1 General FAQ Info#[1]$[2]+[3]

K[4]#[5]K[6]The following was originally compiled in June 1998. It answers some basic questions about this FAQ and hacking.

1.1 How do I add to this FAQ?#[7]K[8]Send comments about info in this FAQ to faq@nmrc.org. Simple flames about typos, the "that's not right" one liners will be ignored. If you wish to contribute corrections please include your research and source of facts. Also if you wish to add your information, I will include it if I can include your email address, unless I can verify the info independently. This way if someone has questions, they can bug you, not me.

It is prefered that you include OS flavor and versions, and other conditions used in testing. Theoretical discussion is fine, just try and back up your findings. Also note that we may often rewrite your submissions to match the "elite" nature of our FAQ ;-)

Anonymous submissions are okay. Encrypt them if you like, here's Simple Nomad's PGP key (also available from MIT's key server):

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.2

mQCNAzEQrjMAAAEEANaIf2AiInhVwmrZEFZ5V2eyZfuJfjoI9unJwRhokw
J4TtVh
ApEwjXVEbJBCPRKOHzibi5IEF2BirpzzlSy0Aj82yZk/iqYtJO60S0aycS
PNPBl5
BmoLJaUjxakmnMMXOl3qdeWWtScpP7B4QTHyfsHRvQz0HSUPxh6RUqAiTz
dxAAUR
tCRTaW1wbGUgTm9tYWQgPHRoZWdub21lQGZhc3RsYW5lLm5ldD4=
=v0Xj
-----END PGP PUBLIC KEY BLOCK-----
```

And the PGP 5 key...

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP for Personal Privacy 5.0

mQGiBDSfNs4RBADW7TK+WK6lta5deV0Pin2KInmwtG9+yB8lBr3yJHh+MP
PfG6NU
vmqoJh1STmaGG8tJ+P4p+vl7PZXflmEneuTwD7ItgtwQWTtUqYkIEKESUu
mW1Xaq
44aBAK9Fi7r3P+zT31vJFJmnRNRhE7tWgwk+YmIODpuUukd2uTWwOVXJrQ
Cg/6Z2
DncKMjg2fQf8mVpk08pe2uEEAKSmSVASHJB4LHXwO8nEGmQYd/ahIIWo2k
I288hM
NH87xkOdileWmEVHVG3+sHreX1EMKAgPWjuYpG3Jo0hUYothpN3mOrT2nf
mZp3OI
I23A4LSc8mT1dnDIKwrjJgEVK5IyEVfSMD27fXFJm4nvC3HYMuLv35JYzQ
2T2fSJ
552wA/9UhLe72U0NpOScnfHdHfMpBifL2MPM+UVGs0co99d2caBMRMtqGi
B3tR2o
041EGr80gfBG6FBohZNyCzXE4J7y2CtfxYeNZ4YwB92xKNoZvjerB1Z3WE
nIBm57
sRd4cAMyXomWdYgO1Wwb48bIJxFtGVEjXXjiIdOJKOk3gyEv37QgU2ltcG
xlIE5v
bWFkIDx0aGVnbm9tZUBubXJjLm9yZz6JAEsEEBECAAsFAjSfNs4ECwMBAg
AKCRAk
eqS9aDjxHRUoAJ4hnn4bIRbO70DfT61RPv3kSiPfbACbBC3L7R/FpiJvV7
y+4RpC
idBfHNq5BA0ENJ83ExAQAPkYoH5aBmF6Q5CV3AVsh4bsYezNRR8O2OCjec
bJ3HoL
rOQ/40aUtjBKU9d8AhZIgLUV5SmZqZ8HdNP/46HFliBOmGW42A3uEF2rth
ccUdhQ
yiJXQym+lehWKzh4XAvb+ExN1eOqRsz7zhfoKp0UYeOEqU/Rg4Soebbvj6
dDRgjG
zB13VyQ4SuLE8OiOE2eXTpITYfbb6yUOF/32mPfIfHmwch04dfv2wXPEgx
EmK0Ng
w+Po1gr9oSgmC66prrNlD6IAUwGgfNaroxIe+g8qzh90hE/K8xfzpEDp19
J3tkIt
AjbBJstoXp18mAkKjX4t7eRdefXUkk+bGI78KqdLfDL2Qle3CH8IF3Kiut
apQvMF
6PlTETlPtvFuuUs4INoBp1ajFOmPQFXz0AfGy0OplK33TGSGSfgMg71l6R
fUodNQ
+PVZX9x2Uk89PY3bzpnhV5JZzf24rnRPxfx2vIPFRzBhznzJZv8V+bv9kV
7HAarT
W56NoKVyOtQa8L9GAFgr5fSI/VhOSdvNILSd5JEHNmszbDgNRR0PfIizHH
xbLY72
88kjwEPwpVsYjY67VYy4XTjTNP18F1dDox0YbN4zISy1Kv884bEpQBgRjX
yEpwpy
1obEAxnIByl6ypUM2Zafq9AKUJsCRtMIPWakXUGfnHy9iUsiGSa6q6Jew1
```

```
XrPdYX
AAICEACOO5eqfVXbBp2hoUaikkiOHQ5BO1rWHJr8WdNgpwxghm8L8LmaM8
td6TaW
lFJtG5OlpHDOoLFHTHh1FJFzi+YpiWvmfkj18pjCiFCGZ04kHfVJ/YGngW
CzlYnu
nT1bO7E9JPb6lBDE1QWgvGBykiTXVUyij7Ih0w0XSQimBNLIG+9OWRxdTb
TL8BBH
4NrVc6pj6ofvD6fcpgQ1QYVvWC28h5MT4vIJE1EySrFs7nTdZvcAB9VOLN
VJequ4
HjU5FP9uFxWxYPdJ5GS+EqwpMOcaFzXZEmNTrSfml8RgE+lQPYKGrgvO9q
MFA/rH
+wgXbRMGLYMtmi7J6vScKhtgdH8N8WI8+M675oTPR1zCexOaWNpcvnC8wH
LKiRCJ
oRklXFaFkPzT7jDEChSibYeTOJ19js+clx4ZTlTHeuzsmzJbjCXkqSkA8v
6xnn8e
RltFPBQviG2SF19eODdJ2DEzXxqSFTJmqd/bVWRI006Vtg7KP+45bVfNOp
W654Zb
urjmJHm0SiykBINTro6mk67eSlXR/OwcowTFecqOm+IrtNLkV2zbDTRLWO
7NIvy/
yat6gn5WcSLQFifaCekngPdyPf9dD3JvXPMhfvC8eZHgHtzbHm62PsVP6p
I345Sv
2pVD/LwFNJvQejs0VzeW1vQDyTvuZsLu2CoRQlUNltvnCAS/7okAPwMFGD
SfNxMk
eqS9aDjxHRECbR0AoMCWRgpax3dcWcso23jEYb1A4N/8AKDSVipa2SJk3y
UtI7qW
pRIi/CztAg==
=c+/T
-----END PGP PUBLIC KEY BLOCK-----
```

1.2 How was this FAQ prepared?#[9]K[10]Testing for a large part of the material was completed in the NMRC lab and at various field locations. Most of the tools used during testing are available from the NMRC web site in the files section (alternate locations are listed in the resources section for these tools).

Specific testing for Netware was done in the lab and at field locations. For NT the lab was used, but due to a recent "moment of clarity" NT is no longer operational in the labs. Field locations will be used from now on. Web related hacking information has been done in the field but due to a couple of odd related projects we currently have resources for this type of testing in the lab. Unix testing is also done in the lab, but primarily limited to Linux, OpenBSD, FreeBSD, and AIX.

Technical info has been discovered (read "quoted without permission because it was out in

9TOC_2
10How was this FAQ prepared?

a public forum so I leeched it") and collected, often the technical detail is complete and self-explanatory in its original source, so I feel no reason to "test" it in a lab environment. I try and quote original material when I can, if I have left you out, let me know.

The actual FAQ was assembled from the various text files and turned into SGML source. The SGML-Tools package was used and only slightly altered to create these web pages. This gives us a single starting place during revisions and the opportunity for a multitude of output formats.

1.3 Is this FAQ available by anonymous FTP or WWW?

#[11]K[12]This FAQ is available online from the following locations:

www.nmrc.org/faqs/hackfaq/index.html.

This FAQ is available in other formats, including its raw SGML. See the www.nmrc.org/faqs/index.html page for details.

Currently due to the new processing of the information manual mirrors will not be supported. Once we've implemented the processes, we will more than likely be providing updates to this FAQ once a month.

1.4 What is the mission and goal of the FAQ?

#[13]K[14]If I said "to teach hacking" I would be lying. First off, no documentation will teach you how to hack. This FAQ answers common questions regarding some of the underlying mechanics from a hacker perspective. Second, I will not be drawn into a debate regarding usage of the term hacker, cracker, phreaker, hacking, cracking, and will certainly not be drawn into a discussion on the moral and legal issues involved. The material is what it is -- no more, no less, and I use terms the way I see fit to answer a question from the intruder perspective.

So the goal here is simply information disemination.

1.5 Where is the disclaimer?

#[15]K[16]There is no disclaimer. Disclaimers are lame and idiotic LawyerSpeak. I don't care how you use this information. If you use it to break the law, fine. If you get caught, fine. If you use it to secure a system, fine. I am responsible for myself, therefore I need no "disclaimer". Instead, here is my EXclaimer -- PISS OFF.

The only thing more lame than a disclaimer on a web page is a disclaimer in a sig file (we all know how millions of dollars in attorney's fees are saved by sig files every year).

1.6 Contributions (and thanks to...)

#[17]K[18]Here are a few of our many contributors of info:

11TOC_3
12Is this FAQ available by anonymous FTP or WWW?
13TOC_4
14What is the mission and goal of the FAQ?
15TOC_5
16Where is the disclaimer?
17TOC_6
18Contributions (and thanks to...)

- The LAN God
- Teiwaz teiwaz@wolfe.net
- Fauzan Mirza fauzan@dcs.rhbnc.ac.uk
- David A Wagner daw@lagos.CS.Berkeley.EDU
- Diceman mailto:diceman@fl.net.au
- PEME[lowbar]Inc
- Craig craigt@online1.magnus1.com
- Einar Blaberg einarb@hem.passagen.se
- SIC -- Hardware, Cyberius, and Jungman
- Michael Edwards m2mike@yahoo.com
- Jacob Ayres jayres@wcrtc.net

...and various sources who wish to remain anonymous...

1.7 Other credits...#[19]K[20]Tech Support (and special thanks to):

- itsme - infamous Netware Netherlands hack fame
- Greg Miller - Programmer/Analyst (home page in the Resources section)

Lab Support:

Ace, Mike, Knobster, Up-uat, Fourth Stooge, B.C.

Documentation and Compilation:

- imnsho@nmrc.org (Hole)

Music Heard During Revising/Editing/Testing:

- Nine Inch Nails
- Live
- "Lost Highway" Soundtrack
- "Spawn" Soundtrack
- Rammstein
- Metallica

19TOC_7
20Other credits...

- Marilyn Manson
- Filter

1.8 Changelog#[21]K[22]Here are the changes that have been made to this FAQ:

March 21, 1999

- Updated information in 11.11
- Added 13.3, 13.4

21TOC_8
22Changelog

2 Attack Basics#[23]$[24]+[25]

K[26]#[27]K[28]**2.1 What are the four steps to hacking?**#[29]K[30]While there is no hard and fast rule to hacking, most system intrusions can be divided into four steps. Depending on techniques involved, there could be less or more, but you should get the basic idea.

- Learn as much as possible about your target before the attack. The techniques involved can be passive to bordering on mini-attacks themselves. And plan out your goals. Using your knowledge gained develop a plan, no matter how small or quick the hack is.

- Initial access to the system. No doubt about it, this is the real attack part. This could be anything from ftp access to a sendmail bug to logging in as a "regular" user. It should either create an opportunity for indirect or direct access.

- Full system access. At this level most goals developed can be carried out -- password file retrieved for cracking, trojan installed, secret file copied, etc. So this stage usually involves either taking advantage of a bug that allows higher priviledges to be obtained, taking advantages of misconfigured system parameters, or a combination of both.

- Tracks are covered and backdoors installed. System logging is doctored to remove traces of the attack and what was done during the attack, and either defenses are lowered or files are tampered with to allow quicker and easier access. Some experienced hackers even patch the system to keep less experienced hackers out of the system (who might possibly tip off a Sys Admin through clumsiness). Once step four is complete, hackers will refer to this system being owned.

Of course some steps might be repeated, especially step two. Or maybe an entire series of mini "1 2 3 4" "1 2 3 4" attacks are used in concert to obtain access to a system or achieve a goal.

23TOC_9
24Attack_Basics
25browse
26Attack Basics
27attackbasics
28attackbasics
29TOC_10
30What are the four steps to hacking?

3 Account Basics#[31]$[32]+[33]

K[34]#[35]K[36]This section deals with the basics regarding computer accounts.

3.1 What are accounts?#[37]K[38]Accounts are a way of identifying users to a computer system. Other terms you may see or here are user IDs, IDs, logins, or some other variant. Most systems when initially accessed will require you to provide an account name, and will usually require you follow up with a password. Not knowing a password sucks, but not knowing a valid account name sucks more.

Account names are usually something either very common, such as a part of the user's name (like `tshimomura` or `kmitnick`), part of a user's function (like `dbadmin` or `webmaster`), or sometimes kind of goofy, like employee numbers (like `u121`), or something made up (like `up-uat` or `imnsho`). Usually if you can find out one or two regular user account names, it might be possible to guess additional names -- particularly if employee numbers or account numbers are used.

Accounts can usually be divided up into four categories -- god, special, regular, and guest. A god account can usually do anything system-wise, from adding more users to changing anybody's password to complete system reconfiguration. As a hacker, this is typically your objective. Special accounts are usually either accounts used by the system itself or accounts that fulfill some type of administrative roll without full god access. Regular accounts are simply that -- the accounts used by regular users for their normal tasks. And guest accounts are accounts designed for anyone to use -- these are usually there as a convenience for those who do not have a regular account on the system. A good example of this is anonymous ftp. Typically guest accounts have fairly restrictive access to the system, especially on publicly accessible systems.

3.2 What are groups?#[39]K[40]Groups are simply groupings of users. They are primarily used to ease system administration. For example, instead of having to assign access to a new hard drive to the forty accounting users, an admin just has to assign the accounting group the access. Even special privileges can often be assigned by group, such as the ability to manage a set of programs or system functions like printing.

Most modern systems allow accounts to belong to more than one group.

31TOC_11
32Account_Basics
33browse
34Account Basics
35accountbasics
36accountbasics
37TOC_12
38What are accounts?
39TOC_13
40What are groups?

4 Password Basics#[41]$[42]+[43]

K[44]#[45]K[46]This section deals with the basics regarding passwords.

4.1 What are some password basics?#[47]K[48]

Most accounts on a computer system usually have some method of restricting access to that account, usually in the form of a password. When accessing the system, the user has to present a valid ID to use the system, followed by a password to use the account. Most systems either do not echo the password back on the screen as it is typed, or they print an asterisk in place of the real character.

On most systems the password is typically ran through some type of algorithm to generate a hash. The hash is usually more than just a scrambled version of the original text that made up the password, it is usually a one-way hash. The one-way hash is a string of characters that cannot be reversed into its original text. You see, most systems do not "decrypt" the stored password during authentication, they store the one-way hash. During the login process, you supply an account and password. The password is ran through an algorithm that generates a one-way hash. This hash is compared to the hash stored on the system. If they are the same, it is assumed the proper password was supplied.

Cryptographically speaking, some algorithms are better than others at generating a one-way hash. The main operating systems we are covering here -- NT, Netware, and Unix -- all use an algorithm that has been made publically available and has been scrutinized to some degree.

To "crack" a password requires getting a copy of the one-way hash stored on the server, and then using the algorithm generate your own hash until you get a match. When you get a match, whatever word you used to generate your hash will allow you to log into that system. Since this can be rather time-consuming, automation is typically used. There are freeware password crackers available on the Internet for NT, Netware, and Unix.

4.2 Why protect the hashes?#[49]K[50]

If the one-way hashes are not the password itself but a mathematical derivative, why should they be protected? Well, since the algorithm is already known, a password cracker could be used to simply encrypt the possible passwords and compare the one-way hashes until you get a match. There are two types of approaches to this -- dictionary and brute force.

Usually the hashes are stored in a part of the system that has extra security to limit access

41TOC_14
42Password_Basics
43browse
44Password Basics
45passwordbasics
46passwordbasics
47TOC_15
48What are some password basics?
49TOC_16
50Why protect the hashes?

from potential crackers.

4.3 What is a "dictionary" password cracker?#[51]K[52]#[53]K[54]A dictionary password cracker simply takes a list of dictionary words, and one at a time encrypts them to see if they encrypt to the one way hash from the system. If the hashes are equal, the password is considered cracked, and the word tried from the dictionary list is the password.

Some of these dictionary crackers can "manipulate" each word in the wordlist by using filters. These rules/filters allow you to change "idiot" to "1d10t" and other advanced variations to get the most from a word list. The best known of these mutation filters are the rules that come with Crack (for Unix). These filtering rules are so popular they have been ported over to cracking software for NT.

If your dictionary cracker does not have manipulation rules, you can "pre-treat" the wordlist. Therion's Password Utility for DOS is a good example of a wordlist manipulation tool that allows all kinds of ways to filter, expand, and alter wordlists. With a little careful planning, you can turn a small collection of wordlists into a very large and thorough list for dictionary crackers without those fancy word manipulations built in.

4.4 What is a "brute force" password cracker?#[55]K[56]#[57]K[58]A brute force cracker simply tries all possible passwords until it gets the password. From a cracker perspective, this is usually very time consuming. However, given enough time and CPU power the password eventually gets cracked.

Most modern brute force crackers allow a number of options to be specified, such as maximum password length or characters to brute force with.

4.5 Which method is best for cracking?#[59]K[60]It really depends on your goal, the cracking software you have, and the operating system you are trying to crack. Let's go through several scenarios.

If you remotely retrieved the password file to a system through some system bug, your goal may be to simply get logged into that system. With the password file you now have the user accounts and the hashes. A dictionary attack seems like the quickest method, as you may simply want access to the box. This is typical if you have a method of leveraging basic access to gain god status.

If you already have basic access and used this access to get the password file, maybe you

51TOC_17
52What is a "dictionary" password cracker?
53dictionary
54dictionary
55TOC_18
56What is a "brute force" password cracker?
57brute
58brute
59TOC_19
60Which method is best for cracking?

have a particular account you wish to crack. While a couple of swipes with a dictionary cracker might help, brute force may be the way to go.

If your cracking software does both dictionary and brute force, and both are quite slow, you may just wish to kick off a brute force attack and then go about your day. By all means I recommend a dictionary attack with a pre-treated wordlist first, followed up by brute force only on the accounts you really want the password to.

You should pre-treat your wordlists if the machine you are going to be cracking from bottlenecks more at the CPU than at the disk controller. For example, some slower computers with extremely fast drives make good candidates for large pre-treated wordlists, but if you have the CPU cycles to spare you might want to let the cracking program's manipulation filters do their thing.

A lot of serious hackers have a large wordlist in both regular and pre-treated form to accommodate either need.

4.6 What is a "salt"?#[61]K[62]#[63]K[64]To increase the overhead in cracking passwords, some algorithms employ salts to add further complexity and difficulty to the cracking of passwords. These salts are typically 2 to 8 bytes in length, and algorithmically introduced to further obfuscate the one-way hash. On the major operating system covered here, only NT does not use a salt. The specifics for salts for both Unix and Netware systems are covered in their individual password sections.

Historically the way cracking has been done is to take a potential password, encrypt it and produce the hash, and then compare the result to each account in the password file. By adding a salt, you force the cracker to have to read the salt in and encrypt the potential password with each salt present in the password file. This increases the amount of time to break ALL of the passwords, although it is certainly no guarantee that the passwords can't be cracked. Because of this most modern password crackers when dealing with salts do give the option of checking a specific account.

4.7 What are the "dangers" of cracking passwords?#[65]K[66]The dangers are quite simple, and quite real. If you are caught with a password file from a system you do not have legitimate access to, you are technically in possession of stolen property in the eyes of the law. For this reason some hackers like to run cracking on someone else's systems, thereby limiting their liability. I would only recommend doing this on a system you have a legitimate or well established account on if you wish to keep a good eye on things, but perhaps have a way of running the cracking software under a different account than your own. This way, if the cracking is discovered (as it often is -- cracking is fairly CPU intensive), it looks to belong to someone else. Obviously you would want to run this under system adminstrator priviledges as you may have a bit more control, such as assigning lower priority to the cracking software, and hiding the

61TOC_20
62What is a "salt"?
63salt
64salt
65TOC_21
66What are the "dangers" of cracking passwords?

results (making it less obvious to the real administrator). Being on a system you have legit access to also allows you better access to check on the progress. Of course if it is known you are a hacker, you'll still be the first to be blamed whether the cracking software is yours or not!

> Running the cracking software in the privacy of your own home has the advantage of allowing you to throw any and all computing power you have at your disposal at a password, but if caught (say you get raided) then there is little doubt whose cracking job is running ;-) but there are a couple of things you can do to protect yourself.
>
> First, encrypt your files. Only decrypt them when you are viewing them, and wipe and/or encrypt them back after you are done viewing them. Also, have a legitimate copy of the OS whose password you are trying to correct, and import the one-way hash into your own password file. Therefore you are cracking "your own" passwords to protect your own system. Granted this isn't exactly foolproof, but it could only help.

5 Denial of Service Basics#[67]$[68]+[69]

K[70]#[71]K[72]This section covers basic info regarding "Denial of Service".

5.1 What is "Denial of Service"?#[73]K[74]

Denial of Service (DoS) is simply rendering a service offered by a workstation or server unavailable to others. This is a controversial subject, since some people think that DoS is not a hack, or rather juvenile and petty. While I can't think of very many reasons why you might want to engage in DoS, I still will continue to include this type of material in the Hack FAQ. What is more sad -- the fact that I include them, or the fact that there are so many of them?

Regardless of your feelings, DoS has been steadily gaining in popularity, be it hackers mad at other hackers, sys admins mad at spammers, or whatever -- virtually everyone I've run into that is aware of the potential of DoS at least has software to do it, admins included.

Reasons that a hacker might want to resort to DoS might include the following:

- A trojan has been installed, but a reboot is required to activate it.
- A hacker wishes to cover their tracks VERY DRAMATICALLY, or cover CPU activity with a random crash to make the site think it was "just a fluke".
- The hacker isn't a hacker at all, but a pissed off lamer who has a poor outlook and too much free time.
- The hacker is acting out of the need (or delusion) that the DoS serves a greater good, such as a DoS attack on Pro Life sites by Pro Choice believers.

Reasons that a Sys Admin might use DoS:

- A Sys Admin may want to ensure that their site is NOT vulnerable by testing out the latest patch.
- A Sys Admin has a runaway process on a server causing problems and cannot physically access the box (I have officially done this twice now).
- The Sys Admin isn't a Sys Admin at all, but a pissed off lamer who has a poor outlook and too much free time.

67TOC_22
68Denial_of_Service_Basics
69browse
70Denial of Service Basics
71denialofservicebasics
72denialofservicebasics
73TOC_23
74What is "Denial of Service"?

5.2 What is the Ping of Death?#[75]K[76]The Ping of Death is a large ICMP packet sent by a workstation to a target. The target receives the ping in fragments and starts reassembling the packet. However, due to the size of the packet once it is reassembled it is too big for the buffer and overflows it. This causes unpredictable results, such as reboots or system hangs.

Windows 95 and Windows NT are capable of sending such a packet. By simply typing in "ping -165527 -s 1 target" you can send such a ping. There are also source code examples available for Unix platforms that allow large ping packets to be constructed. These sources are freely available on the Internet.

Most systems have patches available to prevent Ping of Death from working.

5.3 What is a SYN Flood attack?#[77]K[78]In the TCP/IP protocol, a three way handshake takes place as a service is connected to. First in a SYN packet from the client, with which the service responses with a SYN-ACK. Finally the client responds to the SYN-ACK and the conversation is considered started.

A SYN Flood attack is when the client does not response to the SYN-ACK, tying up the service until the service times out, and continues to send SYN packets. The source address of the client is forged to a non-existant host, and as long as the SYN packets are sent faster than the timeout rate of the TCP stack waiting for the time out, the resources of the service will be tied up.

This is a simplified version of what exactly happens. For more elaborate details and sample Linux code for creating a flood, see Phrack 48 file 13 by daemon9.

5.4 What are other popular Denial of Service attacks?#[79]K[80]Most others involve ICMP packets (re: ping) and creating massive floods of ICMP traffic, or other packet malformations. Search the net for smurf.c or teardrop.c for more details.

75TOC_24
76What is the Ping of Death?
77TOC_25
78What is a SYN Flood attack?
79TOC_26
80What are other popular Denial of Service attacks?

6 Misc Info#[81]$[82]+[83]

K[84]#[85]K[86]This section contains miscellaneous information regarding hacking basics.

6.1 What is a "backdoor"?#[87]K[88]#[89]K[90]

A backdoor is simply a way back into a system that not only bypasses existing security to regain access, but may even defeat any additional security enhancements added onto a system.

Backdoors can range from the simple to the exotic. Simple backdoors might include creating a new user account just for your intrusion needs, or taking over a little-used account. More complex backdoors may bypass regular access completely and involve trojans, such as a login program that gives you administrative access if you type in a special password.

Backdoors can be chained together, which is the technique used by most hackers. This involves a combination of techniques. For example, one or more accounts that have basic user access may have had their passwords cracked, and one or more accounts may be created by the hacker. Once the system is accessed by the hacker, the hacker may activate some technique or exploit a system misconfiguration that allows greater access. Often a hacker will lower the defenses in certain areas by slightly altering system configuration files. Perhaps a trojan program has been installed that will open holes upon command by the hacker. Some of these techniques will be discussed in detail in the individual operating system sections of this FAQ.

6.2 Why do I care about auditing, accounting, and logging?#[91]K[92]

Auditing, accounting, logging -- call it what you will, these are things used to create permanent or semi-permanent records of events on a system. Unfortunately these can record your intrusion activities, sometimes in explicit and evidence-worthy detail. Therefore potential intruders should not only be aware of what record keeping is available (either as a regular feature of the system or as add-ons) and have possible methods for defeating such recordings.

Some types of logging include simple text files with entries showing logins and logouts, maybe failed logins. Others show what programs were accessed, which programs were attempted to be run and the request failed, or keep track of an individual's disk usage. All can reveil info that can allow an administrator to reconstruct an attack.

81TOC_27
82Misc_Info
83browse
84Misc Info
85miscinfo
86miscinfo
87TOC_28
88What is a "backdoor"?
89backdoor
90backdoor
91TOC_29
92Why do I care about auditing, accounting, and logging?

6.3 What are some different logging techniques used by Admins?#[93]K[94]Admins generally prefer to use simple logging techniques so as not to pile onto their current workload. Logs take up space. Large log files are sometimes very difficult to sift through as sys admins are looking for problems. These logs are usually stored in directories generally protected from casual viewing, or at least editing.

6.4 Why should I not just delete the log files?#[95]K[96]Typically log files do not disappear. This might lead a curious sys admin to poke around looking for problems, and the paranoid sys admin to look for intruders. The logs should be edited if possible, or the entries made into them made to look as normal as possible.

6.5 What is a buffer overflow?#[97]K[98]A buffer overflow is when a buffer was assigned by a programmer to hold variable data, and the variable data placed into that buffer is greater that the size of the initial assignment of the buffer. Depending on the operating system and exactly what the "extra" data overflowing the buffer is, this can be used by a hacker to cause portions of a system to fail, or even execute arbitrary code.

> Most buffer overflow exploits center around user-supplied data exceeding a buffer, and the extra data being executed on the stack to open up additional access. Buffer overflows exist on all major network operating systems.

93TOC_30
94What are some different logging techniques used by Admins?
95TOC_31
96Why should I not just delete the log files?
97TOC_32
98What is a buffer overflow?

7 NT Basics#[99]$[100]+[101]

K[102]#[103]K[104]This section deals with the basics and other background info to help prepare for NT hacking.

7.1 What are the components of NT security?#[105]K[106]

There are several different components. Each has a role within the overall NT security model. Because of the amount and complexity of components in the security model, not only should the individual components be explored, but how they work together should be explored.

```
Local Security Authority (LSA)
------------------------------
```

This is also known as the Security Subsystem. It is the central component of NT security. It handles local security policy and user authentication. LSA also handles generating and logging audit messages.

```
Security Account Manager (SAM)
------------------------------
```

SAM handles user and group accounts, and provides user authentication for LSA.

```
Security Reference Monitor (SRM)
--------------------------------
```

SRM enforces access validation and auditing for LSA. It checks user accounts as the user

99TOC_33
100NT_Basics
101browse
102NT Basics
103ntbasics
104ntbasics
105TOC_34
106What are the components of NT security?

tries to access various files, directories, etc, and either allows or denies access. Auditing messages are generated as a result. The SRM contains a copy of the access validation code to ensure that resources are protected uniformly throughout the system, regardless of resource type.

```
User Interface (UI)
-------------------
```

An important part of the security model, the UI is mainly all that the end user sees, and is how most of the administration can be performed.

7.2 How does the authentication of a user actually work?#[107]K[108]First, a user logs on. When this happens, NT creates a token object that represents that user. Each process the user runs is associated with this token (or a copy of it). The token-process combination is refered to as a subject. As subjects access objects such as files and directories, NT checks the subject's token with the Access Control List (ACL) of the object and determines whether to allow the access or not. This may also generate an audit message.

7.3 What is "standalone" vs. "workgroup" vs. "domain"?#[109]K[110]Each NT workstation participates in either a workgroup or a domain. Most companies will have NT workstations participate in a domain for management of the resource by the administrator.

A domain is one or more servers running NT server with all of the servers functioning as a single system. The domain not only contains servers, but NT workstations, Windows for Workgroups machines, and even LAN Manager 2.x machines. The user and group database covers ALL of the resources of a domain.

Domains can be linked together via trusted domains. The advantage of trusted domains is that a user only needs one user account and password to get to resources across multiple domains, and administrators can centrally manage the resources.

A workgroup is simply a grouping of workstations that do not belong to a domain. A standalone NT workstation is a special case workgroup.

User and group accounts are handled differently between domain and workgroup situations. User accounts can be defined on a local or domain level. A local user account can only logon to that local computer, while a domain account can logon from any workstation in the domain.

Global group accounts are defined at a domain level. A global group account is an easy

107TOC_35
108How does the authentication of a user actually work?
109TOC_36
110What is "standalone" vs. "workgroup" vs. "domain"?

way to grant access to a subset of users in a domain to, say, a single directory or file located on a particular server within the domain. Local group accounts are defined on each computer. A local group account can have global group accounts and user accounts as members.

In a domain, the user and group database is "shared" by the servers. NT workstations in the domain DO NOT have a copy of the user and group database, but can access the database. In a workgroup, each computer in the workgroup has its own database, and does not share this information.

7.4 What is a Service Pack?#[111]K[112]Microsoft maintains a large online database of fixes for operating systems and applications. These fixes are refered to as Service Packs. NT has its share, and typically the latest Service Pack has the latest fixes, including security patches.

Installing a Service Pack is NOT something to be taken lightly -- to turn on or off some features involves some Registry editing. Installation can in some circumstances disable or cause conflicts. Often after a new product has been loaded, even a Microsoft product, you must reinstall the Service Pack. For this reason, LAN administrators often neglect the timely installation of Service Packs. For the hacker, this is a decided advantage -- especially if the site has numerous NT servers and workstations in need of patching. One day maybe Microsoft will make Service Pack installation a little less painless, but until then you will find MANY locations will be either under-patched or not patched at all.

Typically Service Packs are fairly well tested, although this is no guarantee everything is "fixed". Admins should not place 100[percnt] of their faith in them, but then hackers should not underestimate their value in closing holes.

7.5 What is a Hot Fix?#[113]K[114]A Hot Fix is what is released between Service Pack releases. A Hot Fix is generally released to address a specific problem or condition. Some Hot Fixes may have a prerequisite of a certain Service Pack, and are typically included in the next Service Pack.

Once again, some of the Hot Fixes are downright dangerous to monkey around with, and many LAN folks will simply neglect installation especially at large NT shops. And once again this is good news for the hacker.

Hot Fixes are not as well tested as the Service Packs are -- often they are released after headline-grabbing security flaws are announced, so they are often rushed to press.

7.6 Where are Service Packs and Hot Fixes?#[115]K[116]The main location for Service Packs can be found at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/xxx/yyy/zzz where xxx is the country, yyy is the NT version, and zzz is the Service Pack. For example, this is the address

111TOC_37
112What is a Service Pack?
113TOC_38
114What is a Hot Fix?
115TOC_39
116Where are Service Packs and Hot Fixes?

for the USA version of Service Pack 3 for NT 4:

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/ussp3

The main location for Hot Fixes can be found at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/xxx/yyy/zzz where xxx is the country, yyy is the NT version, and zzz is the Hot Fix directory. For example, this is the address for the USA versions of Hot Fixes for NT 4 if Service Pack 3 is already installed:

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3

7.7 What's with "C2 certification"?#[117]K[118]I'm not going to get into a bunch of detail on this. There are far better places to go for the info, but I will state this -- running the c2config utility to "lock down" your system will not protect you if you want to run third party software, use the floppy drive, or connect to the network. It is simply a marketing tactic used by Microsoft. The C2 tested configuration had no network access and no floppy drive. Who wants to use that?

And keep in mind that C2 certification does not consider a number of common sense items such as a hard-to-guess password. I can see some value in running the c2config utility and "opening up" the system as needed to make it useable, but this is a lot of work and beyond the scope of what I'm discussing here.

7.8 Are there are interesting default groups to be aware of?#[119]K[120]There are a number of built-in local groups can do various functions, some which would be better off being left to the Administrator. Administrators can do everything, but the following groups' members can do a few extra items (I only verified this on 4.0):

- Server Operators: do a shutdown, even remotely; reset the system time; perform backups and restores.
- Backup Operators: do a shutdown; perform backups and restores.
- Account Operators: do a shutdown.
- Print Operators: do a shutdown.

Also members of these groups can login at the console. As you explore the NT sections of this FAQ and possibly someone else's server, remember these permissions. Gaining a Server Operator account and placing a trojan that activates after a remote shutdown could get you Administrator.

7.9 What are the default directory permissions?#[121]K[122]Like the previous question, I only verified these on 4.0. And remember, Administrators are deities. Otherwise, if it isn't here,

117TOC_40
118What's with "C2 certification"?
119TOC_41
120Are there are interesting default groups to be aware of?
121TOC_42
122What are the default directory permissions?

the group doesn't have access.

root), , APP - Server Operators and Everyone can read and execute files, display permissions on files, and do some changing on file attributes.

- Everyone can list filenames in this directory.

, - Server Operators have full access, Everyone has read access.

- Server Operators and Print Operator have full access, Everyone has read access.

- Server Operators can read and execute files, display permissions on files, and do some changing on file attributes. Replicator has read access.

- Server Operators and Replicator can read and execute files, display permissions on files, and do some changing on file attributes. Everyone has read access.

- Account Operators can read, write, delete, and execute. Everyone can list filenames in this directory.

- Everyone has read, write, and execute.

7.10 Are there any special restrictions surrounding the Administrative Tools group in Presentation Manager?

#[123]K[124]The following default group restrictions in 4.0:

Disk Administrator - Must be a member of the Administrators group.

Event Log - Anyone can run Event Viewer, but only members of the Administrators group can clear logs or view the Security Log.

Backup - Anyone can backup a file they have normal access to, but only the Administrators and Backup Operators can over override normal access.

User Manager - Users and Power Users can create and manage local groups.

User Manager for Domains - Users and Power Users can create and manage local groups if logged on at the server console, otherwise it is restricted to Administrators and Account Operators.

Server Manager - Only Administrators, Domain Admins, and Server Operators can use this on domains they have an account on. Account Operators can only add new accounts to the domain. Some features in Server Manager can only be used by the Administrators and Domain Admins.

123TOC_43
124Are there any special restrictions surrounding the Administrative Tools group in Presentation Manager?

7.11 What is the Registry?#[125]K[126]The Registry is the central core registrar for Windows NT. Each NT workstation or server has its own Registry, and each one contains info on the hardware and software of the computer it resides on. For example, comm port definitions, Ethernet card settings, desktop setting and profiles, and what a particular user can and cannot do are stored in the Registry. Remember those ugly system INI files in Windows 3.1? Well, they are all included with even more fun stuff into one big database called the Registry in NT.

Of interest to hackers is the fact that all access control and assorted parameters are located in the Registry. While I'm tempted to discuss just that portion of the Registry, I'll briefly cover everything for completeness but put the fun stuff up front.

The Registry contains thousands of individual items of data, and are grouped together into "keys" or some type of optional value. These keys are grouped together into subtrees -- placing like keys together and making copies of others into separate trees for more convenient system access.

The Registry is divided into four separate subtrees. These subtrees are called HKEY[lowbar]CLASSES[lowbar]ROOT, HKEY[lowbar]CURRENT[lowbar]USER, HKEY[lowbar]LOCAL[lowbar]MACHINE, and HKEY[lowbar]USERS. We'll go through them from most important to the hacker to least important to the hacker.

First and formost is the HKEY[lowbar]LOCAL[lowbar]MACHINE subtree. It contains five different keys. These keys are as follows:

- SAM and SECURITY - These keys contain the info such as user rights, user and group info for the domain (or workgroup if there is no domain), and passwords. In the NT hacker game of capture the flag, this is the flag. Bag this and all bets are off. The keys are binary data only (for security reasons) and are typically not accessible unless you are an Administrator or in the Administrators group. It is easier to copy the data and play with it offline than to work on directly. This is discussed in a little more detail in the NT Password section.

- HARDWARE - this is a storage database of throw-away data that describes the hardware components of the computer. Device drivers and applications build this database during boot and update it during runtime (although most of the database is updated during the boot process). When the computer is rebooted, the data is built again from scratch. It is not recommended to directly edit this particular database unless you can read hex easily. There are three subkeys under HARDWARE, these are the Description key, the DeviceMap key, and the ResourceMap key. The Description key has describes each hardware resource, the DeviceMap key has data in it specific to individual groups of drivers, and the ResourceMap key tells which driver goes with which resource.

- SYSTEM - This key contains basic operating stuff like what happens at startup, what device drivers are loaded, what services are in use, etc. These are split into ControlSets which have unique system configurations (some bootable, some not), with

125TOC_44
126What is the Registry?

each ControlSet containing service data and OS components for that ControlSet. Ever had to boot from the "Last Known Good" configuration because something got hosed? That is a ControlSet stored here.

- SOFTWARE - This key has info on software loaded locally. File associations, OLE info, and some miscellaneous configuration data is located here.

The second most important main key is HKEY[lowbar]USERS. It contains a subkey for each local user who accesses the system, either locally or remotely. If the server is a part of a domain and logs in across the network, their subkey is not stored here, but on a Domain Controller. Things such as Desktop settings and user profiles are stored here.

The third and fourth main keys, HKEY[lowbar]CURRENT[lowbar]USER and HKEY[lowbar]CLASSES[lowbar]ROOT, contain copies of portions of HKEY[lowbar]USERS and HKEY[lowbar]LOCAL[lowbar]MACHINE respectively. HKEY[lowbar]CURRENT[lowbar]USER contains exactly would you would expect, a copy of the subkey from HKEY[lowbar]USERS of the currently logged in user. HKEY[lowbar]CLASSES[lowbar]ROOT contains a part of HKEY[lowbar]LOCAL[lowbar]MACHINE, specifically from the SOFTWARE subkey. File associations, OLE configuration and dependency information.

7.12 What are hives?#[127]K[128]Hives are the major subdivisions of all of these subtrees, keys, subkeys, and values that make up the Registry. They contains "related" data. Look, I know what you might be thinking, but this is just how Microsoft divided things up -- I'm just relaying the info, even I don't know exactly what all the advantages to this setup are. ;-)

All hives are stored in [percnt]systemroot[percnt]. The major hives and their files are as follows:

Hive	File	Backup File
HKEY_LOCAL_MACHINE SOFTWARE	SOFTWARE.LOG	
HKEY_LOCAL_MACHINE SECURITY	SECURITY.LOG	
HKEY_LOCAL_MACHINE SYSTEM	SYSTEM.LOG	
HKEY_LOCAL_MACHINE SAM	SAM.LOG	
HKEY_CURRENT_USER	USERxxx	USERxxx.LOG
	ADMINxxx	ADMINxxx.LOG
HKEY_USERSDEFAULT	DEFAULT	DEFAULT.LOG

Hackers should look for the SAM file, with the SAM.LOG file as a secondary target. This contains the password info.

127TOC_45
128What are hives?

7.13 Why is the Registry like this and why do I care?#[129]K[130]Who the hell knows why it's this way? ;-)

The main reason is a step towards central administration and combining all that crap from SYSTEM.INI, WIN.INI, and other "legacy" Windows 3.x config stuff into one database. Then nice and neat individual GUI applications could be used to manipulate the data contained inside. And with the idea of a "domain" there are some "centralized" functionalities that are a little more convenient.

Is it better than Windows 3.x? This is debatable, although in my personal opinion I'd say yes. Were the design functions met? Probably not. While the Registry tries to be all things to all subcomponents of a domain, it does tend to smell like there were too many cooks in Microsoft's kitchen and simply not enough spoons. Some functions seem to be well suited for the Registry, some not. It is certainly not "portable" like Novell's NDS, that is you will probably never find the Registry running on a Unix system, whereas Novell's NDS is a much simpler design and is quite portable. Both schemes have their place -- NDS does not contain or manage OS info at the Desktop level and the Registry does.

Who wins? My guess is the people currently offering training classes in any modern OS are probably loving this because it is so complex, therefore it is guaranteed income. And hackers also win, because this is a complex environment where one wrong parameter setting or one Hot Fix not loaded could mean free and easy access.

My main advice to hackers is to play around with the Registry on home systems before the attack, because as you go further and further into an NT environment, you stand more chances of screwing things up, which is an easy way to make yourself known.

129TOC_46
130Why is the Registry like this and why do I care?

8 NT Accounts#[131]$[132]+[133]

K[134]#[135]K[136]The following section deals with Accounts on NT systems.

8.1 What are common accounts and passwords in NT?#[137]K[138]

There are two accounts that come with NT out of the box -- administrator and guest. In a network environment, I have run into local administrator access unpassworded, since the Sys Admin thought that global accounts ruled over local ones. Therefore it is possible to gain initial access to an NT box by using its local administrator account with no password.

Guest is another common unpassworded account, although recent shipments of NT disable the account by default. While it is possible that some companies will delete the guest account, some applications require it. If Microsoft Internet Studio needs to access data on another system, it will use guest for that remote access.

NetFRAME Systems Engineers use "aaa" as the default password for new installs.

8.2 What if the Sys Admin has renamed the Administrator account?#[139]K[140]

It is possible that a Sys Admin will create a new account, give that account the same access as the god account, and then remove part of the access to the former god account. The idea here is that if you don't know the real god account name, you can't get in with god priviledges.

As one might expect, this could break certain programs or functions. For example, what makes root the Unix god is the fact that the UID (User ID number) and GID (Group ID number) are both zero. Any other account set this way is god, and more than one can exist on a single system. But some programs and scripts may not look to see if the user running them is UID zero, they might possibly look to see if the user's name is root. Since often Sys Admins have a stack of stuff to do anyway, monkeying around with the root account is usually not done. If you can gain access to even a limited access account like a guest account, a simple `grep "0:0" /etc/passwd` should let you see whose god equiv or not.

With NT typing "NBTSTAT -A targetipaddress" will give you the new Administrator account, assuming the god account is logged in. A bit of social engineering could get them to log in as well. Nbtstat will also give you other useful information such as services running, the NT domain name, the nodename, and the ethernet hardware address.

Also see section From The Network which discusses a bug that allows you to get the new

131TOC_47
132NT_Accounts
133browse
134NT Accounts
135ntaccounts
136ntaccounts
137TOC_48
138What are common accounts and passwords in NT?
139TOC_49
140What if the Sys Admin has renamed the Administrator account?

Administrator account name.

Renaming or assigning the same rights to a different user name than Admin is more common with Netware than with NT, and I know of NO program that checks to see what the user name is (at least on NT). The paradigm is to check if the rights allow the action, not to see who is really running it.

8.3 How can I figure out valid account names for NT?#[141]K[142]If you are at a server and it is a domain controller (or you have simply hooked one up), try these steps to get a list of accounts on the target machine:

- From the USER MANAGER, create a trusting relationship with the target.
- Enter whatever when asked for a password. Don't fret when it doesn't work. The target is now on your trusting list.
- Launch NT Explorer and right click on any folder.
- Select SHARING.
- From the SHARED window, select ADD.
- From the ADD menu, select your target NT server.
- You will now see the entire group listing of the target.
- Select SHOW USERS and you will see the entire user listing, including full names and descriptions.

This gives you a list of user accounts to target for individual attack. By studying the group memberships, you can even make decisions about who will have more privileges than others.

8.4 What can null sessions to an NT machine tell me?#[143]K[144]By establishing a null session from your NT attacking machine to the target server, there are a few different things you can do to get account info:

net use \server[lowbar]name$""/user:""

if you see "The command completed successfully" then you are connected. Using local.exe and global.exe from the NT Resource Kit shold get you some usefull info. Here are two examples.

Get the local administrators on the target:

local anmistrators \server[lowbar]name

141TOC_50
142How can I figure out valid account names for NT?
143TOC_51
144What can null sessions to an NT machine tell me?

Get the members of the group Domain Admins:

global "domain admins" \server[lowbar]name

For even more information, rum DumpACL and go for the user and group reports. This should give you every account on the box, plus a host of other useful info, such as who logged in last, if a password is required, who is in what group, etc. From this you can target specific accounts to attempt access.

9 NT Passwords#[145]$[146]+[147]

K[148]#[149]K[150]This section deals with NT passwords.

9.1 How do I access the password file in NT?#[151]K[152]

The location of what you need is in \WINNTwhich is the location of the security database. This is usually world readable by default, but locked since it is in use by system compotents. It is possible that there are SAM.SAV files which could be readable. If so, these could be obtained for the purpose of getting password info.

During the installation of NT a copy of the password database is put in \WINNT. Since it was just installed, only the Administrator and Guest accounts will be there, but maybe Administrator is enough -- especially if the Administrator password is not changed after installation.

If the Sys Admin updates their repair disks, or you get a hold of a copy of the repair disks, you can get password database. The file is SAM.[lowbar] in the ERD directory.

If you are insane, you can go poking around in the SAM secret keys. First, schedule service to logon as LocalSystem and allow it to interact with the desktop, and then schedule an interactive regedt32 session. The regedt32 session will be running as LocalSystem and you can play around in the secret keys. However, if you change some stuff this might be very bad. You have to be Administrator to do this, though, so for the hacker you need to walk up to the machine while the Administrator is logged in and distract them by telling them they're giving away Microsoft t-shirts in the lobby (this doesn't always work ;-). Of course you can simply use a couple of different utilities for dumping the password hashes out, like PWDUMP or even running L0phtcrack (which has pwdump code built in) if you are in as Administrator.

9.2 What do I do with a copy of SAM?#[153]K[154]

You get passwords. First use a copy of SAMDUMP.EXE to extract the user info out of it. You do not need to import this data into the Registry of your home machine to play with it. You can simply load it up into one of the many applications for cracking passwords, such as L0phtCrack. See section 3 for more info on NT passwords and cracking them.

145TOC_52
146NT_Passwords
147browse
148NT Passwords
149ntpasswords
150ntpasswords
151TOC_53
152How do I access the password file in NT?
153TOC_54
154What do I do with a copy of SAM?

9.3 What's the full story with NT passwords?#[155]K[156]Two one-way hashes are stored on the server -- a Lan Manager hash, and a Windows NT hash. Lan Manager uses a 14 byte password. If the password is less than 14 bytes, it is concantenated with 0's. It is converted to upper case, and split into 7 byte halves. An 8 byte odd parity DES key is constructed from each 7 byte half. Each 8 byte DES key is encrypted with a "magic number" (0x4B47532140232425 encrypted with a key of all 1's). The results of the magic number encryption are concantenated into a 16 byte one way hash value. This value is the Lan Manager one-way hash of the password. A regular Windows NT password is derived by converting the user's password to Unicode, and using MD4 to get a 16 byte value. This value is the NT one-way hash of the password.

The reason there are two hashes is because the Lan Manager hash is for legacy support. In an all-NT environment it would be desirable to turn off Lan Man passwords. Since Lan Man uses a weakened DES key and converts all alpha characters to uppercase, it is easier to crack. The regular NT method uses a stronger algorithm and allows mixed-cased passwords.

So to crack NT passwords, the username and the corresponding one way hashes (Lan Man and NT) need to be extracted from the password database. Instead of going out and writing some code to do this, simply get a copy of Jeremy Allison's PWDUMP, which goes through SAM and gets the information for you. As previously stated, PWDUMP does require that you are an Administrator to get stuff out of the registry.

Since Microsoft does not salt during hash generation, once a potential password has generated a hash it can be checked against ALL accounts. All current NT crackers take advantage of this. Several freeware and shareware products are available on the Internet. They include:

155TOC_55
156What's the full story with NT passwords?

Cracker	Author(s)	Compiles on...	Notes
c50a-nt-0.20.tgz	Bob Tinsley	Unix	Dictionary cracker, a port of Alec Muffett's Crack 5.0 for Unix.
lc201exe.zip	Mudge and Weld Pond from the L0pht	Unix, includes GUI NT version and DOS version	Best of the bunch, can do brute force very quickly, also can use a dictionary.
NTCrack.tar.gz	Jonathan Wilkins	Unix, includes NT version	Dictionary cracker, on it's second revision.

9.4 How does brute force password cracking work with NT?#[157]K[158]As previously pointed out, the Lan Manager password concantenated to 14 bytes, and split in half. The halves can be worked on individually. If the password was originally only 7 characters or less, that second half is always 0xAAD3B435B51404EE. To further ease brute force cracking, since a substantial reduction in bits occurs during the deriving of the 8 byte DES key from the 7 byte key, less keys have to be tried. Also since the password is converted to upper case before one way encrypting it, Lan Manager password cracking does not have to take into consideration the possibility of lower case letters. L0phtcrack incorporates techniques to exploit all of these possibilities.

> By cracking the Lan Man password first, the NT password can be brute forced to determine the proper case of each alpha character. L0phtcrack 2.01, the latest version as of this writing, is lightning fast.

9.5 How does dictionary password cracking work with NT?#[159]K[160]All three of the password crackers mentioned can do dictionary attacks. Only L0phtcrack does not use rules to

157TOC_56
158How does brute force password cracking work with NT?
159TOC_57
160How does dictionary password cracking work with NT?

permutate the wordlist. It is assumed you have pre-treated the wordlist with L0phtcrack, and quite frankly L0phtcrack is blindingly fast in a dictionary crack anyway.

9.6 I lost the NT Administrator password. What do I do?#[161]K[162]#[163]K[164]Use the Offline NT Password Editor by Petter Nordahl-Hagen. You need to download Petter's code to your Linux machine (you DO have one of those, don't you?) and compile it using a libDES and MD4 library. Now mount the NT drive read/write and follow the instructions in the readme. The instructions are pretty easy to follow, especially if you know enough to get to the point to use them ;-)

> Actually, to make things easier, Petter has built a bootdisk image that steps you through the entire thing. I'll be the first to admit that Petter's code is as dangerous as hell, but it does work and I had no problems. YMMV.
>
> Consider using GetAdmin.exe (in the NT Attack Section) and go from there if you are too paranoid or fearful of booting up Linux to get to an NT machine.

9.7 How does a Sys Admin enforce better passwords?#[165]K[166]There are several freeware utilities that allow for password changing with rules enforced. These range from the simple passwd utility by Alex Frink to Microsoft's own utilities. The NT Server 4.0 Resource Kit has a utility called Passprop that enforces random passwords. Also on Service Pack 2 is a DLL called PASSFILT that will does basically the same thing.

9.8 Can an Sys Admin prevent/stop SAM extraction?#[167]K[168]As long as you can get in as Administrator, you are basically vulnerable. Microsoft has gradually increased its security for the SAM files and the hashes, but as things like L0phtCrack are quickly improved and Microsoft insists on backward compatibility with LAN Manager-style logins, things will be vulnerable. In fact, the latest L0phtCrack can actually sniff the network, store the data exchanged between client and server, and crack the hashes traced. So for you sys admins out there, keep absolutely current of Service Packs and Hot Fixes. For you hackers out there, well, it's a big bright world ;-)

9.9 How is password changing related to "last login time"?#[169]K[170]Let's say an admin is checking the last time certain users have logged in by doing a NET USER /DOMAIN. Is the info accurate? Most of the time it will NOT be.

> Most users do not login directly to the Primary Domain Controller (PDC), they login to a Backup Domain Controller (BDC). BDCs do NOT contain readonly versions of SAM, they contain read-write versions. To keep the already ungodly amount of network traffic

161TOC_58
162I lost the NT Administrator password. What do I do?
163lostntadminpassword
164lostntadminpassword
165TOC_59
166How does a Sys Admin enforce better passwords?
167TOC_60
168Can an Sys Admin prevent/stop SAM extraction?
169TOC_61
170How is password changing related to "last login time"?

down, BDCs do not tell the PDC that they have an update of the last login time until a password change has been done. And the NET USER /DOMAIN command checks the PDC, so last login time returned from this command could be wildly off (it could even show NEVER).

As a hacker, if you happen to know that password aging is not enforced, then you can bet that last login times will probably not be very accurate.

10 NT Console Attacks#[171]$[172]+[173]

K[174]#[175]K[176]This section deals with attacking at the NT Console.

10.1 What does direct console access for NT get me?#[177]K[178]

First off, a number of NT client attacks may not work if your target system does not allow logins except at the console. Any brute force attack will obviously work much quicker if you are not going across the network.

10.2 What about NT's file system?#[179]K[180]

Obviously gaining access to the file system from the console is much easier than across a network, especially if the Sys Admin is trying to keep you out.

> Try booting up the system from an MS-DOS diskette, and running NTFSDOS.EXE to access the NTFS file system. Currently this software is read only, so it is only good for getting copies of existing data. Linux is another OS that will read an NTFS file system, but "simply loading Linux" on a "spare partition" is usually impractical, and hardly simple if you are not familiar with it. See the question regarding recovering a lost NT password that uses Linux in the recovery process. I mean, if you log in as Administrator then you definitely have access to the file system ;-).

10.3 What is Netmon and why do I care?#[181]K[182]

NetMon is Microsoft's Network Monitor. It is a sniffer that runs under NT, and being a sniffer if you have to ask why you care, well, never mind ;-)

> NetMon is protected by a password scheme on version 3.51 that has nothing to do with regular NT security. In Phrack 48 file 15, AON and daemon9 have not only cracked the encryption scheme, they have written exploits for it as well. Check the resources section for the location of the exploit code (it includes full source including a Unix version in case you do not have an NT compiler).
>
> By the way, compared to other commercial sniffers, this early version of NetMon sucks. It would only look at traffic to and from the machine you are running it on. However, newer versions of NetMon supposedly do actual promiscuous sniffing and is a more useful tool. I have not seen this new NetMon but others report good things about it.

171TOC_62
172NT_Console_Attacks
173browse
174NT Console Attacks
175ntconsoleattacks
176ntconsoleattacks
177TOC_63
178What does direct console access for NT get me?
179TOC_64
180What about NT's file system?
181TOC_65
182What is Netmon and why do I care?

11 NT Client Attacks#[183]$[184]+[185]

K[186]#[187]K[188]This section deals with attacking NT remotely.

11.1 What is GetAdmin.exe and Crash4.exe?#[189]K[190]

GetAdmin.exe is a program written by Konstantin Sobolev. It exploits a subfunction in NtAddAtom that does not check the address of the output. By altering where the output can be written to, GetAdmin adds a user to the Administrators group. It works on NT 4.0.

The easiest way to use it is to simply copy it to (along with its DLL, GASYS.DLL) and run it like so: GETADMIN GUEST (or whatever account you wish to add).

This will add Guest to the Administrators group.

GetAdmin will add domain accounts on a primary domain controller and even other domain accounts. Since it is a command line tool, it will work across a telnet session if you've uploaded it to the target.

There is a post SP3 Hot Fix available from Microsoft that defeats this if loaded.

Crash4.exe will allow GetAdmin to work on SP3 patched machines. Simply run Crash4 and followed by GetAdmin as previously mentioned. Crash4 rearranges a few things on the stack to allow GetAdmin to work.

11.2 Should I even try for local administrator access?#[191]K[192]

Oh yes. A lot of NT administrators do not understand that when an NT box joins a domain, if they left that administrator password blank, it doesn't get "filled in" or "overwritten". Belonging to a domain does NOT turn off local users.

If you gain local administrator, try some of these tricks (these will work with the default settings after installation on the target):

- NBTSTAT -A x.x.x.x (plug in the IP address of the box you're after)
- Add the machine name this returns to your LMHOSTS file.
- If you are not on an NT 4.x machine, type NBTSTAT -R to refresh the NetBios names.
- Try NET VIEW \machinename to see the shares

183TOC_66
184NT_Client_Attacks
185browse
186NT Client Attacks
187ntclientattacks
188ntclientattacks
189TOC_67
190What is GetAdmin.exe and Crash4.exe?
191TOC_68
192Should I even try for local administrator access?

- Try DIR \machinenameto list shares if open
- Try NET VIEW \ipaddress or NET VIEW \fully.qualified.name.com, which should get you the user names under NT 4.0.

11.3 I have guest remote access. How can I get administrator access?#[193]K[194]The easiest way is to run GetAdmin as mentioned above, but here is an older tricks for basic NT 3.51, which as some has some stuff read/writeable by default. You could edit the association between an application and the data file extension using regedt32. First off, you should write a Win32 app that does nothing but the following -

```
net user administrator biteme /y
notepad %1 %2 %3 %4 %5
```

In a share you have read/write access to, upload it. Now change the association between .txt files and notepad to point to the location of the uploaded file, like \ThisWorkstation.exe.

Now wait for the administrator to launch a text file by double clicking on it, and the password becomes "biteme".

Of course, if the Sys Admin is smart they will have removed write permission from Everyone for HKEY[lowbar]CLASSES[lowbar]ROOT, only giving out full access to creator.

11.4 What about [percnt]systemroot[percnt]being writeable?#[195]K[196]Well, this can be exploited on NT 4.0 by placing a trojaned FPNWCLNT.DLL in that directory. This file typically exists in a mixed NT/Netware environment. First compile the exploit code written by Jeremy Allison (jra@cygnus.com) and call the resulting file FPNWCLNT.DLL. A pointer to the exploit code is in the Resources section. Now wait for the user names and passwords to get written to a file in .

If you load this on a Primary Domain Controller, you'll get EVERYBODY'S password. You have to reboot the server after placing the trojan in [percnt]systemroot[percnt].

ISS (www.iss.net) has a security scanner for NT which will detect the trojan DLL, so you may wish to consider adding in extra junk to the above code to make the size of the compiled DLL match what the original was, and using a CRC matcher program (several exist on the Internet) to make the CRC between the trojan and the real version match. This will prevent the current shipping version of ISS's NT scanner from picking up the trojan.

193TOC_69
194I have guest remote access. How can I get administrator access?
195TOC_70
196What about [percnt]systemroot[percnt]being writeable?

It should be noted that by default the group Everyone has default permissions of "Change" in [percnt]systemroot, so any DLL that is not in use by the system could be replaced with a trojan DLL that does something else.

11.5 What if the permissions are restricted on the server?

#[197]K[198]By default the NT administrator account does not have a lockout feature like normal users accounts, to prevent a denial-of-service attack on the administrator account. Since failed logins are not logged by default, you could possibly gain administrator access by sheer brute force.

If the Sys Admin runs passprop.exe they can turn on the lockout feature of Administrator.

11.6 What exactly does the NetBios Auditing Tool do?

#[199]K[200]#[201]K[202]Developed by Secure Networks Inc., it comes in pre-compiled Win32 binary form as well as the complete source code. It is the "SATAN" of NetBios based systems.

Here is a quote from Secure Networks Inc about the product -

"The NetBIOS Auditing Tool (NAT) is designed to explore the NETBIOS file-sharing services offered by the target system. It implements a stepwise approach to gather information and attempt to obtain file system-level access as though it were a legitimate local client.

"The major steps are as follows:

"A UDP status query is sent to the target, which usually elicits a reply containing the Netbios 'computer name'. This is needed to establish a session. The reply also can contain other information such as the workgroup and account names of the machine's users. This part of the program needs root privilege to listen for replies on UDP port 137, since the reply is usually sent back to UDP port 137 even if the original query came from some different port.

"TCP connections are made to the target's Netbios port [lsqb]139], and session requests using the derived computer name are sent across. Various guesses at the computer name are also used, in case the status query failed or returned incomplete information. If all such attempts to establish a session fail, the host is assumed invulnerable to NETBIOS attacks even if TCP port 139 was reachable.

"Provided a connection is established Netbios 'protocol levels' are now negotiated across the new connection. This establishes various modes and capabilities the client and server can use with each other, such as password encryption and if the server uses user-level or share-level Security. The usable protocol level is deliberately limited to LANMAN version 2 in this case, since that protocol is somewhat simpler and uses a smaller password

197TOC_71
198What if the permissions are restricted on the server?
199TOC_72
200What exactly does the NetBios Auditing Tool do?
201nbt
202nbt

keyspace than NT.

"If the server requires further session setup to establish credentials, various defaults are attempted. Completely blank usernames and passwords are often allowed to set up 'guest' connections to a server; if this fails then guesses are tried using fairly standard account names such as ADMINISTRATOR, and some of the names returned from the status query. Extensive username/password checking is NOT done at this point, since the aim is just to get the session established, but it should be noted that if this phase is reached at all MANY more guesses can be attempted and likely without the owner of the target being immediately aware of it.

"Once the session is fully set up, transactions are performed to collect more information about the server including any file system 'shares' it offers.

"Attempts are then made to connect to all listed file system shares and some potentially unlisted ones. If the server requires passwords for the shares, defaults are attempted as described above for session setup. Any successful connections are then explored for writeability and some well-known file-naming problems [lsqb]the ".." class of bugs].

"If a NETBIOS session can be established at all via TCP port 139, the target is declared 'vulnerable' with the remaining question being to what extent. Information is collected under the appropriate vulnerability at most of these steps, since any point along the way be blocked by the Security configurations of the target. Most Microsoft-OS based servers and Unix SAMBA will yield computer names and share lists, but not allow actual file-sharing connections without a valid username and/or password. A remote connection to a share is therefore a possibly serious Security problem, and a connection that allows WRITING to the share almost certainly so. Printer and other 'device' services offered by the server are currently ignored."

If you need more info on NAT, try looking at this web location:

http://www.secnet.com/ntinfo/ntaudit.html

11.7 What is the "Red Button" bug?

#[203]K[204]MWC has released an exploit that allows the following to occur -- the registry of a remote machine can be accessed, a list of users AND of shares can be obtained, even if the intruder hasn't logged in.

There is a built in user called "anonymous" that is usually used for communication between machines. This exploit takes advantage of the fact that anonymous is a member of the group Everyone. Because of this, the following can be done:

- Any share that can be accessed by Everyone is vulnerable.
- System and application logs can be read.
- Any NT machine with NetBios bound to the network can have its registry read or written to if Everyone has that access.

203TOC_73
204What is the "Red Button" bug?

- Using Lan Manager calls can give a list of all users, the Administrator (if renamed), and a list of all shares.

Using this access a trojan could be loaded, since often the group Everyone has access to application software.

It is possible that a Sys Admin could have unbound NetBios from the interface. This would disallow some access. Typically at a security aware site you would find the machines outside the firewall, like the Web server or FTP server configured this way (and all other access blocked by the firewall. However if you compromise the machine this could be a handy partial backdoor -- especially if you are using one machine as a "drop" during an attack.

The bug can manually be done -- no exploit code needed. Try this from a 4.00 workstation:

```
net use \targetserver$ "" /user:""
```

Now run User Manager, Event Viewer, Registry Editor, or simply use the net command to target the remote machine.

The administrator account's SID always ends in -500 (Guest is -501) so find that and you have the administrator account, even if renamed. The built-in local groups (documented and undocumented) always have the same SID, so check out your own machine first and compare -- especially if some of these have been renamed.

If all the users are moved from the Everyone group, you not be able to exploit this. For you admins out there, ISS has released a tool to automate this "move users out of Everyone" process. And admins you should check and see what shares that Everyone can get to.

MWC's web site is http://www.ntsecurity.com/, and the exploit code can be found there.

ISS's tool can be found at ftp://ftp.iss.net/everyone2users.exe.

11.8 What about forging DNS packets for subversive purposes?#[205]K[206]Sure. ;-)

By forging UDP packets, NT name server caches can be compromised. If recursion is allowed on the name server, you can do some nasty things. Recursion is when a server receives a name server lookup request for a zone or domain for which is does not serve. This is typical how most setups for DNS are done.

So how do we do it? We will use the following example:

205TOC_74
206What about forging DNS packets for subversive purposes?

We are root on ns.nmrc.org, IP 10.10.10.1. We have pirate.nmrc.org with an address of 10.10.10.2, and bait.nmrc.org with an address of 10.10.10.3. Our mission? Make the users at lame.com access pirate.nmrc.org when they try to access www.lamer.net.

Okay, assume automation is at work here to make the attack smoother...

- DNS query is sent to ns.lame.com asking for address of bait.nmrc.org.
- ns.lame.com asks ns.nmrc.org what the address is.
- The request is sniffed, and the query ID number is obtained from the request packet.
- DNS query is sent to ns.lame.com asking for the address of www.lamer.net.
- Since we know the previous query ID number, chances are the next query ID number will be close to that number.
- We send spoofed DNS replies with several different query ID numbers. These replies are spoofed to appear to come from ns.lamer.net, and state that its address is 10.10.10.2.
- pirate.nmrc.org is set up to look like www.lamer.net, except maybe it has a notice to "go to the new password page and set up an account and ID". Odds are this new password is used by that lame.com user somewhere else...

With a little creativity, you can also do other exciting things like reroute (and make copies of) email, denial of service (tell lame.com that www.lamer.net doesn't exist anymore), and other fun things.

Supposedly SP 3 fixes this.

11.9 What about shares?

#[207]K[208]The main thing to realize about shares is that there are a few that are invisible. Administrative shares are default accounts that cannot be removed. They have a $ at the end of their name. For example C$ is the administrative share for the C: partition, D$ is the administrative share for the D: partition. WINNT$ is the root directory of the system files.

By default since logging is not enabled on failed attempts and the administrator doesn't get locked out from false attempts, you can try and try different passwords for the administrator account. You could also try a dictionary attack. Once in, you can get at basically anything.

11.10 How do I get around a packet filter-based firewall?

#[209]K[210]If the target NT box is behind a firewall that is doing packet filtering (which is not considered firewalling by many folks) and it does not have SP3 loaded it is possible to send it packets anyway. This involves sending decoy IP packet fragments with specially crafted headers that will be "reused" by the

207TOC_75
208What about shares?
209TOC_76
210How do I get around a packet filter-based firewall?

malicious IP packet fragments. This is due to a problem with the way NT's TCP/IP stack handles reassembling fragmented packets. As odd as this sounds, example code exists to prove it works. See the web page at http://www.dataprotect.com/ntfrag for details.

How does it bypass the packet filter? Typically packet filtering only drops the fragmented packet with the offset of zero in the header. The example source forges the headers to get around this, and NT happily reassembles what does arrive.

11.11 I hack from my Linux box. How can I do all that GUI stuff on remote NT servers?

#[211]K[212]Try and get familiar with the net use and net user commands before attacking.

The main problem is adjusting NT file security attributes. Some utilities are available with NT that can be used, but I'd recommend using the NT Command Line Security Utilities. They include:

211TOC_77
212I hack from my Linux box. How can I do all that GUI stuff on remote NT servers?

```
  saveacl.exe - saves file, directory and ownership
permissions to a file
  restacl.exe - restores file permissions and ownership
from a saveacl file
  listacl.exe - lists file permissions in human readable
format
  swapacl.exe - swaps permissions from one user or group
to another
  igrant.exe - grants permisssions to users/groups on
directories
  irevoke.exe - revokes permissions to users/groups on
directories
  setowner.exe - sets the ownership of files and
directories
  audit.exe - add and remove audit triggers to files and
directories
  regilstacl.exe - print registry subkey security to the
screen
  reggrant.exe - grant access to users and groups on
registry subkeys
  regrevoke.exe - revoke access from users and groups on
subkeys
  regsetowner.exe - change registry subkey ownership
  regswapacl.exe - swaps permissions from one user group
to another
  regaudit.exe - add and delete audit triggers on keys
  sharelistacl.exe - list permissions on a local or remote
share
  sharegrant.exe - grant permissions to a local or remote
share
  sharerevoke.exe - revoke permissions from a local or
remote share
  ntuser.exe - manipulate account and group properties
  nu.exe - 'net use' replacement. shows connected drives.
```

Listacl and reglistacl also display the current auditing state of files, directories, and regisrty keys.

Each of the programs contains a built-in help screen. Just run any of the programs with a "-h" argument and the help screen will be displayed. Most utlilities support a "-r" option for recursive options throughout the program.

The collection is $45 (USD), it is shareware, but well worth the price. Even if the set only included the ntuser.exe utility, it would still be worth the money.

Check out ftp://ftp.pedestalsoftware.com/pub/pedestal to download the collection.

12 NT Denial of Service#[213]$[214]+[215]

K[216]#[217]K[218]This section deals with Denial of Service attacks that are specific to NT.

12.1 What can telnet give me in the way of denial of service?#[219]K[220]

There are several DoS attacks involving a simple telnet client that can be used against an NT server.

First, by telnetting to port 53, 135, or 1031, and then typing in about 10 or so characters and hitting enter will cause problems. If DNS (port 53) is running, DNS will stop. If 135 answers, the CPU utilization will increase to 100[percnt], slowing performance. And if port 1031 is hit, IIS will get knocked down. Typically the fix is to reboot the server, as it will be hung or so slow as to render it useless.

Telnetting to port 80 and typing "GET ../.." will also crash IIS.

If the latest service pack is loaded the attack will not work.

12.2 What can I do with Samba?#[221]K[222]

Don't get me started ;-)

As far as DoS, if you connect to a server with Samba to 3.X NT that does not have the latest service pack loaded, you can send it "DIR .. and crash it.

12.3 What's with ROLLBACK.EXE?#[223]K[224]

If the file ROLLBACK.EXE is executed, the registry can be wiped. You must re-install or do a complete restore if this happens to you. Sys Admins will probably want to remove this file. Renamed, it makes for one hell of a nasty trojan.

It is reportedly possible to lock onto a port, say like port 19, and when the server crashes and comes up ROLLBACK.EXE will start trying to unlock the port and subsequently opens up the registry for anyone to wipe it. I was unsuccessful in getting this to happen in the lab, but probably because I find DoS attacks rather lame I didn't try very hard to get it to work. But others claim it can happen, so keep it in mind.

12.4 What is an OOB attack?#[225]K[226]

This attack is fairly simple, and a fair amount of source

213TOC_78
214NT_Denial_of_Service
215browse
216NT Denial of Service
217ntdenialofservice
218ntdenialofservice
219TOC_79
220What can telnet give me in the way of denial of service?
221TOC_80
222What can I do with Samba?
223TOC_81
224What's with ROLLBACK.EXE?
225TOC_82
226What is an OOB attack?

code is available. Basically it involves sending an out-of-band message to a Windows operating system. Typically port 139 is used. This was patched with SP3 and a Hot Fix but apparently with a little monkeying around with the code you can get around this.

This DoS is very popular, mainly because of the wide variety of implementations of sockets. I've seen Unix and Windows NT versions of code, an implementation in Perl, and even an implementation using the Rexx Socket APIs on OS/2.

If you are so inclined, try a web search for "winnuke" which will get you probably a thousand locations with the code.

12.5 Are there any other Denial of Service attacks?#[227]K[228]If a domain user logs onto the console, creates a file and removes its permissions, it is possible that another user can log onto the console and delete the file. The problem affects all versions of NT. However, this isn't what I'd consider "Denial of Service" as it is more like denial of a file. Depending on the file, though, it could be used as DoS.

If you are running smbmount with version 2.0.25 of Linux, you can crash an NT server. smbmount is intended to be run on Linux 2.0.28 or higher, so it doesn't work right on 2.0.25. You also need a legit user account. Running as root, type smbmount //target/service /mnt -U client[lowbar]name, followed by ls /mnt will hang the shell on Linux (no biggie) and blue screen the target server (biggie).

The final DoS I'm aware of involves Microsoft's DNS on NT 4.0 server. If you send it a DNS response when it did not make a query, DNS will crash.

The latest service packs and post service pack patches fix all of these problems.

227TOC_83
228Are there any other Denial of Service attacks?

13 NT Logging and Backdoors#[229]$[230]+[231]

K[232]This section contains info regarding logging and backdoors for NT.

13.1 Where are the common log files in NT?#[233]K[234]

These are located in [percnt]root[percnt]. They are:

- AppEvent.Evt - Records events involving the running of certain applications.
- SecEvent.Evt - Records security events.
- SysEvent.Evt - Records basic events.

As a hacker do not worry about the AppEvent.Evt file much -- you are mainly concerned with items in the regular event log (the SysEvent.Evt file) and the security log (the SecEvent.Evt). By default regular users should be able to read the regular event log, and you may wish to look that over if you can to see if your "visit" left a trace. If it did and the entries look out of place, consider adding entries from other users that are similiar by accessing the system as these other users.

You have to have Administrative Group rights to view the security event log. And you'll certainly want to check that to see what is in it.

13.2 How do I edit/change NT log files without being detected?#[235]K[236]

Well this can be a little tricky as these files are locked in place during NT's operation. You have a couple of choices at this time -- wipe the logs or try to add stuff to them to add camoflage obfuscation. Not elegant, but better than nothing.

13.3 So how can I view/clear/edit the Security Log?#[237]K[238]

You have to be in as an Administrator or as someone in the Administrator's group.

Start the Event Viewer, and from the Log menu select Security. You view individual items by double clicking on them. To clear them (which is an all or nothing proposition) select Clear All Events from Log. If asked to save the info, answer no.

There is currently no way to edit the contents of the Security Event Log, although it is not impossible. One could conceivably boot up the system with Linx on a floppy, copy the logs off for editing in a hex editor, and copy doctored logs back up. I've considered writing the software to do this, although I probably never will.

229TOC_84
230NT_Logging_and_Backdoors
231browse
232NT Logging and Backdoors
233TOC_85
234Where are the common log files in NT?
235TOC_86
236How do I edit/change NT log files without being detected?
237TOC_87
238So how can I view/clear/edit the Security Log?

13.4 How can I turn off auditing in NT?#[239]K[240]This requires Administrator access. From the User Manager go to the Policies menu and select Audit. Turn off the things you wish to turn off.

As far as individual files and directories, you have to right-click on the file or directory from within Explorer, go to Properties and go to the security tab. Click on the auditing button for details, and turn off what you need turned off.

If you need to do this from a command line, check out the question "I hack from my Linux box. How can I do all that GUI stuff on remote NT servers?" in the NT Client Attacks section.

239TOC_88
240How can I turn off auditing in NT?

14 NT Misc. Attack Info#[241]$[242]+[243]

K[244]#[245]K[246]This section has miscellaneous information regarding hacking and NT.

14.1 How is file and directory security enforced?#[247]K[248]

Since files and directories are considered objects (same as services), the security is managed at an "object" level.

An access-control list (ACL) contains information that controls access to an object or controls auditing of attempts to access an object. It begins with a header contains information pertaining to the entire ACL, including the revision level, the size of the ACL, and the number of access-control entries (ACEs) in the list.

After the header is a list of ACEs. Each ACE specifies a trustee, a set of access rights, and flags that dictate whether the access rights are allowed, denied, or audited for the trustee. A trustee can be a user account, group account, or a logon account for a service program.

A security descriptor can contain two types of ACLs: a discretionary ACL (DACL) and a system ACL (SACL).

In a DACL, each ACE specifies the types of access that are allowed or denied for a specified trustee. An object's owner controls the information in the object's DACL. For example, the owner of a file can use a DACL to control which users can have access to the file, and which users are denied access.

If the security descriptor for an object does not have a DACL, the object is not protected and the system allows all attempts to access the object. However, if an object has a DACL that contains no ACEs, the DACL does not grant any access rights. In this case, the system denies all attempts to access the object.

In a SACL, each ACE specifies the types of access attempts by a specified trustee that cause the system to generate audit records in the system event log. A system administrator controls the information in the object's SACL. An ACE in a SACL can generate audit records when an access attempt fails, when it succeeds, or both.

To keep track of the individual object, a Security Identifier (SID) uniquely identify a user or a group.

A SID contains:

- User and group security descriptors

241TOC_89
242NT_Misc__Attack_Info
243browse
244NT Misc. Attack Info
245ntmiscattackinfo
246ntmiscattackinfo
247TOC_90
248How is file and directory security enforced?

- 48-bit ID authority
- Revision level
- Variable subauthority values

A privilege is used to control access to a service or object more strictly than is normal with discretionary access control. Privileges provide access to services rarely needed by most users. For example, one type of privilege might give access for backups and restorals, another might allow the system time to be changed.

14.2 What is NTFS?#[249]K[250]NTFS is the Windows NT special file system. This file system is tightly integrated into Windows security -- it is what allows access levels to be set from the directory down to individual files within a directory.

14.3 Are there are vulnerabilities to NTFS and access controls?#[251]K[252]Not so much vulnerabilities as there are quirks -- quirks that can be exploited to a certain degree.

For example, let's say the system admin has built a home directory for you on the server, but has disallowed the construction of directories or files that you wish to make available to the group Everyone. You are wanting to make this special directory so that you can easily retrieve some hack tools but you are cut off. However, if the sys admin left you as the owner of the home directory, you can go in and alter its permissions. This is because as long as you are the owner or Administrator you still control the file. Oh sure, you may get a few complaints from the system when you are doing it, but it can be done.

Since NTFS has security integrated into it, there are not too many ways around it. The main one requires access to the physical system. Boot up the system on a DOS diskette, and use NTFSDOS.EXE. It will allow you to access an NTFS volume bypassing security.

The last quirk is that if you have a directory with Full Control instead of RWXDPO permissions, then you get a hidden permission called File Delete Child. FDC cannot be removed. This means that all members of the group Everyone can delete any read-only file in the directory. Depending on what the directory contains, a hacker can replace a file with a trojan.

14.4 What is Samba and why is it important?#[253]K[254]Samba is a freeware app developed by Andy Tridgell. It is a great tool for helping integrate Unix into Microsoft Windows and Lan Manager environments. The main idea is that you can, with Samba, allow a Unix machine to access file and directories. The other handy thing about Samba is that like most Unix freeware you get the source code.

Most hackers seem to have Linux up and running, so loading up Samba allows you several

249TOC_91
250What is NTFS?
251TOC_92
252Are there are vulnerabilities to NTFS and access controls?
253TOC_93
254What is Samba and why is it important?

tactical advantages. A number of the exploits described here require access to a privileged port (< 1024). If you are root on your own Linux box, you can start exploits from those needed ports. A lot of the tests in the NMRC lab were conducted using Samba. In fact when World Star Holdings Ltd in Canada had their lame Cybertest '96 contest on June 12th, yours truly used Samba to break in (but I wasn't first).

Samba talks SMB and can directly access Windows NT hardware, and Hobbit (hobbit@avian.org) has put together a very interesting paper entitled "CIFS: Common Insecurities Fail Scrutiny". It is highly recommended reading for admins and hackers alike. Included in the paper are details and source patches to allow easier attacking on NT.

Studying the source code of Samba taught me a lot, but Hobbit's paper puts everything in a whole new light. It provides some well documented basics on how a lot of the communications work, detailing exactly WHY certain protocols and behaviours are vulnerable to abuse.

Get Samba and read its documentation. Read Hobbit's paper and apply the patches. Period.

14.5 How do I bypass the screen saver?#[255]K[256]If a user has locked their local workstation using CTRL+ALT+DEL, and you can log in as an administrator, you will have a window of a few seconds where you will see the user's desktop, and even manipulate things. This trick works on NT 3.5 and 3.51, unless the latest service pack has been loaded.

If the service pack has been loaded, but it's still 3.X, try the following.

- From another NT workstation, type shutdown \ /t:30
- This will start a 30 second shutdown on the target and a Security window will pop up.
- Cancel the shutdown with shutdown \ /a
- The screen saver will kick back in.
- Wiggle the mouse on the target. The screen will go blank.
- Now do a ctrl-alt-del on the target.
- An NT Security window will appear. Select cancel.
- You are now at the Program Manager.

14.6 How can I detect that a machine is in fact NT on the network?#[257]K[258]Hopefully it is a web server, and they've simply stated proudly "we're running NT", but don't expect that...

Port scanning will find some. Typically you'll see port 135 open. This is no guarantee it's not Windows 95, however. Using Samba you should be able to connect and query for the

255TOC_94
256How do I bypass the screen saver?
257TOC_95
258How can I detect that a machine is in fact NT on the network?

existence of HKEY[lowbar]LOCAL[lowbar]MACHINEand then check to determine the version running. If guest is enabled, try this first as Everyone has read permissions here by default.

Port 137 is used for running NetBios over IP, and since in the Windows world NetBios is used, certainly you can expect port 137 to be open if IP is anywhere in use around NT.

Another possible indication is checking for port 139. This tells you your target is advertising an SMB resource to share info, but it could be any number of things, such as a Windows 95 machine or even Windows for Workgroups. These may not be entirely out of the question as potential targets, but if you are after NT you will have to use a combination of the aforementioned techniques coupled with some common sense.

To simplify this entire process, Secure Networks Inc. has a freeware utility called NetBios Auditing Tool. This tool's intent is to test NetBios file sharing configurations and passwords on remote systems. It is discussed more in detail in the NT Client Attack section.

14.7 Can I do on-the-fly disk encryption on NT?#[259]K[260]Try Shade. It allows you to create an encrypted disk device inside a file. This "device" can then be formatted using either NTFS or FAT and used as a regular disk. Shade encrypts on every write operation and decrypts on every read operation to this new device.

Look for Shade at: http://softwinter.bitbucket.co.il/shade.html

14.8 Does the FTP service allow passive connections?#[261]K[262]I was playing around in the registry, looking for odd things, and found this strange entry under System:

```
EnablePortAttack: REG_DWORD:
```

If set to 1, you can do passive connections depending on the TCP port you use. A passive connection is where you can connect to FTP site alice.com, and from there connect to site bob.com. It is used by hackers because any odd connections at bob.com will appear in logs as coming from alice.com. Most typical is a port scan.

A port scanner for doing this from a Unix box can be found at http://www.nmrc.org/files/unix/ftp-scan.c

14.9 What is this "port scanning" you are talking about?#[263]K[264]Port scanning is a

259TOC_96
260Can I do on-the-fly disk encryption on NT?
261TOC_97
262Does the FTP service allow passive connections?
263TOC_98
264What is this "port scanning" you are talking about?

technique to check TCP/IP ports to see what services are available. For example port 80 is typically a web server, port 25 is SMTP used by Internet mail and so on. By scanning and seeing what TCP/IP ports are listening at the end of a TCP/IP address, you can get an idea as to what type of box the target might be, what services are available, and possibly plan an attack if you are aware of an exploit involving a particular service.

> If port 135, 137, 138, and 139 are open on the target of a scan, it is quite possible that the target is NT (although it could be Win95 or even WFW 3.11, see the questions and answers above).

14.10 Does NT have bugs like Unix' sendmail?#[265]K[266]If the server is running a POP3 server like Exchange, you can use a brute force technique to guess passwords. Odds are that the sys admin is not logging or looking at logs for this stuff. In particular, if you are dealing with a sys admin that isn't used to the wild and wooly Unix world, it may not even occur to the admin to look. This is something that NT folks are just now having to face, whereas their Unix admin counterparts have had to maintain this level of scrutiny for a while.

14.11 How is password changing related to "last login time"?#[267]K[268]Let's say an admin is checking the last time certain users have logged in by doing a NET USER /DOMAIN. Is the info accurate? Most of the time it will NOT be.

> Most users do not login directly to the Primary Domain Controller (PDC), they login to a Backup Domain Controller (BDC). BDCs do NOT contain readonly versions of SAM, they contain read-write versions. To keep the already ungodly amount of network traffic down, BDCs do not tell the PDC that they have an update of the last login time until a password change has been done. And the NET USER /DOMAIN command checks the PDC, so last login time returned from this command could be wildly off (it could even show NEVER).
>
> As a hacker, if you happen to know that password aging is not enforced, then you can bet that last login times will probably not be very accurate

14.12 Can sessions be hijacked?#[269]K[270]In theory, however no one has yet coded the exploit. It would involve a complex spoofing job where not only would the session have to be hijacked at the transport level (getting all of the ACK/NACK numbering correct), but the tree ID (TID) and user ID (UID) would have to be spoofed at the redirector and server level respectively. We are talking SMB at this point.

> A more likely session to be hijacked would be a telnet session to an NT server, but this applies to any straight telnet session, NT or not, and is beyond the scope of this question. For more information refer to http://www.nmrc.org/files/unix/ip-exploit.txt..

265TOC_99
266Does NT have bugs like Unix' sendmail?
267TOC_100
268How is password changing related to "last login time"?
269TOC_101
270Can sessions be hijacked?

14.13 Are "man in the middle" attacks possible?#[271]K[272]Ealry versions of LANMAN send the password in the clear -- which is definately sniffer-bait. But the challenge/response authentication used by LANMAN 2.1 and earlier is subject to possible attack -- namely a plaintext attack. Since the challenge is plaintext, an attacker can acquire known plaintext/ciphertext pairs. Offline, the attacker can then test a guess at a password by using it to generate a key, encrypting the plaintext, and comparing it to the corresponding ciphertext. If it matches, the password is compromised.

Since case doesn't matter, a brute force attack is theoretically possible against plaintext/ciphertext pair obtained via a known plaintext attack.

However, this is simply offline attacking. A true man-in-the-middle attack allows a third party to intercept and replace components of the challenge/response conversation with their own, acquiring the password or even taking over the session itself. However, the easier of the two is getting the password.

By catching the start of a conversation and forging the challenge, the client would response with the response to the server, and the attacker would know a part of the equation, shortening the time and effort needed to break the plaintext/ciphertext pair.

By "precompiling" a list of response/password pairs, the password could be determined even quicker.

NT LM 0.12 uses MD4 to generate keying material, and since upper and lower case are allowed, the full 56 bits allowed by DES can be used. This does not eliminate the problem -- it simply increases the difficulty of brute force against a plaintext/ciphertext pair.

However this does nothing towards a realtime attack. The best method would be as follows:

- Client starts a session.
- Attacker sees this session, and waits for the response from the server.
- Server sends the response and the Attacker grabs it.
- Attacker removes the SMB[lowbar]COM[lowbar]NEGPROT bit and sends it to the Client.
- Client receives the Attacker's packet, and now assumes a plaintext password should be used.
- Client receives the real packet from the server, but ignores it thinking it is a dupe.
- Client sends the password in plaintext.
- Attacker grabs the password and now logs into the Server directly.
- Client times out or gets an error, and figures a network error has occurred. Client tries

271TOC_102
272Are "man in the middle" attacks possible?

to log in again.

It is also possible in theory to catch the session before the authentication process even starts. For example:

- Client starts a session, and sends a request to the DNS server to resolve a host name.
- Attacker sees this request, and forges a reply that the Attacker's IP address is the address for the host the Client is requesting.
- Attacker sends request to DNS server cancelling Client's request.
- Client starts to log into Attacker.
- Attacker tells Client to send the password as plaintext.
- Client complies, and Attacker proceeds to login to original host that the Client was asking the DNS server about.
- Attacker kills the session with the Client, and the Client thinks an error has occurred, and tries again.

This attack has been partially implemented with the c2myazz file, which forces a plaintext login.

14.14 What about TCP Sequence Number Prediction?#[273]K[274]This is possible, but unlikely, on anything requiring the TID and UID as a part of the spoof. TCP Sequence Number Prediction involves guessing what the TCP numbering sequence is, and inserting packets to (typically) execute commands on the target host with the proper sequence number.

14.15 What's the story with buffer overflows on NT?#[275]K[276]Dildog has written the definative paper on the subject. Check out "The Tao of Windows Buffer Overflow" at http://www.cultdeadcow.com/cDc-351/ for a complete picture of buffer overflows, how they work, and how to code your own exploits for Microsoft operating systems.

273TOC_103
274What about TCP Sequence Number Prediction?
275TOC_104
276What's the story with buffer overflows on NT?

15 Netware Basics#[277]$[278]+[279]

K[280]#[281]K[282]The following section covers the basics regarding Netware security.

15.1 What's the story with buffer overflows on NT?#[283]K[284]

277TOC_105
278Netware_Basics
279browse
280Netware Basics
281netwarebasics
282netwarebasics
283TOC_106
284What's the story with buffer overflows on NT?

16 Netware Accounts#[285]$[286]+[287]

K[288]#[289]K[290]The following section deals with Accounts on Netware systems.

16.1 What are common accounts and passwords for Netware?#[291]K[292]

Out of the box Novell Netware has the following default accounts - SUPERVISOR, GUEST, and Netware 4.x has ADMIN and USER[lowbar]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:

285TOC_107
286Netware_Accounts
287browse
288Netware Accounts
289netwareaccounts
290netwareaccounts
291TOC_108
292What are common accounts and passwords for Netware?

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
ARCHIVIST	Palidrome default account for backup
CHEY_ARCHSVR	An account for Arcserve to login to the server from from the console for tape backup. Version 5.01g's password was WONDERLAND. Delete the Station Restrictions and use SUPER.EXE to

```
toggle this
                        account and you have an excellent
backdoor.
        WINDOWS_PASSTHRU Although not required, per the
Microsoft Win95
                        Resource Kit, Ch. 9 pg. 292 and
Ch. 11 pg. 401 you
                        need this for resource sharing
without a password.
        ROOT            Found on Shiva LanRovers, gets you
the command-line
                        equiv of the AdminGUI. By default,
no password. A lot
                        admins just use the AdminGUI and
never set up a
                        password.
```

VARs (Value Added Resellers) repackage Netware with their own hardware or with custom software. Here is a short list of known passwords:

```
        VAR      Account     Password  Purpose
        -------  ----------  --------
-----------------------------------------
        STIN     SUPERVISOR  SYSTEM    Travel agency
running SABRE
        STIN     SABRE       -none-    Like a guest
account
        STIN     WINSABRE    WINSABRE  Windows guest
account for NW 2.15c
        STIN     WINSABRE    SABRE     Windows guest
account for NW 3.x
        HARRIS   SUPERVISOR  HARRIS    Tricord reseller,
ships NW preinstalled
        NETFRAME SUPERVISOR  NF        Also NETFRAME and
NFI
        NETFRAME             aaa       New installation
default password
```

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[lowbar]TEMPLATE a password. Occassionally admins will check up on GUEST, but most forget about

USER[lowbar]TEMPLATE. In fact, *I* forgot about USER[lowbar]TEMPLATE until itsme reminded me.

This list is also a good starting point for account names for "backdoors". In some environments these account names will be left alone, particularly in large companies, especially Netware 4.x sites with huge trees. And don't forget account names like Alt-255 or NOT-LOGGED-IN.

16.2 How can I figure out valid account names on Netware?#[293]K[294]

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 your in with any valid account, you can run USERLST.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 guees 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
```

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
```

The same thing will happen as the MAP command. If valid, you will be prompted for a

293TOC_109
294How can I figure out valid account names on Netware?

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.

In 4.1 CHKNULL shows you every account with no password and you do not have to be logged in. For this to work bindery emulation must be on. But there is another way to get them in 4.1:

Once you load up the VLMs you may be able to view the entire tree, or at least all of the tree you could see if logged in. Try this:

```
CX /T /A /R
```

During the installation of 4.1, [lsqb]Public] has browse access to the entire tree because [lsqb]Public] is added to [lsqb]Root] as a Trustee. The Inherited Rights Filter flows this stuff down unless explicitly blocked. If you have the VLMs loaded and access to CX, you don't even have to log in, and you can get the name of virtually every account on the server.

If CX /T /A /R works, then NLIST USER /D will yield a massive amount of information, including who belongs to what groups, and their object ID. By combining the information between these two along with other NLIST options, you can learn a lot about an NDS tree and a server. Here a few more that come in handy:

```
        NLIST GROUPS /D       -List of groups,
descriptions, and members.
        NLIST SERVER /D       -List of servers, versions,
if attached you can determine if accounting is installed.
        NLIST /OT=* /DYN /D   -List of all readable
objects, including dynamic objects, names of NDS trees,
etc.
```

Between using CHKNULL, CX, and NLIST an intruder could not only learn who is in what group and who has access to what, but certainly could learn who the administrators are, and specifically select accounts for attack.

Finally, consider using the Intruder utility from NMRC's Pandora v3.0. This utility has a mode that allows you to give it a list of potential account names, and it will tell you if they are valid and even if they have no password. See http://www.nmrc.org/pandora/index.html

for details.

17 Netware Passwords#[295]$[296]+[297]

K[298]#[299]K[300]This section deals with Netware passwords.

17.1 How do I access the password file in Netware?#[301]K[302]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 located in a different location on the SYS: volume. It is a hidden directory called [lowbar]NETWARE. In this directory are located the NDS files, license files, and a number of other system-related files such as login scripts and auditing files.

295TOC_110
296Netware_Passwords
297browse
298Netware Passwords
299netwarepasswords
300netwarepasswords
301TOC_111
302How do I access the password file in Netware?

```
        File                    What it is
        --------------          --------------------------
        VALUE.NDS               Object and property values
        BLOCK.NDS               Extended property values
        ENTRY.NDS               Object and property types
        PARTITIO.NDS            NDS partition info
(replication info, etc.)
        MLS.000                 License file.
        VALINCEN.DAT            License validation
```

To view the hidden SYS:[lowbar]NETWARE directory, you can try to use RCONSOLE and the Scan Directory option, although later versions of Netware 4.x have patched this (starting with 410pt3). 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 [lowbar]NETWARE directory. SYS:[lowbar]NETWARE is hidden better on 4.1 than 4.0x, but in pre-410pt3 patched 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.

Using JCMD.NLM, it is possible to access SYS:[lowbar]NETWARE, and do many fun things, like copy NDS, etc. But what hackers have asked for is a way to access this directory WITHOUT uploading an NLM via RCONSOLE. You can try using NETBASIC.NLM (see the Netware Console Attacks section for details), and actually copy NDS files to a directory you can access (like SYS:PUBLIC).

17.2 What's the full story with Netware passwords?

#[303]K[304]A Novell proprietary algorithm takes the password, and produces a 16 byte hash. This algorithm is the same for versions 3.x and 4.x of Netware. The algorithm is also inside the LOGIN.EXE file used by the client when logging in. The details of the algorithm itself can be found in the CRYPT.TXT file included with Pandora (see http://www.nmrc.org/pandora/index.html for details).

The 16 byte hash is stored within the bindery files in Netware 3.x and NDS in Netware 4.x. Since the object ID is used in the algorithm, it adds the equivalent of a salt. This along with the fact that the password length plays into the algorithm increases the overhead in cracking multiple passwords at once. Fortunately for the cracker, both the object ID and the password length are stored with the hash, along with that fact that lower case letters are converted to upper case before generating the hash does simplify the process slightly. Password crackers can brute force a little easier since they can eliminate trying lower case letters and concentrate on a particular password length.

17.3 How does password cracking work with Netware?

#[305]K[306]Because of the

303TOC_112
304What's the full story with Netware passwords?
305TOC_113
306How does password cracking work with Netware?

complexity of the algorithm, using it the way it was designed is somewhat slow for cracking, especially by brute force. However the algorithm can be mathematically improved, and in fact WAS improved and optimized just for cracking purposes. See Jitsu-Disk's document CRYPT.TXT that was included with Pandora that details this. The algorithm is dozens of times faster than Novell's original code. However brute force is slow work with Netware, so only use it as a last resort, especially if you have a LOT of time.

This is especially true with regards to the brute force crackers that attack from the client. Since you are dealing with the network itself, expect AT BEST about a password attempt a second from most network cracking utilities.

17.4 How does password cracking work with Netware?

#[307]K[308]With Pandora v3.0 you have the fastest dictionary cracking available. And if you must attack from a client, make sure if you are using a cracker that you are using dictionary attacking.

For Netware 3.x systems, consider using Al Grant's Bindery tool.

17.5 Can an Sys Admin prevent/stop Netware password hash extraction?

#[309]K[310]The best way for a Sys Admin to prevent Netware password hash extraction is to at least try the following:

- Protect the server console. If the console is compromised, all bets are off. Don't use RCONSOLE at all. Go to the console to do any administrator-type work.
- Protect administrative accounts. If one of these accounts are compromised, once again all bets are off. Use these accounts minimally from secured workstations.
- Clean up after yourself. If you run a BINDFIX, DSMAINT, or DSREPAIR, remember that you are leaving files out there that passwords can be recovered from. Do your business, confirm you don't have to fall back using one of these leftover files and then delete and purge them.

You see, once the server has been compromised, sometimes not even completely, there will be NOTHING to stop unwanted password recovery. Hackers, just do the opposite of the above items and you'll be fine ;-)

17.6 Can I reset an NDS password with just limited rights?

#[311]K[312]There is a freeware utility called N4PASS, that is meant for Netware 4.10 (uses NDS calls and is not bindery based). The intention of this package is to enable a Help Desk to reset passwords for users without granting them tons of rights. It uses full logging and does not require massive ACL manipulation to do it.

Obviously being set up to use this utility opens a few doors. The filename is N4PA12.EXE,

307TOC_114
308How does password cracking work with Netware?
309TOC_115
310Can an Sys Admin prevent/stop Netware password hash extraction?
311TOC_116
312Can I reset an NDS password with just limited rights?

and can be retrieved from the author's web site at http://fastlane.net/homepages/dcollins and the author can be reached at dcollins@fastlane.net.

A couple of interesting things about this utility -- if configured incorrectly the server may be compromised in a number of ways. For instance, the password generated is a calculation that uses a 'temp filename', the date, the user's loginname, helpdesk login name, seed value, and a few other items. (its in the n4pass.txt file)

N4PASS is not set to purge immediately, the file is salvagable. Also, if the rights to the N4PASS directory are too open, you can discover the default password, among other things. The text file included with the utility covers this, so read it carefully if you are installing it. If you are hacking, read it carefully too ;-)

It is critical that access to the sys:pass