# Securing Legacy Clients in a Windows Environment Transitioning to Windows 2000 Active Directory

## By

## Paul W. Rondorf

## Table of Contents

## Abstract

Microsoft programs backward compatibility into each new version of their desktop or network operating system. This backward compatibility supports the large number of Windows 9x and Windows NT4 still functioning on countless networks around the world. These “legacy systems” need to be able to function in either a Windows NT4 domain or a new Windows 2000 Active Directory domain. This compatibility and functionality come at the price of security on these legacy systems. Windows 9x uses LanManager (LM) authentication while Windows NT 4 uses NT LanManager version 1 (NTLMv1) and LM for authentication. LM is very easily cracked. NTLMv1 is not much more secure since L0phtCrack can easily crack it. Microsoft recognized this security problem by implementing NT LanManager version 2 (NTLMv2) which first made its appearance with the release of Service Pack 4 of Windows NT4. NTLMv2 is much more secure than either LM or NTLMv1. Windows 9x requires the installation of Internet Explorer 4x to use 128-bit encryption, the installation of Active Directory Client Extensions (ADCE), and modification of the Registry in order to use NTLMv2. Windows NT4 computers require the installtion of at least Service Pack 4 and modification of the Registry in order to use NTLMv2. The cost of such an endeavor is measured in terms of time and effort of system administrators and other support personnel. The pay off comes when you have all legacy clients and servers using NTLMv2 to securely authenticate across the network. I feel it is hard work, but well worth the price.

## Securing Legacy Clients in a Windows Environment Transitioning to Windows 2000 Active Directory

Paul W. Rondorf
GSEC, v1.4b
15 January 2003

## Introduction

Microsoft develops desktop and network operating systems with backward compatibility in mind. Legacy operating systems like Windows 9x and Windows NT 4 are still able to operate with the newer operating system, Windows 2000. This conscious decision by Microsoft is great for all types of organizations since they can replace older PCs and servers as their fiscal resources allow while squeezing a little more use out of the remaining, old PCs running Windows 9x or Windows NT4. These organizations save money at the expense of security since the legacy Windows systems don't have the robust security features provided by Windows 2000. However, steps can be taken to improve the security of these legacy Windows systems while still operating in Windows NT4 domains. These security-related steps include improving the authentication practices of legacy Windows systems, securing network communications, and improving basic systems security. Such actions will carry over when organizations' networks migrate to Windows 2000 Active Directory.

## Improving Client/Server Authentication

The primary authentication protocol in a Windows 2000 Active Directory domain is the three headed dog, Kerberos. However, Windows 2000 still supports the LAN Manager Authentication protocols: LAN Manager (LM), NT LAN Manager v1 (NTLMv1), and NT LAN Manager v2 (NTLMv2) for backward compatibility with legacy Windows 9x and Windows NT4 systems. Legacy clients use these authentication protocols whether they log into a Windows NT4 domain or a Windows 2000 Active Directory domain. The following chart details default authentication methods:

| Client | Domain Controller | Authentication Method |
|---|---|---|
| Windows 2000 | Windows 2000 | Kerberos (NTLM if Kerberos fails) |
| Windows 2000 | Windows NT 4.0 | NTLM |
| Windows 9x | Windows NT 4.0 | LM |
| Windows 9x | Windows 2000 | LM |
| Windows 9x w/Active Directory Client Extensions (ADCE) | Windows 2000 | LM (Configurable to use NTLMv1 or NTLMv2) |
| Windows NT 4.0 | Windows NT 4.0 | NTLMv1 (Configurable to use NTLMv2) |
| Windows NT 4.0 | Windows 2000 | NTLMv1 (Configurable to use NTLMv2) |

It is important to note that a client's password is not sent across then network during the authentication process. Instead, the operating system hashes the user's password which is used as an encryption key to encrypt a random challenge sent to the client from the server. The server encrypts the challenge with the user's password hash from the Security Account Manager (SAM) database. If there is a match between the result on the server and what the client provided, there is proof that the user knows the password.

**LanManager Authentication**

LM authentication evolves around the LM hash which is derived through the following steps:

1. The cleartext password is made 14 characters long by removing characters or padding the password with blanks (null characters).
2. All alphanumeric characters are changed to uppercase with numbers and symbols remaining unchanged.
3. The bits of each character byte are reversed.
4. The 14-byte string is divided up into two 7-byte pieces.
5. Each 7-byte string is used as an encryption key with the Digital Encryption Standard (DES) algorithm to encrypt a fixed string built into the operating system. The fixed string is the same on all Windows computers. It is 8 bytes in length.
6. The two results of encrypting the fixed string with the two DES keys are put back together to produce a 16-byte LanManager hash of the password.

The 16-byte LanManager (LM) hash is notoriously easy to crack for the following reasons:

- Passwords or password phrases longer than 14 characters are no stronger than a 14 character password since the 15th or greater characters are stripped away.
- The password draws no security from using both uppercase and lowercase letters since all alphanumeric characters are changed to uppercase.
- The effective length of the encryption key is reduced from 14 to 7 bytes when the 14-byte password is broken up into two 7-byte parts.
- Any password which is seven characters or less is extremely weak since the second 7-byte part of the password is padding which results in a DES key of nothing but null characters.
- The hash process has no random bytes since Windows uses a fixed string so identical passwords can have the same LanManager hashes. This fact makes it easy for a hacker to crack LanManager hashes using a pre-computed dictionary of LanManager hashes.

The 16-byte LanManager hash is padded with 5 bytes of zero (0) to produce the 21-byte session key when used during NTLMv1 challenge response authentication. This 21-byte session key is then divided up into three 7-byte pieces with each piece used as DES-CBC keys to encrypt the challenge. The three separate encrypted challenges are then put back together and returned to the domain controller as the client's response.

**NT LanManager v1 (NTLMv1) Authentication**

NTLMv1 authentication is derived through the following steps:

1. The password is made 14 characters long by removing characters or padding the password with blanks (null characters).
2. The 14-character string is converted to Unicode to preserve the case of the letters.
3. The 14-character Unicode character string is now hashed with MD4 to produce a 16-byte NT hash of the password.

The NT hash is much stronger than the LM hash because all 14 characters are used and case-sensitivity of the characters is preserved.

The NTLMv1 hash has several security related vulnerabilities. The NTLMv1 hash process still suffers from the lack of random characters added to the NT hash. Use of a fixed string during the NT hash process results in identical NT passwords yielding identical NT hashes. Pre-computed dictionary attacks against the NT hash now become a problem now become a very real source of compromise. Also, both NT and LM hashes are sent in parallel as part of the NTLMv1 authentication process between the client and domain controller. A hacker sniffing the wire for packets wouldn't even have to go after the NT hash if the much weaker LM hash is also readily available.

The NTLMv1 challenge/response authentication process pads the NT hash with 0's to create the 21-byte session key used to encrypt the challenge using DES. It is still harder to compute the NT hash from the server's challenge and the client's response than the accompanying LM hash at this point.

**NT LanManager v2 (NTLMv2) Authentication**

NTLMv2 authentication is much stronger than either LM or NTLMv1 authentication. Details of this authentication method follow:

- NTLMv2 is compatible with 127-character passwords.
- The user's password is still confirmed using challenge/response.
- The LM hash of the user's password plays no part in the NTLMv2 authentication.
- The client inputs a random string to the challenge, commonly called a salt, to prevent Pre-computed dictionary attacks. The client's response is different with every session with the same user password because of this random string.
- MD5 is used with the random string to prevent reverse engineering of the process to get the raw password hash.
- A timestamp is used to ensure timeliness of the response.
- A client challenge is sent to the server to ensure the server actually possesses the client's password. This check by the client isn't performed with NTLMv1.

- The best way to compromise this means of authentication is through a dictionary/brute force search of all possible passwords. Such a means of attack is impractical if long password phrases (passphrases) are used.
- A man-in-the-middle (MITM) isn't feasible because of the client challenge to the server.
- A replay attack is also a bust since the server's challenge is different every time.
- Downgrade attacks, downgrading authentication to either LM or NTLMv1, can be stopped by changing registry values on the client or server to require NTLMv2.
- NTLMv2 authentication isn't compromised by L0phtcrack because this password cracking tool can't extract the password hash.

Computation of the client's response to an NTLMv2 challenge from the domain controller uses the following equation:

Client Response = HMAC-MD5(K, server's challenge + M) + M

K = HMAC-MD5(MD4(password), username + domain)
M = ResponseType + HiResponseType + time + client's challenge to server + servername + server's domain

HMAC-MD5 produces a hash that requires a key (K) to compute the hash. The time and a random challenge to the server create the salt. The MD4(password) is treated as the HMAC when computing K. Also, notice that this process includes a timestamp. It is imperative that the date and time on the client and server be synchronized within 30 minutes in order for NTLMv2 to work. You can use the NET TIME command to automatically synchronize the clocks of the client and server.

It is obvious at this point that the goal must be to implement NTLMv2 authentication because of the additional security it provides. Windows 9x clients run into a couple problems at this point. These clients can't have a computer account in Active Directory (AD). User accounts in AD for individuals using the Windows 9x systems isn't a problem. However, password changes to these user accounts must go to the Windows 2000 domain controller serving as the Primary Domain Controller (PDC) Emulator. The PDC Emulator acts like the Windows NT PDC to the Windows 9x clients. It is one of the five Flexible Single Master of Operation (FSMO) roles within a Windows 2000 Active Directory forest/domain.

**Windows 9x Clients and Active Directory Client Extensions**

Windows 9x clients also run into trouble when they try to communicate with Active Directory (AD). AD is at the core of the Windows 2000 network operating system. All computer systems actively participating within a Windows 2000 AD domain must have the means to communicate with the AD. The Directory Service Agent (DSA) exists within the Local Security Authority of

Windows 2000. The DSA is the conduit through which computer systems travel on their way to communicate with the AD. Windows 9x clients need a way to be able to communicate with the DSA.

The solution to this problem lies with the installation of Active Directory Client Extensions (ADCE) on Windows 9x computers. The ADCE installation file, dsclient.exe, is included on the Windows 2000 Server CD-ROM at \Clients\Win9x\dsclient.exe. I'd recommend downloading the latest version from Microsoft. The version downloaded from Microsoft is the 56-bit exportable version. It is a good idea to use the maximum encryption available, 128-bit, on all Windows 9x systems in the United States for maximum security. You must also ensure that the 128-bit version of Internet Explorer 4.x or later is installed on the Windows 9x client(s) before you install ADCE.

Installing ADCE on Windows 9x clients loads the following files:

- Secur32.dll
- Msnp32.dll
- Vredir.vxd
- Vnetsup.vxd

ADCE adds the following features to each client:

- Windows 9x clients can now use the Light Weight Directory Access Protocol (LDAP) to search AD for all types of objects including users, shares, and printers.
- Support for the use of NTLMv2 authentication. It is interesting to note that the removal of the dsclient.exe installation will not remove NTLMv2 support. You can choose to install ADCE on Windows 9x clients while they still log into an NT4 domain for the NTLMv2 support.
- Windows 9x clients use the domain controller located closest to them on the network to log into the Windows 2000 domain.
- Active Directory Scripting Interface (ADSI) scripting to Active Directory is available. You should also install the latest version of Windows Scripting Host (WSH) as well.
- Access to Windows 2000 Distributed File System (Dfs) is now available. Dfs adds fault tolerant and load balancing file shares in Active Directory.

Installation of ADCE on Windows 9x computers does not provide the following:

- Kerberos support.
- Group Policy or Intellimirror support. These features come with implementation of Windows 2000 Active Directory.
- IPSEC or L2TP. IPSEC provides end-to-end encryption of virtual private network (VPN) connection between two VPN clients. L2TP is the tunneling protocol which supports the VPN.
- Service Principal Name – a computer account in Active Directory.

- Mutual Authentication. It is when the client and the server can identify each other during the authentication process.

### Configuration of NTLMv2 Authentication Levels

The LMCompatibilityLevel NTLMv2 has six configurable registry values for Windows 9x and Windows NT4 computers. The six possible settings and the results of each setting follow (Q239869):

| Level Number | Results of setting LMCompatibilityLevel for authentication. |
|---|---|
| 0 | Send LM and NTLM response; never use NTLM 2 session security. Clients use LM and NTLM authentication, and never use NTLM 2 session security; domain controllers accept LM, NTLM, and NTLM 2 authentication. |
| 1 | Use NTLM 2 session security if negotiated. Clients use LM and NTLM authentication, and use NTLM 2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLM 2 authentication. |
| 2 | Send NTLM response only. Clients use only NTLM authentication, and use NTLM 2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLM 2 authentication. |
| 3 | Send NTLM 2 response only. Clients use NTLM 2 authentication, and use NTLM 2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLM 2 authentication. |
| 4 | Domain controllers refuse LM responses. Clients use NTLM authentication, and use NTLM 2 session security if the server supports it; domain controllers refuse LM authentication (that is, they accept NTLM and NTLM 2). |
| 5 | Domain controllers refuse LM and NTLM responses (accept only NTLM 2). Clients use NTLM 2 authentication, use NTLM 2 session security if the server supports it; domain controllers refuse NTLM and LM authentication (they accept only NTLM 2). |

### Enabling NTLMv2 Authentication on Windows 9x Computers

Just installing ADCE is not enough. NTLMv2 must be activated on each Windows 9x client by configuring the LMCompatibilityLevel registry value. Maximum encryption is in place since 128-bit encryption was installed before installation of ADCE. The following steps are now taken to activate NTLMv2 on a Windows 9x client (Q239869):

1. Start Registry Editor (Regedit.exe).

2. Locate and click the following key in the registry:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control

3. Create an LSA registry key in the registry key listed above.

On the **Edit** menu, click **Add Value**, and then add the following registry value:

Value Name: LMCompatibility
Data Type: REG_DWORD
Value: 3
Valid Range: 0,3
Description: This parameter specifies the mode of authentication and session security to be used for network logons. It does not affect interactive logons.

It is a good idea to test all configuration changes in a lab environment before putting them into place in the production environment.

**Enabling NTLMv2 Authentication on Windows NT4 computers**

Windows NT4 client computers must have Service Pack 4 loaded in order to take advantage of NTLMv2. However, it is recommended that Service Pack 6a be installed since it fixes multi-domain issues with NTLMv2. NT4 administrators should also install ADCE on NT4 clients for Active Directory integration. NTLMv2 must also be activated on NT4 clients by making the following modification to the registry (Q239869):

1. Start Registry Editor (Regedit.exe).
2. Locate and click the following key in the registry:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

Value Name: LMCompatibilityLevel
Value Type: REG_DWORD
Value Data: 0 - 5

The value range of the LMCompatibilityLevel registry value comes from the chart on the previous page. It is a good idea to test all configuration changes in a lab environment before putting them into place in the production environment.

The same NT4 rules regarding the configuration of NTLMv2 also apply to all NT4 domain controllers to close the authentication loop.

**Requiring NTLMv2 Authentication on Windows 2000 Computers**

Implementing the required use of NTLMv2 on Windows 2000 computers is much easier. All you have to do is configure a Group Policy for both Windows 2000 domain controllers and regular systems. The procedure to change the policy on domain controllers follows:

1. Open the Domain Controller Security Policy console.
2. Define the Security Option policy by setting LAN Manager Authentication Level to:

    Send NTLMv2 Response Only\Refuse LM

It is a good idea to test all configuration changes in a lab environment before putting them into place in the production environment.

**Removing the LM Hash**

The network has evolved to the point where all Windows 9x and NT4 clients are configured to use NTLMv2 and the planned migration to Windows 2000 Active Directory is complete. A good security move should be to remove the LM hash from as much of the new AD domain as possible. This action provides two benefits:

1. Removing the LM hash from the AD or SAM removes the possibility of the LM hash being cracked if the AD or local SAM database is captured.
2. Helps to prevent the use of LanManager authentication protocol ever again.

Configuring a group Policy to take care of all Windows 2000 member servers and client workstations is easy to configure. However, there are a few issues to consider:

- Windows 9x computers with the ADCE installed will not be able to authenticate.
- Windows 9x clients won't be able to change their own passwords, even if they have ADCE installed. This issue may create a significant administrative burden if the network has a large number of Windows 9x computers.
- The LM hash isn't removed from a user's account until the next time a user changes his or her password.

It is also recommended that administrators install Service Pack 2 for Windows 2000 on Windows 2000 systems before removing the LM hash from AD or the local SAM database.

**Security of Network Communications**

It is a good idea to take the full implementation of NTLMv2 one step further by increasing the strength of session security. The type of session security used in a client – server session is decided when the client requests one of the following:

- NTLMv2 session security.
- 128-bit or 56-bit encryption.

- Message confidentiality.
- Message integrity.

The server indicates in its response if it can support the request. An administrator can specify that a server support only a certain type of session security. However, this configuration maybe risky since the server won't support a client request if it can't provide the type of session security requested. This risk goes away if strict configuration management standards are enforced on all client and server systems.

Windows 9x and Windows NT4 clients support the following two types of session security:

- NTLMv2 negotiated session security
- Server Message Block (SMB) signing

SMB signing secures file access, file creation, and file transfer between Windows 2000 servers and Windows 9x or Windows NT4 client computers. It provides mutual authentication and message integrity for these types of actions. Mutual authentication prevents man-in-the-middle attacks. Message integrity checks to ensure that packets have not been modified in any way. SMB will only be used if both sides of a connection have SMB enabled. SMB signing is enabled on Windows 9x and Windows NT4 SP3 systems by making two modifications to the Registry on each system. Modifications to the Registry of Windows 2000 system can be done through the use of a Group Policy. A drawback to the implementation of SMB signing is that the CPU's on all clients and servers take about a 15% performance hit.

NTLMv2 negotiated session security is not possible 100% of the time since not all network communications use NTLM. A program using Secure RPC is a good example of a program capable of using NTLM. Since it can use NTLM, it can be configured to require the use of NTLMv2. Windows 9x clients require the installation of ADCE in order to restrict session security. Windows NT4 systems require Service Pack 3 or later in order to restrict session security. The Registry of the Windows NT4 systems, using regedt32.exe, and of Windows 9x, using regedit.exe, must be modified as follows:

1. Locate the HKEY_LOCAL_MACHINE\System\CurrentControlSet \Control\LSA\MSV1_0.
2. Add the REG_WORD value NtlmMinClientSec.
3. Enter the value you require from the following table:

| Value | Required | Note |
|---|---|---|
| 0x00000010 | Message integrity | If message integrity isn't negotiated, the session fails. |
| 0x00000020 | Message confidentiality | If message integrity isn't negotiated, the session fails. |
| 0x00080000 | NTLMv2 session security | If NTLMv2 isn't negotiated, the session fails. |
| 0x20000000 | 128-bit encryption | If 128-bit encryption fails, the connection fails. |
| 0x80000000 | 56-bit encryption | If 56-bit encryption fails, the connection fails. |

## Conclusion

Network security can be enhanced by simply learning about all the possible security features of the various operating systems functioning on the network. Implementing NTLMv2 on Windows 9x and Windows NT4 computers can be quite a chore. It is not a job any system administrator should start until he or she has the following:

- Management's 100% support of the endeavor.
- The ability to have 100% visibility of all Windows 9x and Windows NT4 systems requiring configuration. It would be impossible to gauge the scope of the project without knowing the number of systems requiring modification.
- Scripts and/or batch files to automate the process on the Windows 9x and Windows NT4. Windows 2000 systems are taken care of using Group Policies.
- A good test lab where all configuration changes can be thoroughly tested.

Embarking on an NTLMv2 implementation plan also requires "buy in" from all organizations involved. The CEO or COO can provide invaluable assistance by making the initiative everyone's priority. The project will never get off the ground unless you have his/her support. Also, I would count on their support until you educate them as to the benefits of the project.

I feel that despite all the work involved, upgrading to NTLMv2 is a worthwhile adventure.

# References

How to Disable LM Authentication on Windows NT (Q147706)
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q147706&sd=tech

How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT (Q239869)
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q239869&sd=tech

Description of the Microsoft Windows Registry
http://support.microsoft.com/default.aspx?scid=kb;EN-US;256986

Ask Us About... Security, June 2000
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/askus/au052200.asp

Protect Your Passwords; Windows 2000 Magazine, Issue: October 1998, pg. 127, Author(s) : Randy Franklin Smith

How do I disable LanManager challenge/response in NT?; Windows NT/2000 FAQ, Web Exclusive, Dec 22, 1999, Author: John Savill

Windows 2000 Security Gains; Windows 2000 Magazine, Issue: Winter 1999, pg. 81, Author(s) : Randy Franklin Smith

Why NT Passwords Are Weak; Windows 2000 Magazine, Issue: Winter 2000, pg. 106, Author(s) : Randy Franklin Smith

NT Gatekeeper: LMCompatibilityLevel Settings and NTLMv2; Security Administrator, Issue: September 2001, pg. 11, Author(s): Jan De Clercq

Access Denied--Implementing NTLMv2 on Win2K, NT, and Win9x Machines; Security Administrator, Issue: December 2001
pg. 6, Author(s): Randy Franklin Smith

Q. How can I prevent the OS from storing LAN Manager (LM) hashes in Active Directory (AD) and the SAM?; Windows NT/2000 FAQ, Issue: Web Exclusive, October 8, 2001; Author(s): John Savill

Windows 2000 Security, Author: Roberta Bragg, Publisher: New Riders, 2001

Cannot Use Shares with LMCompatibilityLevel set to Only NTLM 2 Authentication (Q236414)
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B236414

HOW TO: Install the Active Directory Client Extension (Q288358)
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B288358

INFO: Advanced Installation of Directory Services Client for Windows NT 4.0 (Q295166)
http://support.microsoft.com/default.aspx?scid=kb;EN-US;295166

New Registry Key to Remove LM Hashes from Active Directory and Security Account Manager (Q299656)
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B299656

How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT (Q239869)
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B239869

HOW TO: Install the Active Directory Client Extension (Q288358)
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B288358

INFO: Advanced Installation of Directory Services Client for Windows NT 4.0 (Q295166)
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B295166