

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Password and Network Logon Security in Windows NT 4.0.

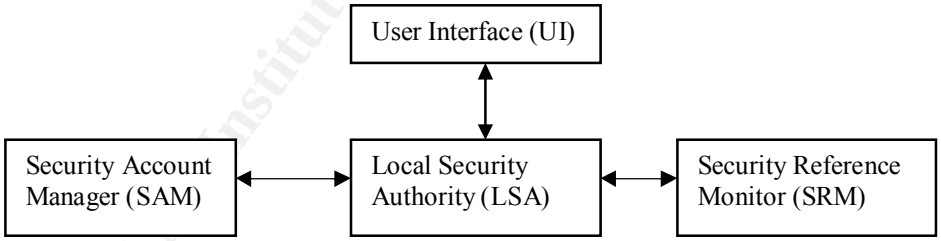
A brief overview of the Windows NT security model.

The Windows NT security model is designed such that every Windows NT object has its own security attributes which control user access to the object. These security attributes comprise of an access-control list, and object description data; this combination forms the Security Descriptor.

The access-control list (ACL) comprises two sections. First, the Discretionary Access-Control List (DACL) details which specific users and groups have what level of access to the object. Second, the System Access-Control List (SACL) details which system objects and services have access to the list.

The DACL contains an entry for each user and group registered in the system, the entries being called access-control entries (ACE). When an object is created by a user or Windows NT service, a security descriptor is always created. If the creator does not specify security attributes, Windows NT creates no access-control entries, which means no one has access to the object. This falls in line with Class C security in that "what is not explicitly permitted, is forbidden."

The main components in the Windows NT security model are as follows:



The Local Security Authority (LSA) is the core component of the NT security model, dealing with local security policy and user authentication. It is also responsible for generating and logging of security audit messages.

The Security Account Manager (SAM) manages the user and group accounts, and provides authentication services for the Local Security Authority.

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

The Security Reference Monitor (SRM) provides access validation and auditing for the Local Security Monitor. User access to files are passed or denied by the Security Reference Monitor, which also generates audit records where appropriate. Resources are protected uniformly throughout the system, regardless of resource type, using a copy of the access validation code held by the Security Reference Monitor.

The User Interface is the view seen by the end-user.

The above description shows how the Windows NT security system offers a very fine level of access-control for individual users and groups. Since user access rights can be extensively customized, a user may have access rights beyond the normal, and thus all users should be protected from loss of password integrity.

A review of the steps involved in a successful remote logon at a Windows NT Server.

1. The Domain and Username are sent in cleartext from the user's computer to the remote Windows NT server. The Password isn't sent, a challenge-response protocol is used to verify that the user supplied password is authentic. (Using NTLMv2, discussed later, modifies this step slightly)
2. The authenticating Windows NT server's Security Accounts Manager (SAM) compares the logon username and challenge-response with information in the user accounts database.
3. If access is authorized, the authenticating Windows NT server's Local Security Authority (LSA) constructs a security access token and passes it to the server process, which creates a user ID (UID) referencing the security access token. This token reflects both the user privileges and those of all groups that the user belongs to.
4. The User ID is then returned to the client computer for use in all subsequent requests to the server.

After the session has been created, the client computer sends requests marked with the user ID it received during session setup. The server provides access according to the security access token held in the server's internal tables, which was created in step 3.

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

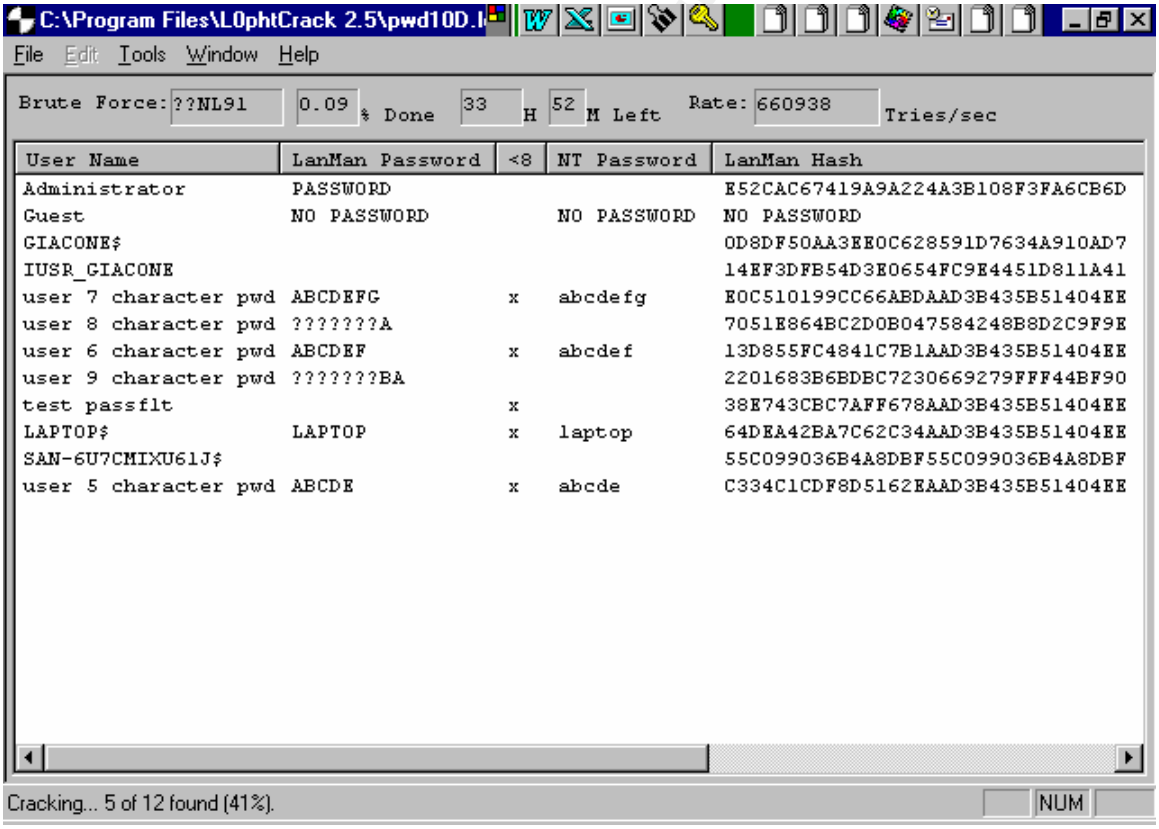
LAN Manager vs NT Passwords.

NT Server 4.0 and NT Workstation store both an NT and LAN Manager version of the password for user accounts. The LAN Manager passwords are not case sensitive.

The LAN Manager password hash has a somewhat simple creation mechanism as follows:

1) The password is converted to uppercase.
2) It is truncated to 14 characters, halved into 2 parts, each of which are padded and reversed.
3) The result is hashed with a "magic" number.

If the password is 7 or less characters, the last 7 characters of the LanMan Hash are the same, as shown in the following L0phtCrack session:

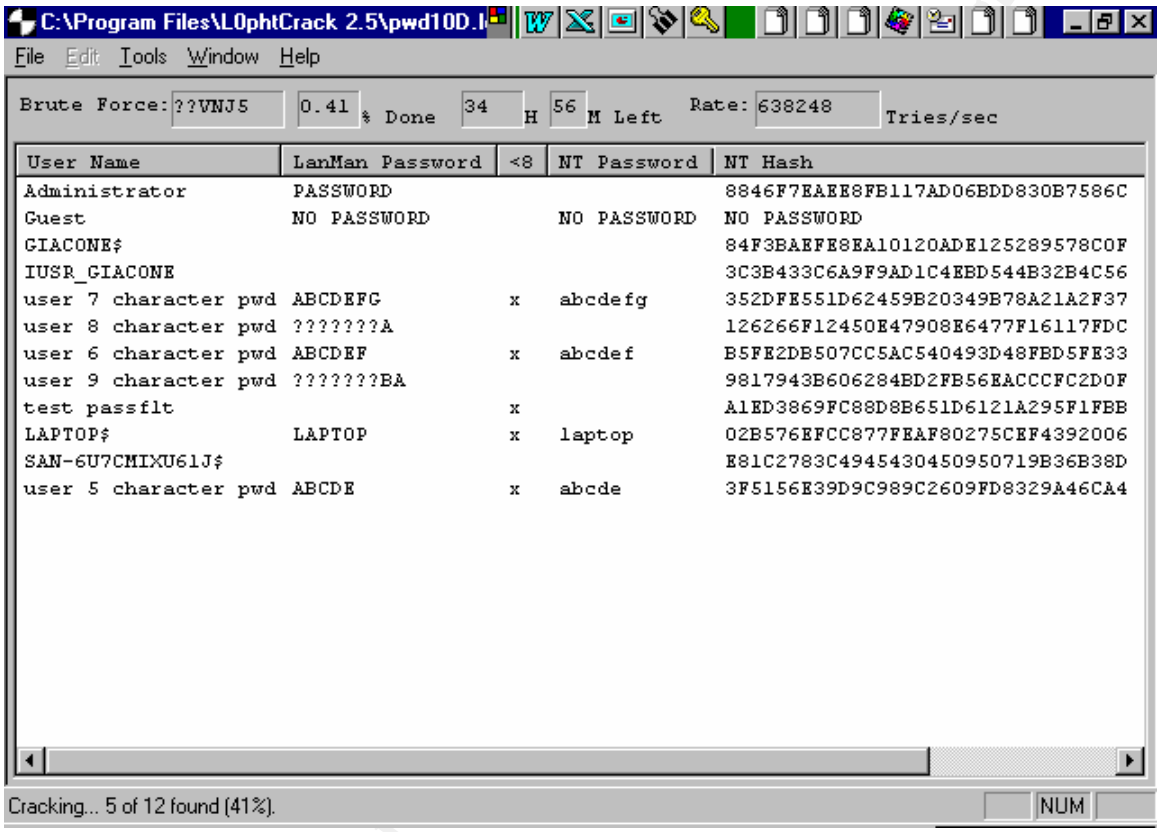


Note that Users "user 5 character pwd", "user 6 character pwd" and "user 7 character pwd" all have the last 16 bytes of the 32 byte hash the same AAD3B435B51404EE, as

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

does the machine LAPTOP$. This has enabled L0phCrack to correctly identify these accounts as ones having a password of 7 characters or fewer.

For comparison, here are the NT Hash passwords displayed:



The NT passwords are case sensitive, but can lose this attribute. If the client computer is not running NT, the password will be treated as non case sensitive. If a non-NT client computer issues the NET PASSWORD command to change the password, the resulting password becomes case insensitive for any client computer Windows operating system

The NT password is generated using the MD4 algorithm. In the default (NTLMv1) mode, it uses no "salt", thus identical passwords generate identical NT hashes. NTLMv2, available in Service Pack 4, can be enabled to avoid this condition (default is disabled). NTLMv2 also brings several other features that should be considered.

To enable NTLMv2 Authentication, the registry must be modified:

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

Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Control\Lsa
Value Name: LMCompatibilityLevel
Value Type: REG_DWORD
Value Data: 0 to 5

Values 0 through 3 apply to clients, Values 4 and 5 apply to domain controllers.

Value: Meaning:

0 This is the default if the value is undefined. The user's computer will authenticate exactly as it did under Service Pack 3 and earlier. The User's computer will send both LanManager and NT (MD4) responses to the domain controller. NTLMv2 will not be used.

1 The User's computer will attempt to negotiate the use of NTLMv2 with the domain controller. If unsuccessful, LM and NT (MD4) authentication will be used.

2 The user's computer will only use NT (MD4) authentication. LM and NTLMv2 authentication will not be used. Domain Controllers must be at Service Pack 4 or higher.

3 The user's computer will only use NTLMv2 authentication. Servers running Windows 9x, Windows For Workgroups, and Windows NT Service Pack 3 can still be accessed as long as the domain controllers have been upgraded to Service Pack 4 or higher, and the user-level security is in use (or share-level with blank passwords.) When clients are set to 4 or 5, the effective setting is 3.

4 This setting is used on domain controllers. When set, the domain controller will refuse LM authentication requests from clients, but will accept NT (MD4) and NTLMv2 clients. Thus, the client computers must be Windows NT.

5 This setting is used on domain controllers. When set, the domain controller will refuse both LM and NT (MD4) authentication request from clients, accepting only NTLMv2. Thus clients must be Windows NT with Service Pack 4 and NTLMv2 enabled in the registry.

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

It should be remembered that Windows 9x and earlier clients require LAN Manager authentication, thus limiting the scope of this feature. A suggested value of "REG_WORD=1" would allow Windows 9x and Windows for Workgroup clients to connect, and force appropriately configured Windows NT workstations and servers to use the enhanced security afforded by NTLMv2.

Hacker techniques in acquiring passwords.

There are three main techniques for acquiring passwords: manual, automated, and sniffing NT login exchanges right off the wire.

Manual password acquisition.

Manual password acquisition might be social engineering, guessing, or perhaps even threatening (though that may be considered a variety of social engineering!)

Social engineering includes asking directly or subversively for the username and password (or just the password if the username has already been acquired.) Many users are unaware of the risks of giving out their password(s), and a comprehensive approach to this problem is left to other resources discussing social engineering in detail.

Guessing is sometimes very rewarding – notice the preceding L0phCrack have correctly identified the Administrator password as PASSWORD – not very secure! Some low privilege role accounts may have no password while others use the company or department name, or even their pets' or spouse's first name (more social engineering!) Often, third party software have easy passwords, for example, a backup software package, with wide privileges, may have a password of BACKUP.

The most common target for guessing attacks is known local accounts on stand-alone NT servers or workstations. These tend to be more lax and reflect the culture of the individual system administrators and users, compared with the (hopefully) more stringent central IT organization.

Automated password guessing.

There are several widely available programs that automate password guessing. These include Legion and NetBIOS Auditing Tool (NAT). NAT is based on code from

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

Andrew Tridgell's SAMBA and is a command-line utility accepting a list of usernames, a list of passwords, and a range of IP addresses. Rhino9NAT is a graphical interface to the command-line utility, and has the same functionality. The program attempts to log onto the remote hosts, and connect to the host shares. The results are logged to a text file. Rhino9's Legion is very similar, but has a GUI interface and the ability to scan multiple Class C IP address ranges. Null passwords accounts can be enumerated using NTInfoScan (also known as Mnemonix) from David Litchfield.

The usernames can be targeted using NULL user sessions and NBTSTAT, while the IP addresses can be reconnoitered using NSLOOKUP, Tracert, Ping and Port scanning, NBTSTAT, Share scanning, and SNMP snooping, to name a few.

While the network provides one vector for automated password guessing, do not forget data on Emergency Repair Disks (ERD), or backup copies of the SAM. The ERD disks can contain the SAM, though it usually is too large to fit on a floppy and the SAM on the ERD is often the original installation copy with just the ADMINISTRATOR and GUEST accounts, whose passwords and account status have been appropriately secured. The backup copy of the SAM is placed in the %SystemRoot%\Repair folder whenever RDISK /S- is run. A hacker could attempt to run the RDISK /S- and then share the repair folder or relocate the backup SAM to a shared folder such as the \wwwroot folder. Another source of the SAM is backup tapes, which should be stored in a suitably secure location.

SAM encryption using SYSKEY

A solution to this vulnerability is to strongly encrypt the SAM. Service Pack 3 contains the SYSKEY utility, which generates a 128-bit random key to encrypt the password hashes in the SAM. This random key is then encrypted with another key, the System key, and stored in one of several location choices. When the system boots, this System Key must be available in order to decrypt the password hashes in the SAM, the system will not boot without it. The choices of location are:

1) Using a "complex obscuring function" to conceal the System Key on the computer. The convenience of having available for an unattended boot must

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

be weighed against the possibility that the "complex obscuring function" may someday be broken and the System Key penetrated by hackers.

2) The System Key can be stored on a floppy. This system will require the floppy to boot. Failure of the floppy or acquisition of it by a hacker could be a concern
3) The System Key can be generated using a MD5 method from a password up to 128 characters. This password must be typed in at boot time for the system to boot, so it must be securely protected against loss.

The SYSKEY process is one-way. Once the SAM has been SYSKEY'd, the only way to return to an unencrypted version is to restore from backup, with the subsequent loss of modifications to the SAM since the backup was created.

There is a danger of losing the System Key, and therefore the ability to reboot. The process can be used on selected systems that are more vulnerable to attack, leaving the SAM un-SYSKEY'd on some Domain Controllers, perhaps the Backup Domain Controllers. L0phtCrack, Quackenbush Password Appraiser, and other password decryption techniques cannot break the SYSKEY'd SAM at this time.

Two final notes:

1) Use the version dated after 12/99, since the previous version has reportedly been compromised!
2) SYSKEY has no effect on the PWDUMP2 tool, which reads directly from RAM, thereby using the hashes with the SYSKEY encryption backed out.

Sniffing for passwords.

A user logging into a remote Windows NT host typically sends their username and domain name across the network in cleartext, unless NTLMv2 is configured (see page 5 for details on NTLMv2). A challenge-response protocol is used to verify the password entered at the client; the password itself is not sent. If a packet sniffer can capture the complete authentication process, this challenge-response can be broken to reveal the encryption hash of the user's password. The encryption hash can then be broken using dictionary-based or brute force methods. L0phtCrack from L0pht Heavy

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

Industries can perform both the sniffing and the hash-breaking phases. A interesting note is that while by default L0phtCrack (version 2.4) tries appending two digits in its brute force attack, it doesn't check for leading numerals.

With the increase in switching used in networks, the opportunity to sniff is becoming significantly reduced.

A cautionary note:

Even without cracking the password, a skilled hacker could use a man-in-the-middle attack to modify or capture NetLogon channel packets. The Netlogon channel is a RPC channel used by Windows NT domain controllers to synchronize their user accounts database, for pass-through authentication of users, and the creation of trusts between domains. By default, only the password used to setup the channel is protected, leaving all subsequent data unencrypted and not checked for integrity. Windows NT Service Pack 4 introduced the ability to add encryption and integrity checking for the NetLogon channel. Using these options can add a 10% or higher CPU load to the host.

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Services\Netlogon\Parameters
Value Name:	- see below -
Value Type:	REG_DWORD
Value Data:	0 or 1

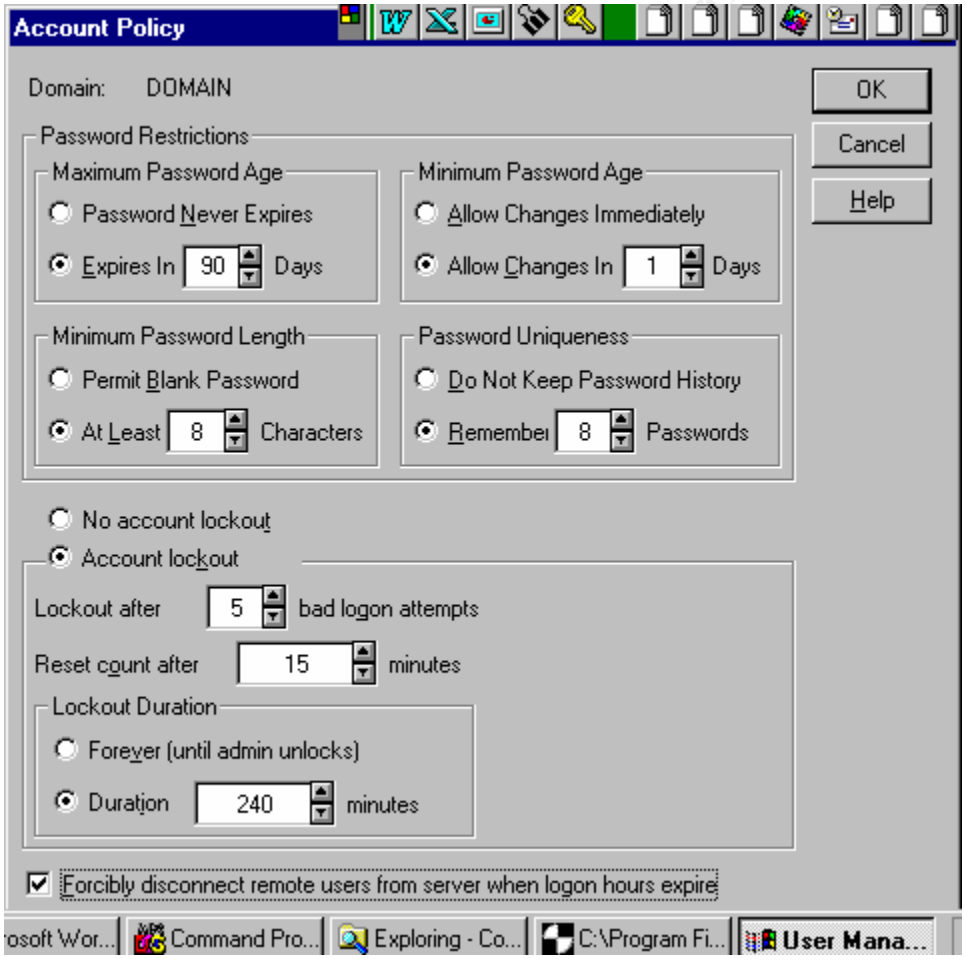
Value Name:	Effects:
SignSecureChannel	When set to 1, all outgoing NetLogon channel packets will be digitally signed for integrity checking.
SealSecureChannel	When set to 1, all outgoing NetLogon channel traffic will be encrypted. This option also forces digital signing.
RequiresSignOrSeal	When set to 1, all outgoing NetLogon channel traffic must at least be digitally signed, but may also be encrypted. These options will be negotiated. Should a remote system support neither option, the NetLogon connection to it will fail. Enable this value only if all

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

domain controllers have been upgraded to Service Pack 4. This includes domain controllers in trusted domains.

Securing passwords.

The first step in securing passwords is to review the account and password policies for all domain users in the User Manager utility of Windows NT. It is found under Policies – Account.



The following extract is from the SANS GIAC Windows NT Security workshop in May, 2000:

"Maximum Password Age determines how long a user can keep the same password. In a medium-security network, set this value to no more than 45 to 90 days.

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

Minimum Password Length determines how few characters a password may have. Valid numbers are 0 to 14. In a medium-security network, set this value to at least eight characters. The eight character limit is important due to the way Windows NT stores the so called LanManager hash of the user's password in the SAM database.

Password Uniqueness specifies the number of prior passwords (up to 24) domain controllers should "remember" for each user account. When a user changes his or her password, the new password is compared against the list of that user's prior passwords. If the domain controller can "remember" that the new password has been used before, the user is forced to choose a different password. This policy is important because users will recycle their favorite passwords. In a medium-security network, set this value to keep a history of 8 to 13 prior passwords.

The Minimum Password Age is used in conjunction with the Password Uniqueness policy. The purpose of the Minimum Password Age policy is to prevent users from cycling through enough passwords such that the domain controller will not "remember" their favorite password. Minimum Password Age compels a user to keep a new password for a period of time (up to 999 days). This prevents users from conveniently flushing out their password history list. In a medium-security network, set this value to 1 to 5 days.

Lockout after Bad Logon Attempts. After a specifiable number of failed logon attempts, an account can be locked out. A locked out account can only be re-enabled in User Manager by an administrator. In a medium-security network, enable account lockout after no more than five bad attempts, and perhaps as little as three.

Lockout Duration. When an account is locked out, it can either be locked out forever or for a specifiable number of minutes (up to 99999). If the account is locked out forever, users will have to contact an administrator and request that the account be re-enabled. In a medium-security network, set this value to 4 hours.

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

This will prevent a hacker from guessing a significant number of passwords in an evening, but still permit users to reacquire control of their accounts without burdening administrators. Moreover, a one-hour lockout will limit the Denial of Service attacks that aim at locking out all users.

Reset Counter. A domain controller will keep a counter of bad logon attempts for each account. This counter can be reset to zero after a specifiable number of minutes (1 to 99999). This is the maximum amount of time that can transpire between bad logons and still trigger account logout. For example, if accounts are locked out after five bad logon attempts, and a user has already tried four times, the user should wait until the counter of bad logons is reset to zero before trying again. If the user is a hacker, he will not know there is a lockout trigger and will quickly cause the account to lock. In a medium-security network, configure this option to reset the count of bad logon attempts to zero after fifteen minutes.

Remote User Disconnect. When a user on the LAN remains logged in after his or her logon hours restrictions, that user is not forcibly logged out. This is to prevent damage to application data. Because remote dial-in users represent a larger threat, there is an option to "Forcibly disconnect remote from server users when logon hours expire." Beware that this may cause the remote user to lose application data. In a medium-security network, this option should be enabled."

The above explanation and suggested settings are fairly complete, yet do not cover all potential problems. The Lockout mechanism relies upon a specifiable number of failed logon attempts occurring within a certain time frame. The Reset Counter setting allows a hacker to try one try less that the "Lockout After Bad Logon Attempts" value, pause for Reset Counter value time, and continue, cycling thus until his or her goal is achieved. The pause while hacking this account can be usefully filled with attacks on other accounts in the same manner. Undoubtedly, this feature is used by many sniff and brute force crack software methods. In order to utilize this feature, the hacker would need the appropriate values, some of which he or she can acquire with a null user session. A Utility called

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

NTUSER, available from www.pedestalsoftware.com, can enumerate most of the account and password policy.

D:\ ntsec> ntuser –s 127.0.0.1 policy

MIN PASSWORD LENGTH	0 characters
MAX PASSWORD AGE	42d 22h 47m 31s
MIN PASSWORD AGE	0d 0h 0m 0s
FORCE LOGOFF	False
PASSWORD HISTORY	1 changes
LOCKOUT DURATION	0d 0h 30m 0s
LOCKOUT RESET	0d 0h 30m 0s
LOCKOUT THRESHOLD	Disabled

(This is an example from SANS GIAC NT Security Workshop, May 2000)

The NTUSER is a powerful utility in the very useful NTSEC suite from Pedestal Software, though the "Lockout After Bad Logon Attempts" setting seems to be absent, and naming convention differs from that in the User Manager-Policies-Accounts interface.

Securing the Administrator account password.

By the very nature of the privileges afforded the Administrator account, it requires substantive password security. It alone is not locked out by bad logon attempts, even if the User Manager account policies have been set to do so. This can be resolved using the PASSPROP utility on Service Pack 3 or later. PASSPROP allows the account to be locked out if failed logons over the network generates a "Lockout After Bad Logon Attempts" condition. The Administrator will still be able to perform an interactive console logon, as long as he or she has "log on locally" rights.

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

PASSPROP is a command-line utility with the following qualifiers:

PASSPROP [/complex] [/simple] [/adminlockout] [/noadminlockout]

/complex	Force passwords to be complex, requiring passwords to be a mix of upper and lowercase letters and numbers or symbols.
/simple	Allow passwords to be simple.
/adminlockout	Allow the Administrator account to be locked out. The administrator can still log on interactively on domain controllers.
/noadminlockout	Don't allow the administrator account to be locked out.

Additional properties can be set using User Manager or the NET ACCOUNTS command.

Another consideration is to use extended ASCII characters in the password, for example, holding the Alt key and typing 145 (on the numeric keyboard), then releasing the Alt key will generate a non-standard character not used by default in password cracking software. It should be noted that some applications such as web-based ones cannot handle the extended characters and thus this approach may prove problematic. In addition, Windows 9x and Windows for Workgroup clients seem to have trouble with the extended ASCII.

Remove "Access This Computer Over Network" right.

User Manager, under Policies – User Rights, allows the denial of the "Access This Computer Over Network" right. This can be used to prevent hackers attacking the Administrator account on the server. It may be an appropriate response on the more vulnerable servers, for example web servers. Obviously, the Administrator would have to log on locally to perform his or her duties – ensure that the "Log On Locally" right is given to them! An alternative is to leave the Administrator with the "Access This Computer Over Network" right, but user the User Manager – User Properties – Logon Workstations setting to limit the client to appropriate workstations.

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

Other options:

While there are ways of identifying the name of the Administrator account, it is a good idea to rename it as another way to mislead hackers. A honey-pot account can be created by copying the rename Administrator account (to get its description field), and naming the copy Administrator. Obviously, the bogus Administrator account should be stripped of any significant rights, permissions, and group memberships. More information about honey-pot accounts is available in other sources.

Administrative users should normally use a regular account for non-administrative functions, using their administrative account only if its rights are required.

Secure against weak passwords.

Users can be forced to use a minimum password length using the User Manager – Policies – Account settings. To force users to use complex passwords, the PASSFILT.DLL password filter first seen in Service Pack 3 can be enabled. With the Service Pack applied, the following settings need to be added to the registry:

HIVE:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Control\Lsa
Value Name:	NotificationPackages
Value Type:	REG_MULTI_SZ
Value Data:	PASSFILT

When a user changes their password across the network, the password filter enforces the following attributes:

1. The new password must be six or more characters long.
   (User Manager – Policies – Account can enforce a longer password)
2. The new password cannot contain any part of the user's full name
3. The new password must contain at least three out of the following four characters:
   - Uppercase letters.
   - Lowercase letters.
   - Numbers.
   - Non-alphanumeric symbols.

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

It is significant that passwords entered into User Manager – User Properties – Password do not get filtered, and so Administrators can inadvertently still create user passwords that are weak.

Conclusion.

The default security for password and network logon in Windows NT 4.0 can be significantly enhanced. Many of these enhancements were made available with the release of Service Packs 3 and 4.

One remaining significant concern is the social engineering aspect. Encryption and other techniques work only if the user is educated about the need for security. The implementation of complex passwords, password expiration limits, and such, require willingness from the user. Perhaps even more pertinent, realization of appropriate security requires the buy-in and strong support from management.

- End -

References:

Windows NT 4.0 Server Security Guide
Marcus Goncalves
Prentice Hall
ISBN 0-13-679903-5

Windows NT Resource Kit for Windows NT Server version 4.0
Microsoft Press
ISBN 1-57231-344-7

Hacking Exposed – Network Security Secrets & Solutions
Stuart McClure, Joel Scambray, & George Kurtz
Osborne / McGraw-Hill
ISBN 0-07-212127-0

Hacker Proof – The Ultimate Guide to Network Security
Lars Klander
Jamsa Press
ISBN 1-884133-55-X

SANS GIAC Windows NT Security Workbook (May,2000) Version 3.5

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

Jason Fossen & Jesper Johansson
Sans Institute

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

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