you in a DOS type environment. Then type COPY SYS:_NETWARE*.* SYS:\LOGIN.



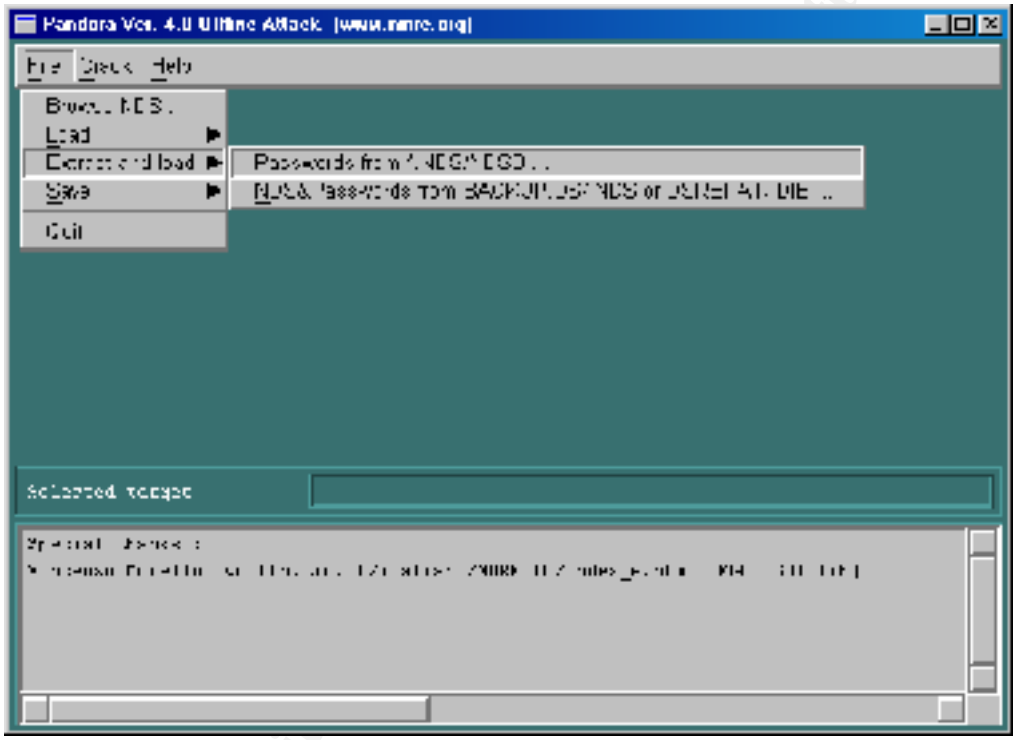
On some systems, particularly NetWare 5.1, this built in copy will fail. If that is the case then there are several other copy utilities that will work. The COPY.NLM from Novell and the Enhanced Toolkit also from Novell are both downloadable from http://support.novell.com. There are also over a dozen utilities from Compaq and others at http://www.netwarefiles.com that will also work fine. Any utility can be placed on a floppy and loaded directly from the server console, or placed in any directory on the target server, such as a user's home directory.

Once the files are in SYS:\LOGIN then the attacker can exit the RCONSOLE session or walk away from the server. This process takes less then 60 seconds and requires absolutely no username or password beyond the RCONSOLE session itself.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

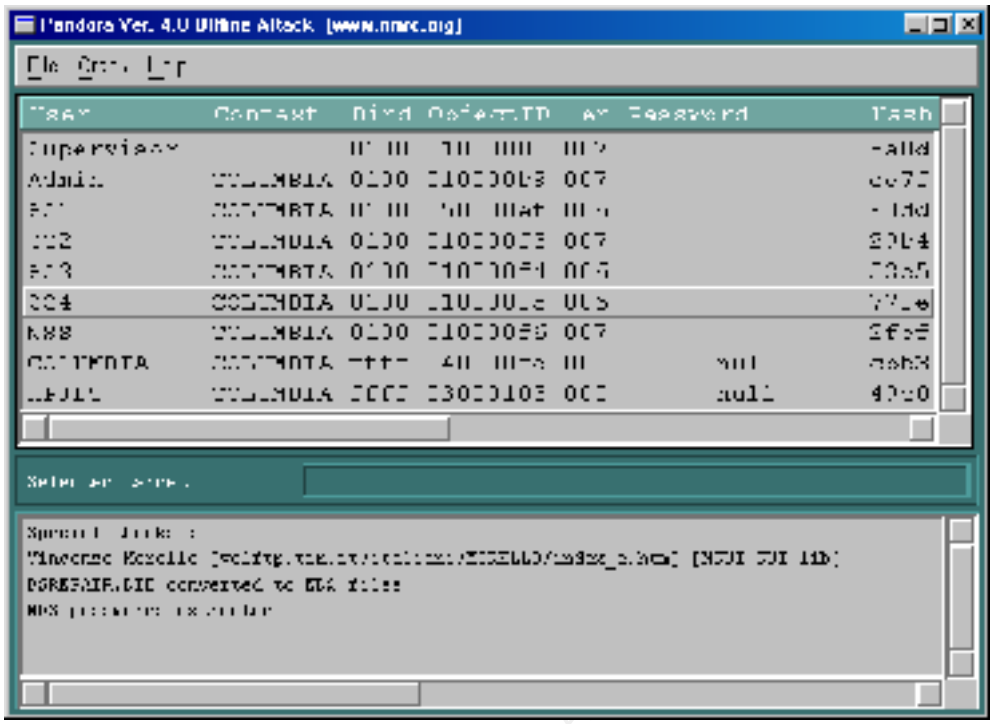
At this point the attacker simply goes to any networked workstation, opens a DOS window and goes to drive F: (or whatever the local machines first network drive is configured to be). In some cases where there are multiple servers, the NET.CFG file may need to be created or edited to list the target server as the preferred server. The attacker could also simply map a drive to \\servername\SYS\LOGIN from an explorer window. The next step is to copy the files to the local workstation.

One the DSREPAIR.DIB file or the NDS files are on the local workstation, the attacker launches Pandora off-line.

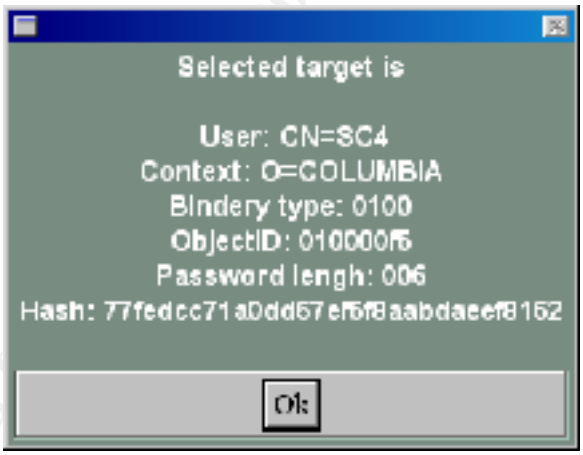


From the File menu, select Extract and load. Then select one of the two options based on which types of files were obtained. Note that if a DSREPAIR.DIB file was used (or BACKUP.DS from DSMAINT.NLM, which is another method not discussed above since it will interrupt services) then the individual NDS files will be extracted by Pandora automatically. Once loaded all usernames, contexts, user ID's, length of passwords and password hashes are displayed. Users that do not have passwords assigned will display as null passwords. This is particularly important to remember when creating new users as a network administrator. Many administrators simply create users without passwords, forcing the user to set one upon the first login. This opens a window of opportunity for the attacker. Remember that only the usernames that existed in the replicas that resided on the target server are shown.

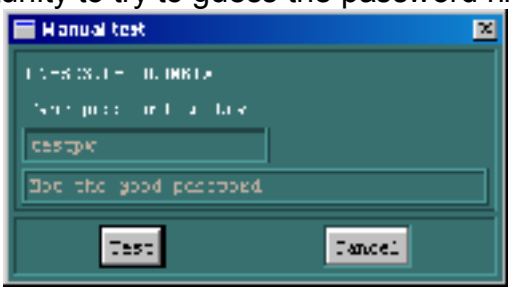
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



For more information or to select a user, simply double click the username.

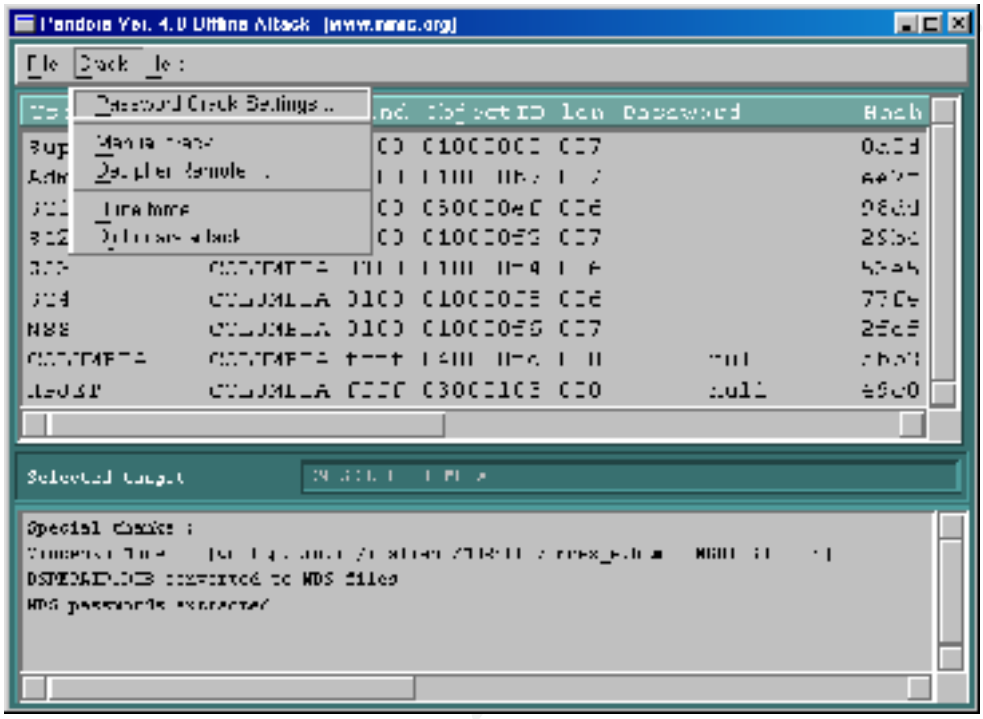


Once an attacker has selected an appropriate target, the Crack menu is selected. From here there are several options. The Manual Crack option gives the attacker the opportunity to try to guess the password himself.

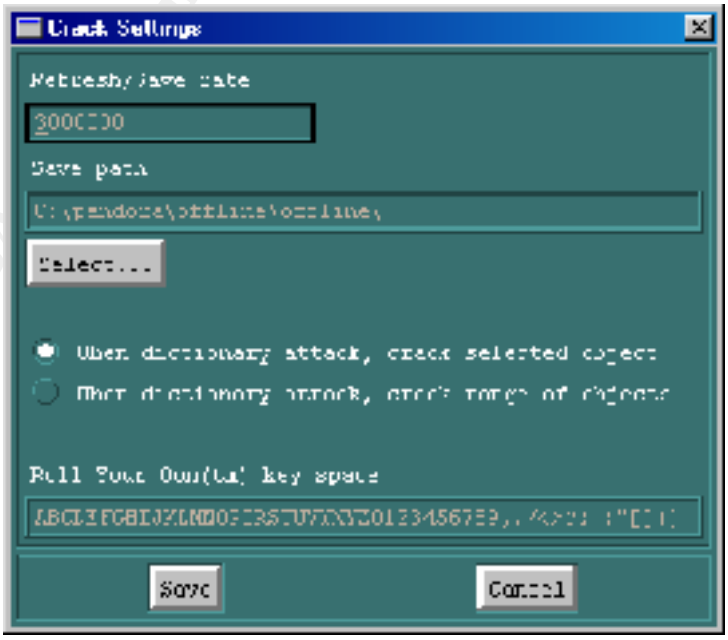


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The Decipher Remote is shown in an example above and is used to decrypt the RCONSOLE hash when used in AUTOEXEC.NCF. Again, this is an instant process due to a weak RCONSOLE algorithm.

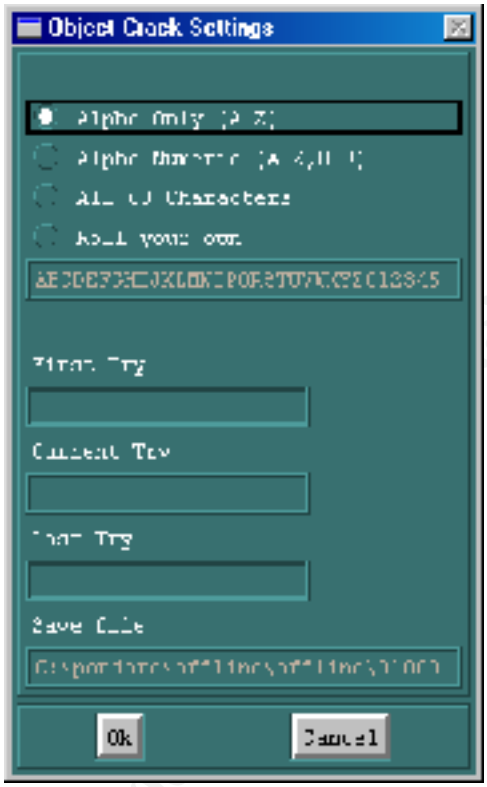


Under Password Crack Settings the attacker can select how often the crack progress is saved, to where it is saved and even create his own key space for a custom brute force attack. This is useful especially when foreign languages might come in to play.



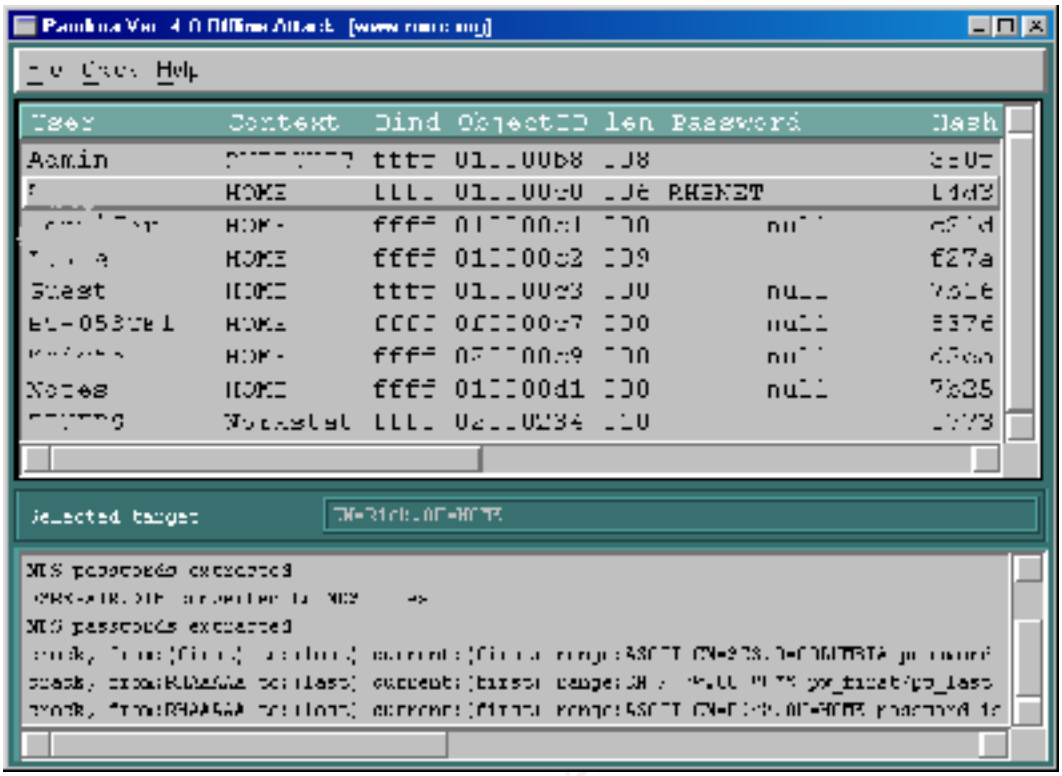
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A Dictionary attack simply asks for a dictionary file, similar to the English words list provided with L0pht Crack. When Brute Force Attack is selected the following options appear:



The attacker can try a variety of brute force attacks, as well set parameters for beginning and ending ranges. Remember that NetWare is not case sensitive, so the time required for a brute force attack is reduced over UNIX or NT for the same length password. Once the options are selected the attacker hits OK to start the attack. The current try and number of tries per second is shown at the bottom of the screen and updated every 10 seconds or so. Once the password is cracked, it appears in the list. Multiple passwords can be cracked simultaneously simply by starting one after the other.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



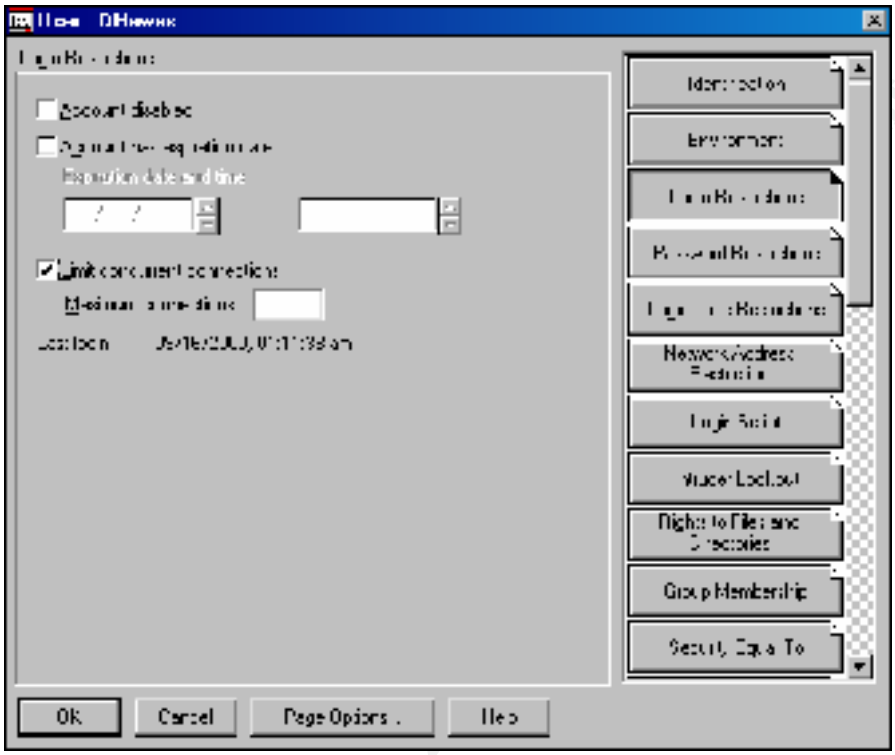
The above example shows a 6-character password, all letters. On the 266MHz test machine this took approximately 8 minutes to decrypt. A longer password or more complex password would obviously take longer. In another example a Pentium 133 was used to crack a 7-character password. The attack method was brute force with all letters and numbers. The crack took 7 hours for a password of “Pentium”. With today’s 750MHz laptops and 1GHz+ workstations, 8 character passwords are relativity easy to obtain. 9 character passwords and longer begin to become too long to wait for the average attacker. These can take weeks. If the attacker is more then just mildly curious though, he will wait it out.

SIGNATURE OF THE ATTACK

This type of attack is very difficult to spot. At minimum, an administrator should review the SYS:\ETC\CONSOLE.LOG log files to look for suspicious activity recorded on the server console. Simply unloading and reloading CONLOG easily erase this log. The erased file will still, however, reside on the volume in a ready-to-purge state and is salvageable. Again, this is not very difficult to overcome for an experiences attacker, but you may get lucky. If NETBASIC was loaded then there will usually be a console screen entitled NMX Library Manager, which generally does not shut down until a reboot. In NWAdmin on the details of users with supervisor rights can be checked to determine the last time they logged in. If an administrator notices an unusual

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

login time for another administrator or his own account, this would be a tell tale sign.



Note that backup programs are often configured to log in as a user with administrator rights, so investigate this possibility before determining that the server was compromised. There are commercial applications that establish and monitor user trends profiles, such as those from Bindview and Axent. These applications can be configured to page an administrator is for example a user who has only logged on between 9 and 5 Mon – Fri for 2 years suddenly logs in at 10PM on Saturday.

The most telling sign to this type of attack would by the existence of a DSREPAIR.DIB file or .NDS files outside of SYS:_NETWARE. Although any user can read files in SYS:\LOGIN, only supervisors can delete or rename files here. This would be a good folder to monitor for new files. If the attacker is an insider, however, with his own home directory (where he has full rights), he will be able to erase and purge the file undetected.

HOW TO PROTECT AGAINST IT

The single most important thing that can be done to foil this type of attack is to establish and enforce a strong password policy. This policy should force passwords with letters, numbers and punctuation that are at least 8 characters long – 10 or more characters for supervisor users. These passwords should also change on a regular basis and the Unique Password option should be selected to prevent users from re-using any of their last 16 passwords.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The next most important thing you can do is preventing physical access to all servers. This is followed closely by not using remote management tools like RCONSOLE over SPX or RCONj or TCP/IP. Violating either of these two recommendations is asking for trouble.

The next step, if in a NetWare 5.x environment is to enable the built in screen saver feature. Set it to activate immediately when loaded and to re-activate after 60 seconds of inactivity. By default the screen saver requires an NDS username and NDS password of a user with supervisor rights to the server to get in. This authentication is required both at the console and through RCONSOLE or RCONj.

Disable floppy drive and CD-ROMs so that someone gaining physical access to the server cannot load a third party copy utility (or other "hacking" tools for that matter). Place network administrators and servers on separate LAN segments or VLAN's then the general user population and use switched instead of hubs to reduce the chance of rogue sniffers capturing information. Set network address restrictions and login time restrictions for all users with supervisor access. This way even if the attacker gets the password, he would need to be in the right place at the right time to use it. With spoofing, this is not 100% fool proof, but it is yet another barrier that an attacker would need to cross.

In a NetWare 5.x environment running eDirectory (NDS version 8) there are some additional options. The best of which is to utilize the Novell Modular Authentication Service (NMAS) package. The basic version of this is free. NMAS allows you to do away with passwords all together and use fingerprint readers, face scanners, magnetic cards or a variety of other devices – most of which can be purchased for under $100 per machine. The NMAS Enterprise Edition offers the ability to require multiple forms of authentication, and offers graded authentication. This would allow a user with a password only to get to low-level files, but then force that user to add a fingerprint or other method to gain access to more secure files. NetWare 5.1 also ships with a PKI X.509 v3 Certificate Authority out of the box. With Certificate Server 2.0 you can implement user certificates that you can require for authentication. These can even be embedded in smartcards and used in addition to NMAS features. The bottom line is that passwords must be difficult to crack. In order to make them that difficult, most users have a hard time remembering them. This leads to users violating password policy, or worse, writing down passwords. Biometric or other token-based methods of authentication are a good replacement or addition to passwords.

SOURCE CODE / PSEUDO CODE

The entire source code for both the on-line and off-line versions of Pandora is available for free at: http://www.nmrc.org/pandora/download.html. There are also some well-written documents on the crypt.c algorithm and NDS in general in the documentation section of this site.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ADDITIONAL INFORMATION

The main source for information, documentation and the latest versions of Pandora is the Pandora Homepage at: http://www.nmrc.org/pandora/index.html

Additional NetWare "black-hat" tools can be found at: http://www.nmrc.org/files. This includes several of the above references applications as well as a good, if somewhat outdates, Novell Hacking FAQ. This FAQ, along with the Pandora documentation can be a real eye-opener for a Novell administrator and provide some excellent starting points to secure your network.

Novell's official response to the Pandora threat can be found at: http://www.novell.com/products/nds/pandora.html#2 This page refers to methods to prevent some of the Pandora on-line attacks. It does not address the off-line attacks.

Novell's official site for NMAS is http://www.novell.com/products/nmas/ with additional information regarding Novell security at http://www.novell.com/security.

Neworder also has some good information and utilities relating to Novell security. As with many underground sites, there are also many outdated utilities here. It is still amazing how many networks are not patched up and still vulnerable to many of these attacks that have been around for literally years. http://neworder.box.sk/box.php3?gfx=neworder&prj=neworder&key=hacknovl&txt=Novell%20security

An InfoWorld article from 1998 about Pandora and NMRC can be found here http://www.infoworld.com/cgi-bin/displayStory.pl?980713.ehnetware.htm

SITED SOURCES

[1] Jitsu-Disk (alias). "Hacking the Crypto.c Algorithm." NMRC Pandora Project. 1999. URL: http://www.nmrc.org/pandora/crypt.txt

© SANS Institute 2000 - 2002, Author retains full rights.