GIAC Windows 2000

PRACTICAL ASSIGNMENT FOR

SANS Tract 5

Making the Crackable Password "Non-Crackable"

December 2000

Prepared By

Lois Loser

TABLE OF CONTENTS

Introduction

This paper is the practical assignment portion of the GIAC-NT certification curriculum (Track 5) sponsored by SANS. As such, this document will address password security in Windows 2000, as well as NT. It will discuss where each window platform stores passwords, how to gain access to the password file, and then how to crack user and administrator passwords. We will look at the various tools for exploiting passwords, as well security features in 2000 and NT that are meant to raise the "barrier" to the would be hacker.

The main discussion will center on the use of unprintable ASCII characters imbedded in user names and passwords that can thwart a hacker's attempt in gaining access to your domain by cracking passwords. How many times have you sat through a security training course and heard the instructor say, "Just put an unprintable character in your password." Well, Jason, Jaseper, Gene, and others at SAN's, which unprintable (or ALT-character) is safe to use? Or are all the ALT-characters equal in reducing your security risks? This paper will answer that question.

As Microsoft states in their Introduction to Windows 2000 Security – "Security requires simplicity." The simplicity of unprintable characters is unbeatable.

Cracking Passwords – Windows 2000/NT

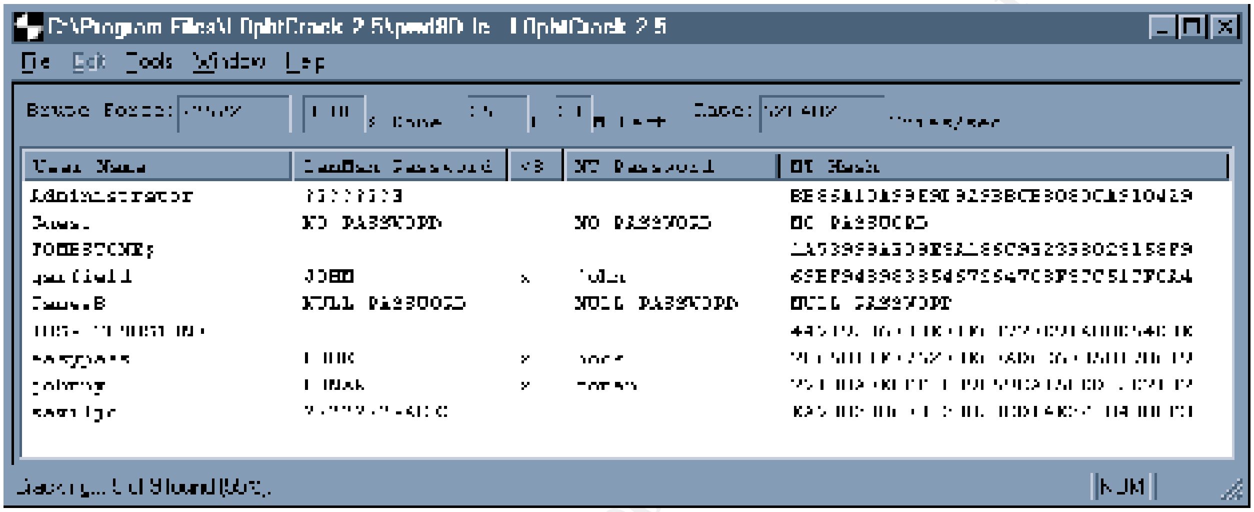
In its efforts to maintain backward compatibility, Microsoft Windows 2000 contains the same security flaw in passwords as NT – the LAN Manager password scheme. When implementing Windows 2000 in native mode, Windows utilizes all the Windows 2000 security features. However, if a mixed environment exists (Windows 2000, NT, 9x, Macintosh), then Windows reverts to the Windows NT security mechanisms. To support pre-NT clients and servers, NT automatically sends and accepts the LM responses, which is a dangerous weakness and opens a vulnerability in a hacker's ability to capture and crack passwords.

L0phtCrack 2.5

Another vulnerability in the LAN Manager password scheme is that a fourteen-character password is broken into two halves of seven characters each. This enables a program like L0phtCrack 2.5 to take two 7-character passwords versus one 14-character password and attempt to crack them both simultaneously. By simultaneously cracking the two halves of the password, the hacker reduces the time required to crack passwords.

Windows NT will allow L0phtCrack 2.5 to run against the NT 4.0 domain server and get the user name and password hash list from any local or network computer. Once the hacker knows this information, the hacker can just start cracking away at his leisure. However in Windows 2000 environment, L0phtCrack 2.5 will return only the Administrator and Guest account information. This is because L0phtCrack 2.5 is pulling the information from the SAM database. Here is where Microsoft raised the security barrier in Windows 2000 – Active Directory now contains user account information, not the SAM data base. Although an administrator may feel relief that L0phtCrack 2.5 will no longer work on Windows 2000, the relief is short-lived due to another utility (PWDump2) that will dump the user account and password hash to a text file. L0phtCrack 2.5 imports this text file into its application for the hacker's use.

Below is a screenshot of L0phtcrak 2.5 in action. Notice how LAN Manager passwords are all in upper case. This allows L0phtCrack 2.5 to dismiss all lower case letters when attempting to crack a password. This lowers the barrier a hacker must cross over to gain the knowledge he is after.

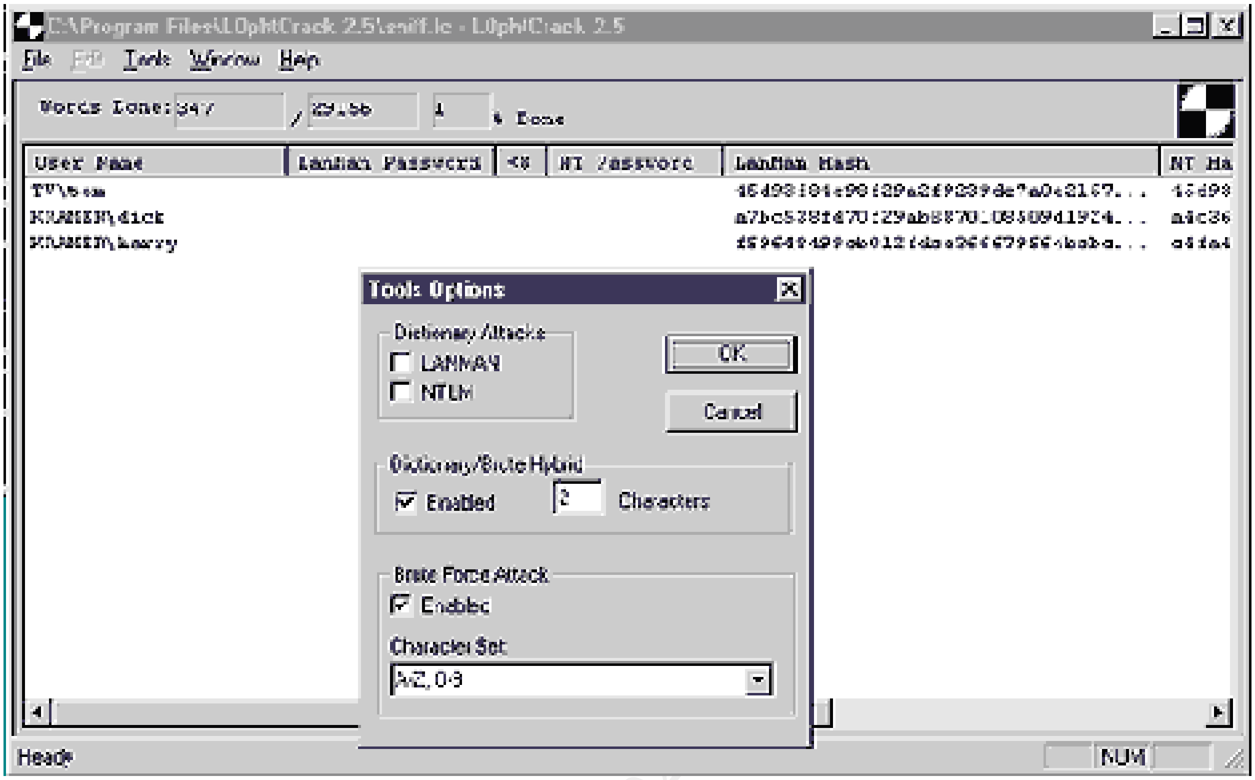


User Name	LanMan Password	<8	NT Password	NT Hash
Administrator	[illegible]			[illegible]
Guest	NO PASSWORD		NO PASSWORD	NO PASSWORD
[illegible]				[illegible]
garfield	JOHN	x	John	[illegible]
[illegible]	NULL PASSWORD		NULL PASSWORD	NULL PASSWORD
[illegible]				[illegible]
[illegible]	[illegible]	x	[illegible]	[illegible]
johnny	[illegible]	x	[illegible]	[illegible]
[illegible]	[illegible]			[illegible]

Cracking... [illegible]

Once the data is collected, the attack can begin using one of the many flexible tools L0phtCrack 2.5 offers. To crack a password hash, L0phtCrack 2.5 first performs a dictionary attack by iterating through a list of common words found in a dictionary. After exhausting the dictionary attack, L0phtCrack 2.5 will then attempt a hybrid attack. The hybrid attack takes the dictionary listing and adds different combinations of a few characters to the beginning and end of each word prior to the hashing.

The screen shot below demonstrates a hybrid attack in combination with a dictionary.



C:\Program Files\L0phtCrack 2.5\sniff.lc - L0phtCrack 2.5
File Edit Tools Window Help

Words Done: 947 / 29156 1 % Done

User Name	LanMan Password	<8	NT Password	LanMan Hash	NT Ha
TV\tom				45498184e98f29a2f9239de7a0e2167...	45d98
KRAMER\dick				a7bc5381470f29ab8870108509d1924...	a4c36
KRAMER\harry				f59649499ab012fdae2666795fcbaba...	a4fa4

Tools Options

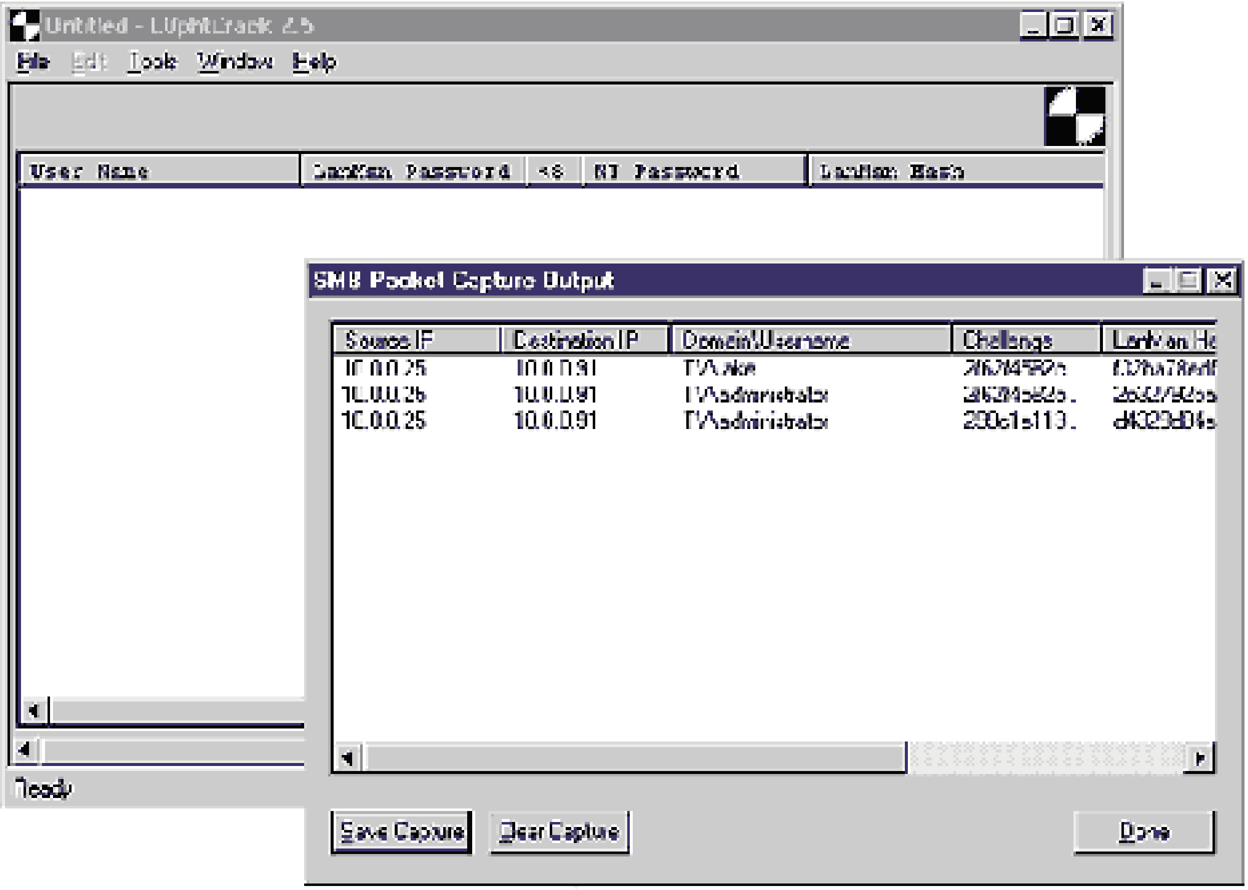
Dictionary Attacks
☐ LANMAN
☐ NTLM

Dictionary/Brute Hybrid
☑ Enabled 2 Characters

Brute Force Attack
☑ Enabled
Character Set: A-Z, 0-9

This hybrid attack calculates how a user might implement the policies passprop enables, i.e., bird1, 2funny, etc. This method will take longer than dictionary-only attack, but less time than a brute force attack. Finally, L0phtCrack 2.5 will attempt a brute force attack.

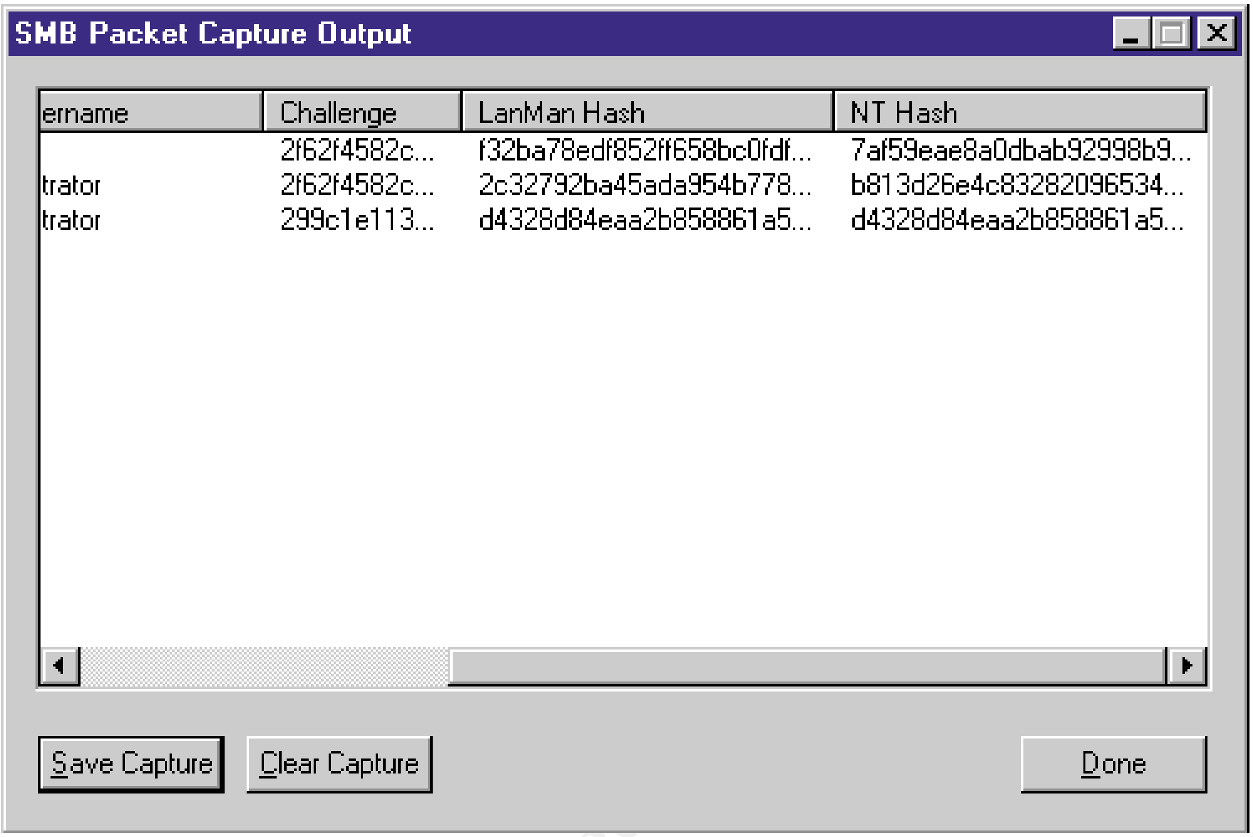
L0phtcrack 2.5 can also sniff passwords as they transverse the network via its SMB Packet Capture Output utility. The new GUI sniffer eliminates the need for a special packet driver. This shrink-wrapped tool lets even novice intruders easily learn the passwords of everyone logging on to the network segment. The screen shot below demonstrates the output of this utility. The capture can be saved at any time using the Save Capture button. To crack these hashes you must save the capture and then open the captured file using the File Open Password command. Also, you can capture and crack other passwords at the same time.


Untitled - L0phtCrack 2.5
File Edit Tools Window Help
Ready
SMB Packet Capture Output
Save Capture
Clear Capture
Done

User Name	LanMan Password	<8	NT Password	LanMan Hash

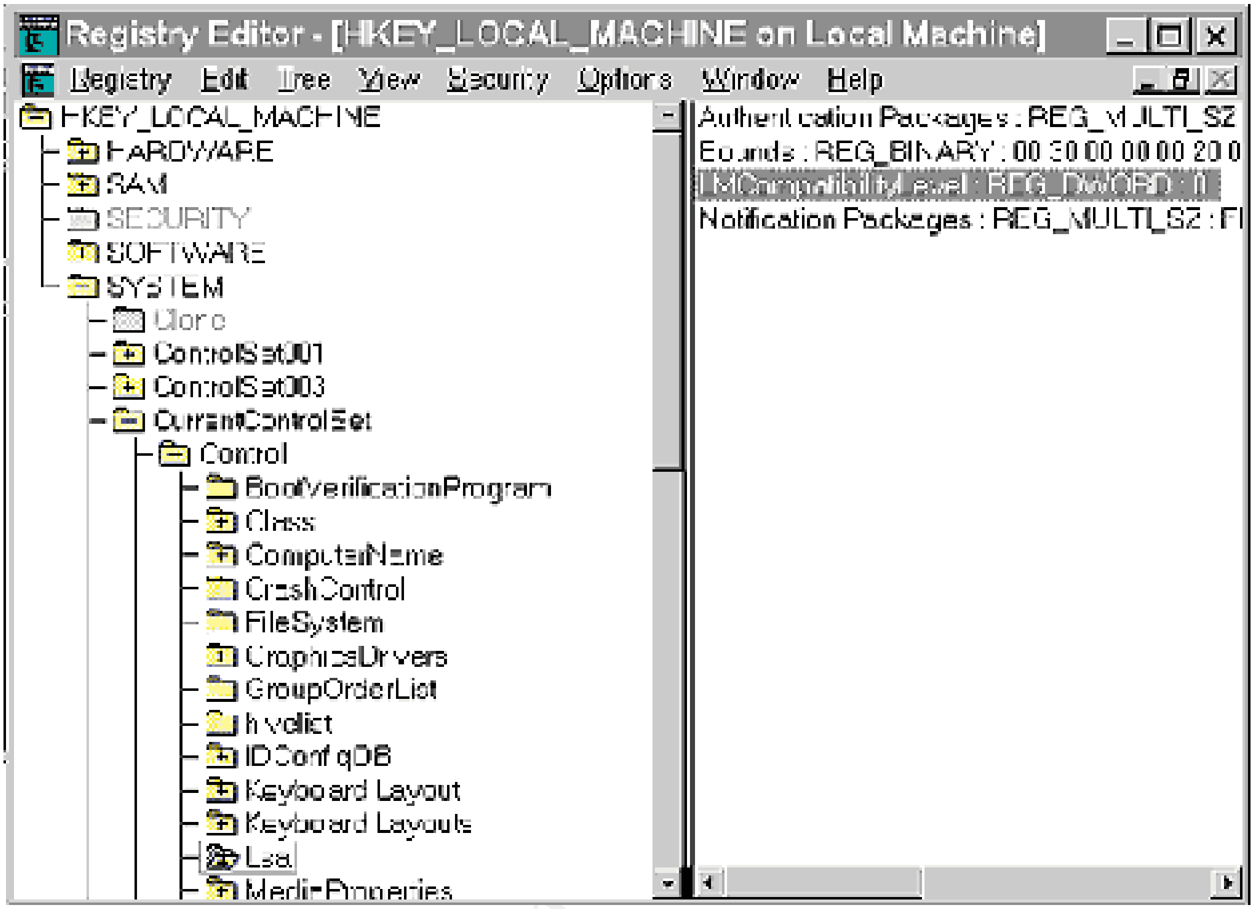
Source IP	Destination IP	Domain\Username	Challenge	LanMan Ha
10.0.0.25	10.0.0.91	T\Jake	2f6714592a	f37ba78ed
10.0.0.25	10.0.0.91	T\administrator	2f62f4582b...	2b6076d2ea
10.0.0.25	10.0.0.91	T\administrator	290c1e113...	d4323d04e

Not only is the source IP, destination IP, domain name, username collected, but also the LM and NTLM hashes. Notice the LM hash and the NT hash are different. This is because of Microsoft's creation of new LM response and NT response versions for security and backward compatibility.



ername	Challenge	LanMan Hash	NT Hash
	2f62f4582c...	f32ba78edf852ff658bc0fdf...	7af59eae8a0dbab92998b9...
trator	2f62f4582c...	2c32792ba45ada954b778...	b813d26e4c83282096534...
trator	299c1e113...	d4328d84eaa2b858861a5...	d4328d84eaa2b858861a5...

The LMCompatibilityLevel Registry value controls what logon responses the clients send to the server and what responses the servers accept. LMCompatibilityLevel is in the HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSetControl\ Lsa key.



```
Authentication Packages : REG_MULTI_SZ
Bounds : REG_BINARY : 00 30 00 00 00 20 0
LMCompatibilityLevel : REG_DWORD : 0
Notification Packages : REG_MULTI_SZ : FI
```

You can set LMCompatibilityLevel, of type REG_DWORD, between the levels 0 and 5, with level 5 offering the highest security and lowest backward compatibility. To provide the highest security, you need to prevent transmission of the LM response, which is vulnerable to shrink-wrapped intruder tools. Listed below is a brief description of the security function for each value of LMCompatibilityLevel.

LMCompatibilityLevel Security Settings

Level	Security Function
Level 0	Send LM response and NTLM response; never use NTLMv2 session security
Level 1	Use NTLMv2 session security if negotiated between client and server
Level 2	Send NTLM authentication only
Level 3	Send NTLMv2 authentication only
Level 4	Domain controller refuses LM authentication on down level clients
Level 5	Domain controller refuses LM and NTLM authentication (accepts only NTLMv2)

PWDump2

Todd Sabin released an update to PWDump2 that will get the unencrypted password hashes from the OS memory. To use PWDump2 requires administrator privileges and the LSASS process ID.

To find the LSASS ID, click the Processes tab in Task Manager. To execute PWDump2, at the command line type:

```
Pwdump2 LSASS# > hashes.txt
```

On a Windows NT system, PWDump2 will write the username and password hashes for each account in the local system's SAM to the file hashes.txt. If you run this utility on a Windows 2000 system and the hashes.txt file only contains the Administrator and the Guest account, the user has the older version of PWDump2 and will need to update. Below is information to discern which version you have and are running.

	Originial date/file size	Update date/file size
PWDump2	8.23.98/46,080 bytes	3.28.00/32,768 bytes
Samdump.dll	8.23.98/49,644 bytes	3.28.00/36864 bytes

The newest version of PWDump2 has two enhancements. First you no longer need to know the LSASS ID number, the application determines this information. Also, the newer version recognizes you are on a Windows 2000 domain controller and dumps the hashes from the Active directory. Execution is as simple as typing:

```
Pwdump2 > hashes.txt.
```

Life just continues to get easier for the would-be hacker. After obtaining the hashes, the hacker merely needs to run L0phtCrack 2.5 against the text file.

Protecting Passwords on Windows NT

Although everyone is quick to state that Windows NT stores passwords in the SAM, this can be a misleading statement if one thinks the SAM database resides in one area of the O/S only – on the Primary Domain Controller (PDC). In actuality, Windows NT stores passwords in several areas. NT stores a permanent working copy of the SAM database on your hard drive, as well as on all domain controllers including Backup Domain Controllers (BDC). The PDC holds the master copy of the SAM. NT queries the SAM on the BDCs for storing and retrieving user credentials, i.e., passwords. During day-to-day operations, NT is likely to store the SAM database in two places on a hard disk: the %systemroot% repair directory and the %systemroot%system32\config directory. Although the \config directory contains a working version of the SAM database that the live O/S uses, programs such as Windows Explorer can't directly access the database for copying while the system is running. This inaccessibility results from the fact that the Local Security Authority (LSA) system process has locked the file for exclusive use.

Although users cannot ordinarily access the SAM key with the Registry editor because NT limits the permissions on the key to the built-in SYSTEM account, it can be exploited under the user context of the SYSTEM account. Hackers know how NT handles the SAM and realize the vulnerability that exists to compromise the SAM database from any computer attached to the domain. Microsoft introduced several methods for protecting the SAM from these vulnerabilities.

User Manager – Policies – Account

The easiest method for protecting passwords is in the User Manager – Policies – Account. Using this NT feature, an administrator can set user policy to include length of password, password aging, and limit reuse of passwords. The drawback to using this method only is passwords are as strong as a user will make it. The user can make passwords containing dates, names, or dictionary words.

Passfilt.dll

NT 4.0 SP2 introduced the Passfilt.dll as a next step to raising the barrier for creating stronger passwords. Passfilt.dll implements the following password policy:

> Passwords may not contain your user name or any part of your full name.
> Passwords must be at least six characters long.
> Passwords must contain characters from at least three of the following four classes:

English upper case letters	A, B, C, ... Z
English lower case letters	a, b, c, ... z
Westernized Arabic numerals	0, 1, 2, ... 9
Non-alphanumeric ("special characters") such as punctuation symbols	({}[],.<>;:'"?/|\\`~!@#$%^&*()_-+=)

When implementing passfilt.dll, the program hard-codes the above requirements into the file. Neither the user interface nor the registry can make these changes. If requirements change, someone must write a new .dll to incorporate changes.

A word of caution: passfilt.dll is not effective on Windows 3.x, Windows for Workgroups 3.x, or Macintosh. This makes it unenforceable on the O/S's identified above. Windows 95 does not support case-sensitivity in passwords. However, on a Window 95 computer when a password is changed to New1pass, the user can use New1pass, NEW1PASS, New1Pass, new1pass, etc. to log on to the domain. But when the user logs into the domain using a Windows NT computer, New1pass is the required password.

To ensure Strong Password functionality occurs throughout the domain structure, make the following changes on all PDCs (or stand-alone servers, where needed). Remember passfilt.dll is not necessary on BDCs since the PDC is the only machine where changes to the domain accounts database are made. However, since BDCs can become a PDC, administrators should install passfilt.dll on all BDCs. If an administrator promotes a BDC to a PDC without passfilt.dll installed, then strong password enforcement will be lost.

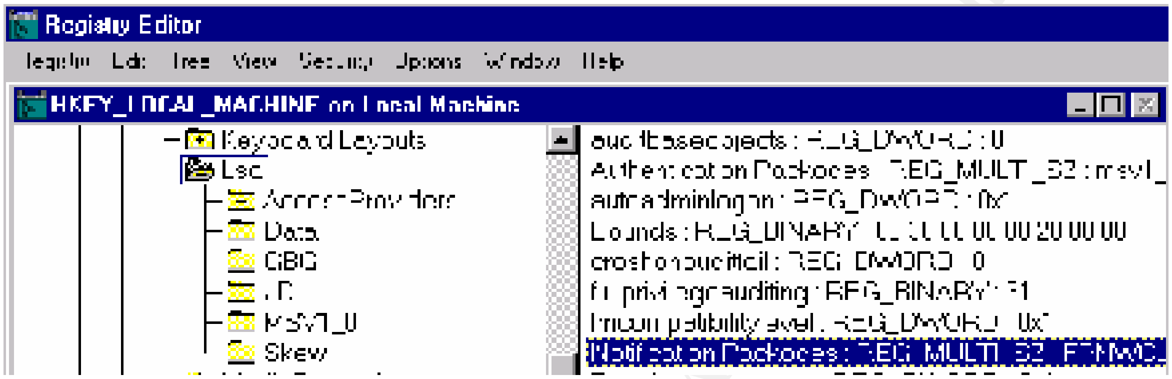
To install passfilt.dll, follow these steps:

1.Install the latest Windows NT 4.0 service pack.

2.Copy Passfilt.dll to the %SYSTEMROOT%\SYSTEM32 folder.

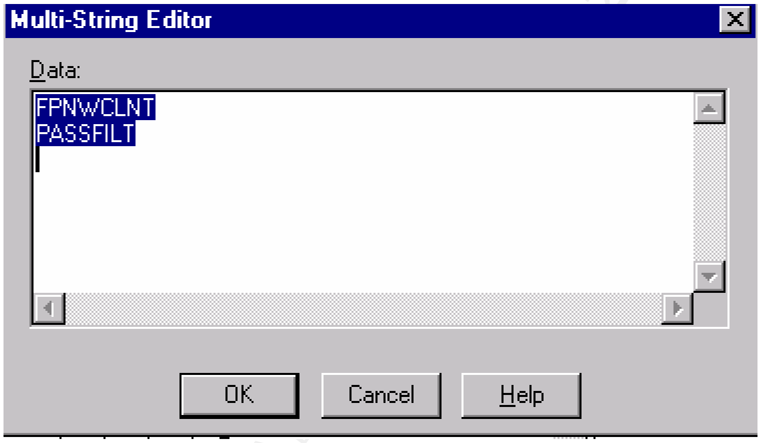
3. Go the following key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA

4. Double-click the "*Notification Packages*" key and add the following value:


Registry Editor
Registry Edit Tree View Security Options Window Help
HKEY_LOCAL_MACHINE on Local Machine
Keyboard Layouts
Lsa
AccessProviders
Data
GBG
JD
MSV1_0
Skew

auditbaseobjects : REG_DWORD : 0
Authentication Packages : REG_MULTI_SZ : msv1_
autoadminlogon : REG_DWORD : 0x
Bounds : REG_BINARY : 00 30 00 00 00 20 00 00
crashonauditfail : REG_DWORD : 0
fullprivilegeauditing : REG_BINARY : 01
lmcompatibilitylevel : REG_DWORD : 0x
Notification Packages : REG_MULTI_SZ : FPNWCL

5. If the value FPNWCLNT is already present, place the following entry beneath the FPNWCLNT entry: PASSFILT



FPNWCLNT
PASSFILT

6. Click OK and then exit Registry Editor.

7. Shut down and restart the computer running Windows NT Server.

Passprop.exe

Passprop.exe is a utility available in the NT Resource Kit. This command line utility has four available switches. This utility expands on the capabilities of User Manager and passfilt.dll.

Passprop /simple – Restores simple passwords (NT default)

Passprop /complex—Forces passwords to have a mixture of upper and lower-case, symbols or numbers.

Passprop /adminlockout—Allows the Administrator account to be locked out except for interactive sessions at a Domain Controller.

Passprop /noadminlockout—Restores NT default when Administrator account can't be locked out.

SYSKEY

A final method is using SYSKEY. The system key technology encrypts the SAM database and requires the use of an encryption key to boot the O/S. The administrator has three options when implementing SYSKEY:

1) use a machine generated random key as the system key and store the key on the local machine using a complex algorithm;
2) use a machine-generated random key and store the key on a diskette; or,
3) use an administrator-chosen password to derive the system key.

A word of caution when using SYSKEY – there is NO uninstall process should you change your mind on how to implement SYSKEY. The storage method you chose must be optimal for your network. Also, immediately after installing SYSKEY a new Emergency Repair Disk (ERD) must be created. Without a new ERD an administrator will not be able to recover the system when recovery process is needed. Although administrators logged into the system still have the ability to dump the SAM database into a crackable format, if a hacker gains access to your system and copies the SAM, he will not be able to extract usable password hashes.

The \repair directory contains the same information as the ERD, which you create using rdisk.exe and use for system recovery. Both the \repair directory and the ERD contain copies of the SAM database and require ample protection. Protect your ERD with the same security as your backup tapes.

To protect the \repair directory, set the permissions to disallow unwanted users from accessing the directory and its files, especially the sam._ file, which contains a copy of the SAM database. To protect files in the \repair directory, carefully perform the following steps using cacls.exe from the Microsoft Windows NT Server 4.0 Resource Kit, or a similar tool. Open a command prompt, navigate to %systemroot% (usually C:\winnt), and type

```
cacls repair /g administrators:F system:F /t
```

You've now granted administrators and the system user full control to the subdirectory and all the files stored in it. Since the administrator did not edit the ACL, NT removed all other users' permissions.

It is also important to remember that SYSKEY does not encrypt the username – only the password. SYSKEY does prevent SAM dumping with the tool built into L0phtCrack 2.5 and PWDump. However, PWDump2 can dump the SAM because it uses DLL injection techniques that PWDump does not (see discussion above on PWDump2).

What makes Windows 2000 different from NT?

However, Microsoft raised the barrier on this password vulnerability in Windows 2000. Windows 2000 will still send information to L0phtcrack 2.5 and the application accepts the information. However, the information is worthless because it is not the true NTLM or LM hash. Windows 2000 stores passwords and user identification data in Active Directory. In Windows 2000 all domain controllers in the domain are peers; therefore, each domain controller holds a copy of the Active Directory.

Windows 2000 also uses Kerberos 5.0 to authenticate passwords. Kerberos is the new security protocol that replaces the NT LAN Manager authentication protocol found in Windows NT. Kerberos allows a user to prove his identity without revealing information that could compromise network security with a three components to the authentication process. First is the Client/server (CS) Exchange, or the client application that represents the user. In this sub-protocol, the client presents the ticket for admission to a service. Next is the Ticket-Granting Service (TGS) Exchange where the KDC distributes a service session key and a ticket for the service. The last component is Authentication Service (AS) Exchange where the KDC gives the client a logon session key and a TGT. In most cases the KDC is a central repository for information about clients. Although Kerberos is an effective tool to prevent unauthorized network access, no protector is fail-safe. Kerberos can fall victim to a dictionary attack on passwords if users do not utilize strong passwords.

Protecting Passwords on Windows 2000

As mentioned earlier, Windows 2000 contains all the security features as Windows NT, hence the functionality described above in passfilt.dll is now included in the operating system security components for Windows 2000. To configure strong password requirements for the domain, configure a group policy object linked to the domain. To implement strong password requirements, follow these steps:

1. Start the Group Policy Editor in the Microsoft Management Console (MMC) snap-in. A quick method is to:
    a. Right click the domain object in the Active Directory Users and Computers MMC snap-in
    b. Click on Properties
    c. Click on Group Policy tab
    d. Click the Default Domain Policy GPO link
    e. Click on Edit
2. Navigate to the following node in the group policy object: Group Policy Object Policy\Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy

3. Double click Passwords must meet complexity requirements of installed password filter to produce the application dialog box
4. Change the template setting to Enabled to active strong password requirements

A word of caution: As with all policy settings, the change is not in effect until the next time group policy objects are applied to the domain controllers.

Creating the "non-crackable" password

Creating the "non-crackable" password is truly an oxymoron – it is usually only a matter of time until someone finds a way to crack the "non-crackable" password. Windows NT passwords can contain special ALT characters, as well as some extra Windows characters. Scott Crawford, a Network Administrator from Evangel University, Springfield, MO, recently studied how L0phtCrack 2.5 analyzes passwords in Windows NT. Since L0phtCrack 2.5 only offers to crack up to 68 of the possible 256 characters in the ASCII character set, Crawford's research discovered that **187 characters** of 380 that **L0phtCrack 2.5 cannot crack**.

The average hacker is usually looking for the "low hanging fruit", that is, run L0phtCrack 2.5 using the standard offerings from within L0phtCrack 2.5, i.e., dictionaries and hybrid searches. As described earlier, to crack a password hash, L0phtCrack 2.5 first performs a dictionary attack by iterating through a list of common words. L0phtCrack 2.5 hashes each word in the list and compares that hash to the hash from the SAM (Windows NT). If the hashes match, L0phtCrack 2.5 has the password. Once L0phtCrack 2.5 exhausts the dictionary, it iterates through the word list again using a hybrid attack that adds combinations of a few characters to the beginning and end of each word prior to hashing. This attempt gathers any passwords that a user has created by simply appending random characters to a common word. Finally, L0phtCrack 2.5 resorts to brute force to crack any remaining hashes, trying every possible combination of characters.

To access the ALT-characters for use in the "non-crackble" password, a user must hold down on the ALT key plus enter a three or four digit number on the numeric keyboard. The ALT key must be held down while the additional numeric keypad keys are pressed. Also, my research demonstrates that the num-lock key does not need to be activated to utilize the ALT-characters – the num-lock key can be on or off. The advantage of using the ALT-characters is the greater number of combinations added to the range of passwords a user can utilize. The ALT-characters do not correspond to regular keys. Crawford states that passwords with ALT-characters imbedded are not crackable by L0phtCrack 2.5 even when the characters are added to a customized dictionary.

Testing the "non-crackable" password

Being a bit dubious as to the validity of Crawford's study, I recreated the research on a Windows 2000 platform by creating 380 accounts where the user name and password corresponded with the ALT chart below.

Table 1 - all ALT combinations and their corresponding characters (Crawford)

0 = NUL	36 = $	72 = H	108 = l	144 = √â	180 = ,î§	216 = ,ï™	252 = ,Åø	0159 = ≈∏	0195 = √É	0231 = √ß
1 = ,ò∫	37 = %	73 = I	109 = m	145 = √¶	181 = ,ï°	217 = ,îò	253 = ¬≤	0160 = BLANK	0196 = √Ñ	0232 = √®
2 = ,òª	38 = &	74 = J	110 = n	146 = √Ü	182 = ,ï¢	218 = ,îå	254 = ,ñ†	0161 = ¬°	0197 = √Ö	0233 = √©
3 = ,ô•	39 = '	75 = K	111 = o	147 = √¥	183 = ,ïñ	219 = ,ñà	255 = BLANK	0162 = ¬¢	0198 = √Ü	0234 = √™
4 = ,ô¶	40 = (	76 = L	112 = p	148 = √∂	184 = ,ïï	220 = ,ñÑ	0127 =	0163 = ¬£	0199 = √á	0235 = √´
5 = ,ô£	41 =)	77 = M	113 = q	149 = √≤	185 = ,ï£	221 = ,ñå	0128 = ,Ç¨	0164 = ¬§	0200 = √à	0236 = √¨
6 = ,ô†	42 = *	78 = N	114 = r	150 = √ª	186 = ,ïë	222 = ,ñê	0129 = ¬Å	0165 = ¬•	0201 = √â	0237 = √≠
7 = ,Ä¢	43 = +	79 = O	115 = s	151 = √π	187 = ,ïó	223 = ,ñÄ	0130 = ,Äö	0166 = ¬¶	0202 = √ä	0238 = √Æ
8 = ,óò	44 = ,	80 = P	116 = t	152 = √ø	188 = ,ïù	224 = Œ±	0131 = Δí	0167 = ¬ß	0203 = √ã	0239 = √Ø
9 = ,óã	45 = -	81 = Q	117 = u	153 = √ñ	189 = ,ïú	225 = √ü	0132 = ,Äû	0168 = ¬®	0204 = √å	0240 = √∞
10 = ,óô	46 = .	82 = R	118 = v	154 = √ú	190 = ,ïõ	226 = Œì	0133 = ,Ä¶	0169 = ¬©	0205 = √ç	0241 = √±
11 = ,ôÇ	47 = /	83 = S	119 = w	155 = ¬¢	191 = ,îê	227 = œÄ	0134 = ,Ä†	0170 = ¬™	0206 = √é	0242 = √≤
12 = ,ôÄ	48 = 0	84 = T	120 = x	156 = ¬£	192 = ,îî	228 = Œ£	0135 = ,Ä°	0171 = ¬´	0207 = √è	0243 = √≥
13 = ,ô™	49 = 1	85 = U	121 = y	157 = ¬•	193 = ,î¥	229 = œÉ	0136 = ÀÜ	0172 = ¬¨	0208 = √ê	0244 = √¥
14 = ,ô´	50 = 2	86 = V	122 = z	158 =,Çß	194 = ,î¨	230 = ¬µ	0137 = ,Ä∞	0173 = ¬≠	0209 = √ë	0245 = √µ
15 = ,òº	51 = 3	87 = W	123 = {	159 = Δí	195 = ,îú	231 = œÑ	0138 = ≈†	0174 = ¬Æ	0210 = √í	0246 = √∂
16 = ,ñ∫	52 = 4	88 = X	124 = |	160 = √°	196 = ,îÄ	232 = Œ¶	0139 = ,Äπ	0175 = ¬Ø	0211 = √ì	0247 = √∑
17 = ,óÑ	53 = 5	89 = Y	125 = }	161 = √≠	197 = ,îº	233 = Œò	0140 = ≈í	0176 = ¬∞	0212 = √î	0248 = √∏
18 = ,Üï	54 = 6	90 = Z	126 = ~	162 = √≥	198 = ,ïû	234 = Œ©	0141 = ¬ç	0177 = ¬±	0213 = √ï	0249 = √π
19 = ,Äº	55 = 7	91 = [	127=,åÇ	163 = √∫	199 = ,ïü	235 = Œ¥	0142 = ≈Ω	0178 = ¬≤	0214 = √ñ	0250 = √∫
20 = ¬∂	56 = 8	92 = \	128 = √á	164 = √±	200 = ,ïö	236 = ,àû	0143 = ¬è	0179 = ¬≥	0215 = √ó	0251 = √ª
21 = ¬ß	57 = 9	93 =]	129 = √º	165 = √ë	201 = ,ïî	237 = œÜ	0144 = ¬ê	0180 = ¬¥	0216 = √ò	0252 = √º
22 = ,ñ¨	58 = :	94 = ^	130=√©	166 =¬™	202 = ,ï©	238 = Œµ	0145 = ,Äò	0181 = ¬µ	0217 = √ô	0253 = √Ω
23 = ,Ü®	59 = ;	95 = _	131 =√¢	167 = ¬∫	203 = ,ï¶	239 = ,à©	0146 = ,Äô	0182 = ¬∂	0218 = √ö	0254 = √æ
24 = ,Üë	60 = <	96 = `	132 =√§	168 = ¬ø	204 = ,ï†	240 = ,â°	0147 = ,Äú	0183 = ¬∑	0219 = √õ	0255 = √ø
25 = ,Üì	61 = =	97 = a	133 =√†	169 = ,åê	205 = ,ïê	241 = ¬±	0148 = ,Äù	0184 = ¬∏	0220 = √ú	
26 = ,Üí	62 = >	98 = b	134 = √•	170 = ¬¨	206 = ,ï¨	242 = ,â•	0149 = ,Ä¢	0185 = ¬π	0221 = √ù	
27 = ,Üê	63 = ?	99 = c	135 =√ß	171 = ¬Ω	207 = ,ïß	243 = ,â§	0150 = ,Äì	0186 = ¬∫	0222 = √û	
28 = ,àü	64 = @	100 = d	136=√™	172 = ¬º	208 = ,ï®	244 = ,å†	0151 = ,Äî	0187 = ¬ª	0223 = √ü	
29 = ,Üî	65 = A	101 = e	137 = √´	173 = ¬°	209 = ,ï§	245 = ,å°	0152 = Àú	0188 = ¬º	0224 = √†	
30 = ,ñ≤	66 = B	102 = f	138=√®	174 = ¬´	210 = ,ï•	246 = √∑	0153 = ,Ñ¢	0189 = ¬Ω	0225 = √°	
31 = ,ñº	67 = C	103 = g	139 =√Ø	175 = ¬ª	211 = ,ïô	247 = ,âà	0154 = ≈°	0190 = ¬æ	0226 = √¢	
32 = SPACE	68 = D	104 = h	140=√Æ	176 = ,ñë	212 = ,ïò	248 = ¬∞	0155 = ,Ä∫	0191 = ¬ø	0227 = √£	
33 = !	69 = E	105 = i	141 = √¨	177 = ,ñí	213 = ,ïí	249 = ,àô	0156 = ≈ì	0192 = √Ä	0228 = √§	
34 = "	70 = F	106 = j	142 =√Ñ	178 = ,ñì	214 = ,ïì	250 = ¬∑	0157 = ¬ù	0193 = √Å	0229 = √•	
35 = #	71 = G	107 = k	143 =√Ö	179 = ,îÇ	215 = ,ï´	251 = ,àö	0158 = ≈æ	0194 = √Ç	0230 = √¶	

I then used PWDump2 (latest version) to dump hashes to a text file and then ran L0phtcrack 2.5 against the file. Below are two tables demonstrating results.

Table 2 - ALT characters cracked with L0phtCrack 2.5 (Crawford)

Alt-0=NUL	Alt-72=H	Alt-112=P	Alt-0138=S	Alt-0206=I
Alt-33=!	Alt-73=I	Alt-113=Q	Alt-0139=<	Alt-0207=I
Alt-34="	Alt-74=J	Alt-114=R	Alt-0140=O	Alt-0208=D
Alt-35=#	Alt-75=K	Alt-115=S	Alt-0141=?	Alt-0210=O
Alt-36=$	Alt-76=L	Alt-116=T	Alt-0142=Z	Alt-0211=O
Alt-37=%	Alt-77=M	Alt-117=U	Alt-0143=?	Alt-0212=O
Alt-38=&	Alt-78=N	Alt-118=V	Alt-0144=?	Alt-0213=O
Alt-39='	Alt-79=O	Alt-119=W	Alt-0145=`	Alt-0215=X
Alt-40=(	Alt-80=P	Alt-120=X	Alt-0146='	Alt-0216=O

Alt-41=)	Alt-81=Q	Alt-121=Y	Alt-0147="	Alt-0217=U
Alt-42=*	Alt-82=R	Alt-122=Z	Alt-0148="	Alt-0218=U
Alt-43=+	Alt-83=S	Alt-123={	Alt-0150=-	Alt-0219=U
Alt-44=,	Alt-84=T	Alt-124=|	Alt-0151=-	Alt-0221=Y
Alt-45=-	Alt-85=U	Alt-125=}	Alt-0152=~	Alt-0222=_
Alt-46=.	Alt-86=V	Alt-126=~	Alt-0153=T	Alt-0224=A
Alt-47=/	Alt-87=W	Alt-131=A	Alt-0154=S	Alt-0225=A
Alt-48=0	Alt-88=X	Alt-133=A	Alt-0155=>	Alt-0226=A
Alt-49=1	Alt-89=Y	Alt-136=E	Alt-0156=O	Alt-0227=A
Alt-50=2	Alt-90=Z	Alt-137=E	Alt-0157=?	Alt-0232=E
Alt-51=3	Alt-91=[	Alt-138=E	Alt-0158=Z	Alt-0234=E
Alt-52=4	Alt-92=\	Alt-139=I	Alt-0159=Y	Alt-0235=E
Alt-53=5	Alt-93=]	Alt-140=I	Alt-0168="	Alt-0236=I
Alt-54=6	Alt-94=^	Alt-141=I	Alt-0169=C	Alt-0237=I
Alt-55=7	Alt-95=_	Alt-147=O	Alt-0173=-	Alt-0238=I
Alt-56=8	Alt-96=`	Alt-149=O	Alt-0174=R	Alt-0239=I
Alt-57=9	Alt-97=A	Alt-150=U	Alt-0175=_	Alt-0240=D
Alt-58=:	Alt-98=B	Alt-151=U	Alt-0179=3	Alt-0242=O
Alt-59=;	Alt-99=C	Alt-152=Y	Alt-0180='	Alt-0243=O
Alt-60=<	Alt-100=D	Alt-160=A	Alt-0184=,	Alt-0244=O
Alt-61==	Alt-101=E	Alt-161=I	Alt-0185=1	Alt-0245=O
Alt-62=>	Alt-102=F	Alt-162=O	Alt-0190=_	Alt-0248=O
Alt-63=?	Alt-103=G	Alt-163=U	Alt-0192=A	Alt-0249=U
Alt-64=@	Alt-104=H	Alt-0128=?	Alt-0193=A	Alt-0250=U
Alt-65=A	Alt-105=I	Alt-0129=?	Alt-0194=A	Alt-0251=U
Alt-66=B	Alt-106=J	Alt-0130=,	Alt-0195=A	Alt-0253=Y
Alt-67=C	Alt-107=K	Alt-0132=,	Alt-0200=E	Alt-0254=_
Alt-68=D	Alt-108=L	Alt-0133=.	Alt-0202=E	Alt-0255=Y
Alt-69=E	Alt-109=M	Alt-0134=+	Alt-0203=E	
Alt-70=F	Alt-110=N	Alt-0136=^	Alt-0204=I	
Alt-71=G	Alt-111=O	Alt-0137=%	Alt-0205=I	

Table 3 - ALT characters NOT cracked with L0phtCrack 2.5 (Crawford).

Alt-1=☺	Alt-135=ç	Alt-188=╝	Alt-226=Γ	Alt-0164=¤
Alt-2=☻	Alt-142=Ä	Alt-189=╜	Alt-227=π	Alt-0165=¥
Alt-3=♥	Alt-143=Å	Alt-190=╛	Alt-228=Σ	Alt-0166=¦
Alt-4=♦	Alt-144=É	Alt-191=┐	Alt-229=σ	Alt-0167=§
Alt-5=♣	Alt-145=æ	Alt-192=└	Alt-230=µ	Alt-0170=ª
Alt-6=♠	Alt-146=Æ	Alt-193=┴	Alt-231=τ	Alt-0171=«
Alt-7=•	Alt-148=ö	Alt-194=┬	Alt-232=Φ	Alt-0172=¬
Alt-8=◘	Alt-153=Ö	Alt-195=├	Alt-233=Θ	Alt-0176=°
Alt-9=○	Alt-154=Ü	Alt-196=─	Alt-234=Ω	Alt-0177=±
Alt-10=◙	Alt-155=¢	Alt-197=┼	Alt-235=δ	Alt-0178=²

Alt-11=♂	Alt-156=£	Alt-198=╞	Alt-236=∞	Alt-0181=µ
Alt-12=♀	Alt-157=¥	Alt-199=╟	Alt-237=φ	Alt-0182=¶
Alt-13=♪	Alt-158=₧	Alt-200=╚	Alt-238=ε	Alt-0183=·
Alt-14=♫	Alt-159=ƒ	Alt-201=╔	Alt-239=∩	Alt-0186=º
Alt-15=☼	Alt-164=ñ	Alt-202=╩	Alt-240=≡	Alt-0187=»
Alt-16=►	Alt-165=Ñ	Alt-203=╦	Alt-241=±	Alt-0188=¼
Alt-17=◄	Alt-166=ª	Alt-204=╠	Alt-242=≥	Alt-0189=½
Alt-18=↕	Alt-167=º	Alt-205=═	Alt-243=≤	Alt-0191=¿
Alt-19=!!	Alt-168=¿	Alt-206=╬	Alt-244=⌠	Alt-0196=Ä
Alt-20=¶	Alt-169=⌐	Alt-207=╧	Alt-245=⌡	Alt-0197=Å
Alt-21=§	Alt-170=¬	Alt-208=╨	Alt-246=÷	Alt-0198=Æ
Alt-22=▬	Alt-171=½	Alt-209=╤	Alt-247=≈	Alt-0199=Ç
Alt-23=↨	Alt-172=¼	Alt-210=╥	Alt-248=°	Alt-0201=É
Alt-24=↑	Alt-173=¡	Alt-211=╙	Alt-249=·	Alt-0209=Ñ
Alt-25=↓	Alt-174=«	Alt-212=╘	Alt-250=·	Alt-0214=Ö
Alt-26=→	Alt-175=»	Alt-213=╒	Alt-251=√	Alt-0220=Ü
Alt-27=←	Alt-176=░	Alt-214=╓	Alt-252=ⁿ	Alt-0223=ß
Alt-28=∟	Alt-177=▒	Alt-215=╫	Alt-253=²	Alt-0228=ä
Alt-29=↔	Alt-178=▓	Alt-216=╪	Alt-254=■	Alt-0229=å
Alt-30=▲	Alt-179=│	Alt-217=┘	Alt-255=B	Alt-0230=æ
Alt-31=▼	Alt-180=┤	Alt-218=┌	Alt-0127=	Alt-0231=ç
Alt-32=S	Alt-181=╡	Alt-219=█	Alt-0131=ƒ	Alt-0233=é
Alt-127=⌂	Alt-182=╢	Alt-220=▄	Alt-0135=‡	Alt-0241=ñ
Alt-128=Ç	Alt-183=╖	Alt-221=▌	Alt-0149=•	Alt-0246=ö
Alt-129=ü	Alt-184=╕	Alt-222=▐	Alt-0160=B	Alt-0247=÷
Alt-130=é	Alt-185=╣	Alt-223=▀	Alt-0161=¡	
Alt-132=ä	Alt-186=║	Alt-224=α	Alt-0162=¢	
Alt-134=å	Alt-187=╗	Alt-225=ß	Alt-0163=£	

Table 1 illustrates Table 2 and Table 3 overlaid with the highlighted cells indicating which of the 380 ALT-characters are "non-crackable" ALT-characters. Looking at the tables one will notice many underscores after the ALT-character. This can be confusing because these appear to be blank or an "_", but each of these ALT-characters corresponds with a symbol of some type. The table (Kleppinger) below demonstrates how these characters look.

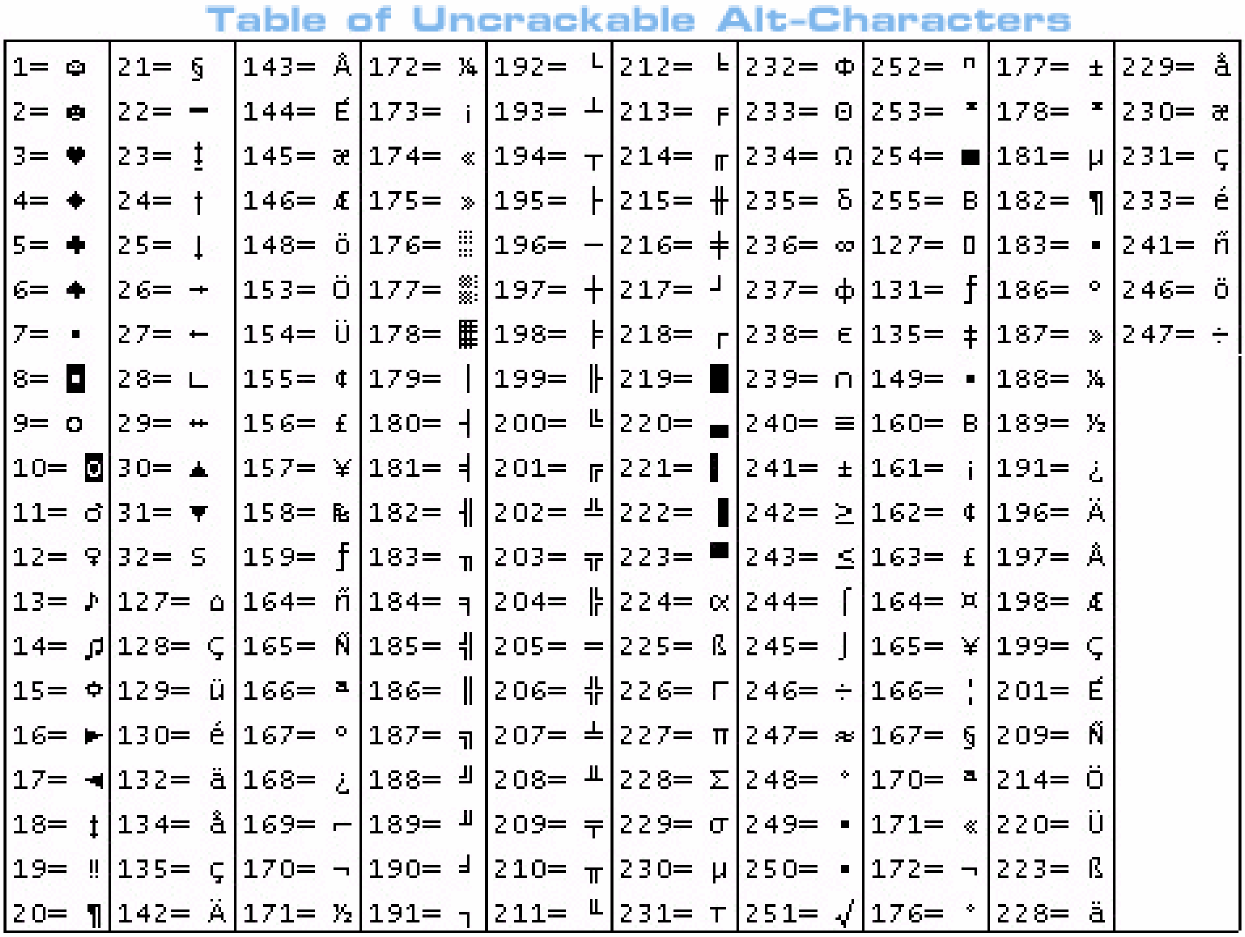


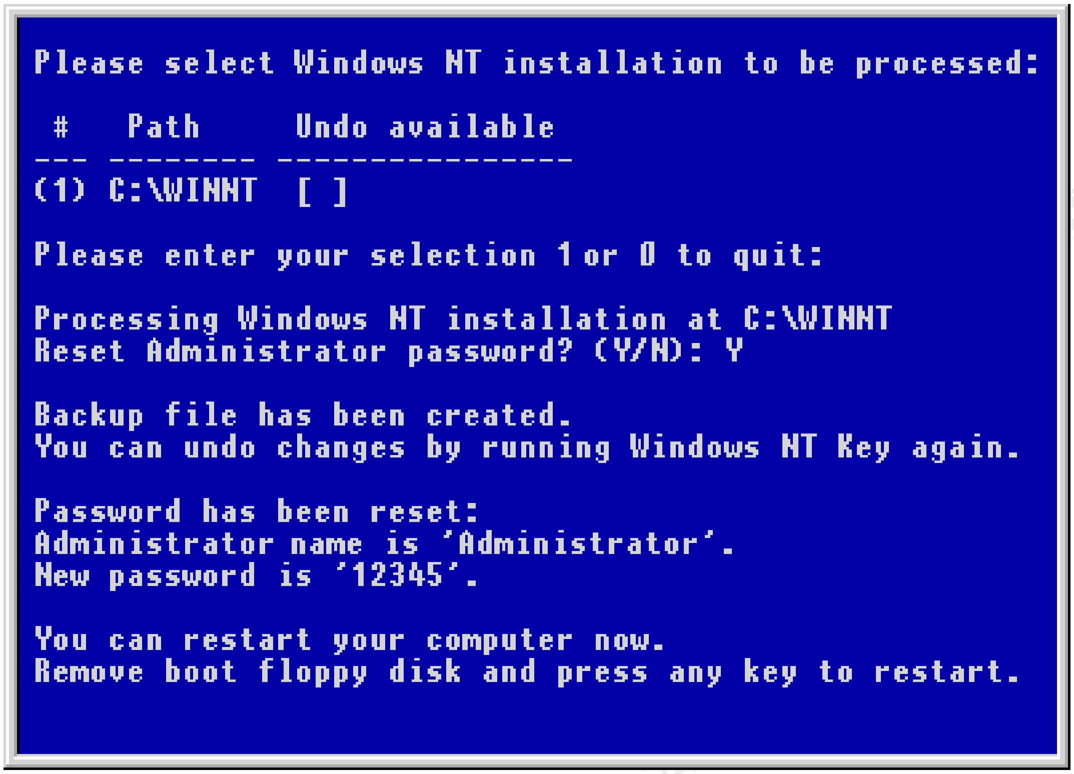
Table of Uncrackable Alt-Characters

1= ☺	21= §	143= Å	172= ¼	192= └	212= ╘	232= Φ	252= ⁿ	177= ±	229= å
2= ☻	22= ▬	144= É	173= ¡	193= ┴	213= ╒	233= Θ	253= ²	178= ²	230= æ
3= ♥	23= ↨	145= æ	174= «	194= ┬	214= ╓	234= Ω	254= ■	181= µ	231= ç
4= ♦	24= ↑	146= Æ	175= »	195= ├	215= ╫	235= δ	255= B	182= ¶	233= é
5= ♣	25= ↓	148= ö	176= ░	196= ─	216= ╪	236= ∞	127= ▯	183= ·	241= ñ
6= ♠	26= →	153= Ö	177= ▒	197= ┼	217= ┘	237= φ	131= ƒ	186= º	246= ö
7= •	27= ←	154= Ü	178= ▓	198= ╞	218= ┌	238= ε	135= ‡	187= »	247= ÷
8= ◘	28= ∟	155= ¢	179= │	199= ╟	219= █	239= ∩	149= •	188= ¼	
9= ○	29= ↔	156= £	180= ┤	200= ╚	220= ▄	240= ≡	160= B	189= ½	
10= ◙	30= ▲	157= ¥	181= ╡	201= ╔	221= ▌	241= ±	161= ¡	191= ¿	
11= ♂	31= ▼	158= ₧	182= ╢	202= ╩	222= ▐	242= ≥	162= ¢	196= Ä	
12= ♀	32= S	159= ƒ	183= ╖	203= ╦	223= ▀	243= ≤	163= £	197= Å	
13= ♪	127= ⌂	164= ñ	184= ╕	204= ╠	224= α	244= ⌠	164= ¤	198= Æ	
14= ♫	128= Ç	165= Ñ	185= ╣	205= ═	225= ß	245= ⌡	165= ¥	199= Ç	
15= ☼	129= ü	166= ª	186= ║	206= ╬	226= Γ	246= ÷	166= ¦	201= É	
16= ►	130= é	167= º	187= ╗	207= ╧	227= π	247= ≈	167= §	209= Ñ	
17= ◄	132= ä	168= ¿	188= ╝	208= ╨	228= Σ	248= °	170= ª	214= Ö	
18= ↕	134= å	169= ⌐	189= ╜	209= ╤	229= σ	249= ∙	171= «	220= Ü	
19= ‼	135= ç	170= ¬	190= ╛	210= ╥	230= µ	250= ·	172= ¬	223= ß	
20= ¶	142= Ä	171= ½	191= ┐	211= ╙	231= τ	251= √	176= °	228= ä	

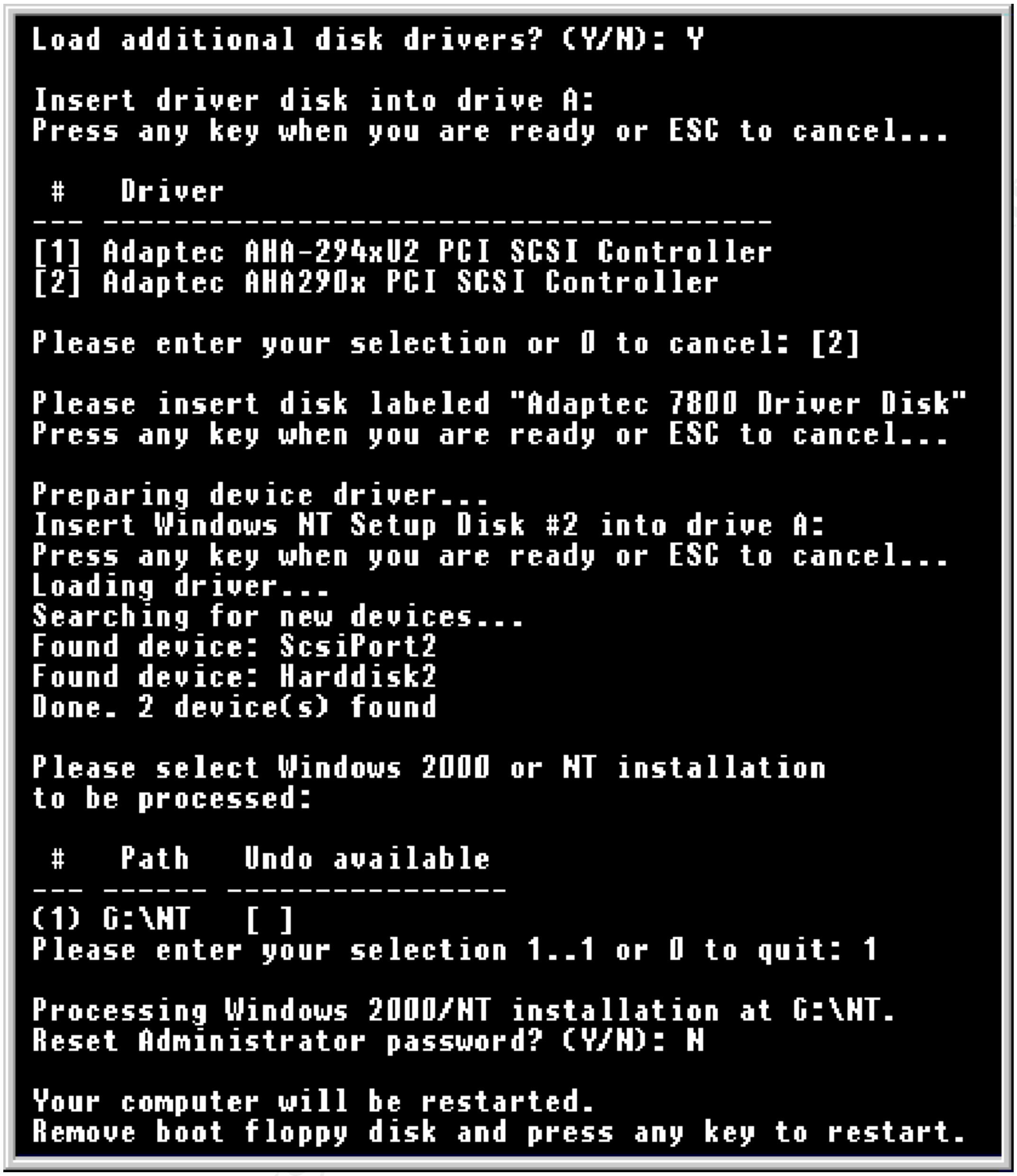
Physical Security

Word of caution, physically secure all domain controllers within your Windows 2000/NT domain. Even using the "non-crackable" password strategy, an unsecured domain controller lends itself to a vulnerability from Windows 2000/NT Key by Passware. This vulnerability allows an intruder who physically gets access to your servers to change the Administrator password, secure boot password or key disk password. This program will help you create the Windows Key boot disks that you will use to unlock your system.

The below screen shots illustrate how Windows 2000/NT key works:



```
Please select Windows NT installation to be processed:

 #   Path      Undo available
--- -------- ----------------
(1) C:\WINNT  [ ]

Please enter your selection 1 or 0 to quit:

Processing Windows NT installation at C:\WINNT
Reset Administrator password? (Y/N): Y

Backup file has been created.
You can undo changes by running Windows NT Key again.

Password has been reset:
Administrator name is 'Administrator'.
New password is '12345'.

You can restart your computer now.
Remove boot floppy disk and press any key to restart.
```



```
Load additional disk drivers? (Y/N): Y

Insert driver disk into drive A:
Press any key when you are ready or ESC to cancel...

 #   Driver
--- -------------------------------------
[1] Adaptec AHA-294xU2 PCI SCSI Controller
[2] Adaptec AHA290x PCI SCSI Controller

Please enter your selection or 0 to cancel: [2]

Please insert disk labeled "Adaptec 7800 Driver Disk"
Press any key when you are ready or ESC to cancel...

Preparing device driver...
Insert Windows NT Setup Disk #2 into drive A:
Press any key when you are ready or ESC to cancel...
Loading driver...
Searching for new devices...
Found device: ScsiPort2
Found device: Harddisk2
Done. 2 device(s) found

Please select Windows 2000 or NT installation
to be processed:

 #   Path   Undo available
--- ------ ---------------
(1) G:\NT   [ ]
Please enter your selection 1..1 or 0 to quit: 1

Processing Windows 2000/NT installation at G:\NT.
Reset Administrator password? (Y/N): N

Your computer will be restarted.
Remove boot floppy disk and press any key to restart.
```

If the hacker is gains Administrator control over your system, the hacker now owns your system and all the information contained therein.

Conclusion

First let me state for the record, all account/password testing was done using L0phtCrack 2.5. This is important since L0pht Heavy Industries' is preparing to introduce L0phtCrack 3.0. Although marketing calls L0phtCrack 3.0 the “best windows NT/2000 Password auditor” for administrators, it may also be the administrator’s worse nightmare. L0phtCrack 3.0 will feature a new wizard to assist “novice password auditors”. Password hashes will be retrievable from local machines, remote machines, NT 4.0 ERD, and by sniffing the network. The wizard offers four standard levels of password checking:

1. Quick Password Crack (LOW) – dictionary check plus minor variations
2. Strong Password Crack (MEDIUM) – dictionary check plus all alphanumeric combinations
3. Exhaustive Password Crack (HIGH) – all combinations of keys on the keyboard
4. Advance – for advance users who want to customize the password test

The HIGH and Advance options may be the troublesome if a hacker can enter the ALT-characters into a customized listing, or if the HIGH option will automatically scan for these keystroke combinations. Remember, Crawford's research demonstrated L0phtCrack 2.5 could not crack 187 ALT-characters even when the ALT-characters were known. Retesting the "non-crackable" password with L0phtCrack 3.0 is essential.

Administrators can take a major step forward in protecting user passwords from L0phtCrack and other such utilities by amending password policies to include the ALT-characters as part of the user's password. And if the password can be more secure using the ALT-characters, consideration to the length of user password needs to be addressed.

Recommendations:

- Use at least one ALT characters identified in Table 3 in all passwords
- Physically secure all servers that contain passwords or sensitive information
- Passwords should expire in 45 days
- Allow changes immediately
- Require passwords to include at least seven characters
- Remember the last 12 passwords
- Lock out passwords after three bad attempts
- Set the lockout duration to Forever
- Audit passwords routinely
- Disable unused accounts and audit monthly

By implementing the "non-crackable" ALT-character into each password, the length of the password becomes cloudy. Should the system force the user into a long password that is the user writes down and tapes to the monitor or keyboard, or should it be shorter, easier to remember? The shorter password removes the vulnerability of the user writing down the password. Also, implementing the "non-crackable" ALT-characters, passfilt, passprop, and SYSKEY are not essential to secure your system. However, to ensure passwords contain the "non-crackable" ALT-characters, passfilt.dll needs rewriting to include the 187 acceptable ALT-characters are included as part of the parameters of passfilt.dll.

Windows 2000 in mixed mode continues to make your system vulnerable to the NT security issues. Converting to the native mode for Windows 2000 will eliminate many of these vulnerabilities. Native mode also allows the implementation of Group Policies Objects and Templates that will enable the administrator to make changes on a global level.

As stated earlier – “Security requires simplicity.” Nothing is more simple that the inclusion of the “non-crackable” ALT-character in all passwords.

References

Bobby, J. (7/16/00). Password Cracking Using Focused Dictionaries. (2/2/01). [Available Online]. http://sans.org/infosecFAQ/authentic/cracking.htm

Chacon M. (10/97). Kerberos is on guard in Windows NT .0. (2/24/01) [Available Online]. http://www.win2000mag.com/Articles/Index.cfm?ArticleID=138

Crawford, Scott, Network Administrator. Evangel University.

Edwards M.J. & LeBlanc. (8/99). Where NT stores passwords: Guard your system against attacks. (2/6/01). [Available Online]. http://www.win2000mag.com/Articles/Index.cfm?ArticleID=5705

Kleppinger, J. (1/3/01). How to make windows 2000 and NT 4 passwords uncrackable. (1/5/01). [Available Online]. http://sysopt.earthweb.com/articles/win2kpass/index.html

L0pht Heavy Industries'. (2000). L0phtCrack. (1/8/01) [Available Online]. http://www.securitysoftwaretech.com/l0phtcrack

Microsoft Corporation. (2000). PassFilt.dll. 2/2/01 [Available Online]. http://msdn.microsoft.com/library/psdk/logauth/pswd_about_9x7w.htm

Microsoft Corporation. (1999). Enabling strong password functionality in Windows 2000. (2/25/01). [Available Online]. http://support.microsoft.com/support/kb/articles/Q225/2/30.ASP

Microsoft Corporation. Q161990 (2000). How to enable strong password functionality in Windows NT. 2/2/01. [Available Online]. http://support.microsoft.com/support/kb/articles/Q161/9/90.asp

Microsoft Corporation. (1/5/00) IT Introduction to Windows 2000 security. (2/27/01). [Availble Online]. http://www.microsoft.com/windows2000/guide/server/solutions/secintro.asp

Microsoft Corporation. (9/13/99). How to enforce strong passwords. (2/14/01). [Available Online]. http://www.microsoft.com/TechNet/lastpage/questions/990913.asp

Passware. (2001). Windows 2000/NT Key. (2/18/01). [Available Online]. http://www.lostpassword.com/windows-2000-nt.htm

Platinum Technology, Inc. (1998). Enforce strong passwords in NT 4.0. (2/2/01). [Available Online]. http://www.microsoft.com/TechNet/winnt/Winntas/Tips/platinum/ptespass.asp

Sabin, t. (2000). PWDump2. (2/24/01). [Available Online]. http://razor.bindview.com/tools/desc/pwdump2_readme.html

Smith, R.F. (7/6/00). Cracking user passwords in windows 2000. (1/8/01). [Available Online]. http://www.webspan.net/~tas/pwdump2/pwdump2.zip