Global Information Assurance Certification Paper

How To Defend Against L0phtcrack v3 With Windows 2000 Group Policy Objects.

Stephen Pullum

29 November 2001

There are several levels of security that must be implemented in order to provide good network security for an organization. This paper is a how-to guide for defending against a exploit and vulnerability based on an environment in which a Windows 2000 domain running in native mode. The vulnerability is weak passwords and its exploiter is none other than L0phtcrack v3 by @Stake.

RFC 1244, the Site Security Handbook, attempts to address the need for security policies and procedures by stating, "Security threats are different today. The time honored advice says "don't write your password down and put it in your desk" lest someone find it. With world-wide Internet connections, someone could get into your system from the other side of the world and steal your password in the middle of the night when your building is locked up. Viruses and worms can be passed from machine to machine. The Internet allows the electronic equivalent of the thief who looks for open windows and doors; now a person can check hundreds of machines for vulnerabilities in a few hours." It is imperative that before any successful countermeasures can be deployed against software like L0phtcrack an assessment of organizational policies and procedures be conducted.

Sunbelt Software (www.sunbelt-software.com) provides a weekly newsletter called W2Knews. They performed a survey titled The Weak Security-Link: Passwords. This is an excerpt from that survey:

The question we asked was: "In your company, have you implemented for your users – (Percentages directly behind each option)

- Strong password policy, enforced by AD and Group Policy: 24.39%

- Strong password policy, implemented via the Resource Kit: 17.19%

- Written policy about password strength: 19.14%

- No written policy, no additional tools, rely on NT/W2K's password functionality: 37.31%

This means really that more than half of you, your users are very likely leaving your domains open to attack. After all the security measures taken to make your network impenetrable, that one liability could undermine your entire operation.

Simply put, passwords still are the weakest link that hackers prey upon and the most neglected security hole. Hackers often use "dictionary attacks" that compare common words from several wordlists to your users' passwords.

Further into this paper we will describe one of the most widely used dictionary attacking programs available, L0phtcrack v3.

You can subscribe to W2Knews by going to www.w2knews.com/subscribe.cfg?id=w2k

The Windows 2000 logon process is the starting point for password cracking. Understanding how Windows interacts with the user and their password is essential in beginning to crack the process. Windows 2000 attempts to use Kerberos as the primary source of user authentication requiring a Key Distribution Center (KDC) service running on a Windows 2000 server. If the KDC service is not found for Kerberos authentication, then Windows uses Windows NT LAN Manager (NTLM) or NTLM v2. KDC is a service that runs on all domain controllers and works with Active Directory and Kerberos security authentication services. With Kerberos authentication, a server does not need to go to a domain controller to authenticate a client/user. The server can authenticate the client by examining credentials presented by the client. Clients obtain credentials for a particular server once and reuse them throughout a network logon session.

Dr.K, in his book titled The Complete H@ckers Handbook describes the logon process in 9 fundamental steps. These 9 steps involves several elements of the Windows 2000 system before it allows access to the desktop, but it all starts with the userid and password given to the logon process. The 9 steps are as follows:

1. The user presses CTRL-ALT-DELETE to alert the system.
2. The user enters a userid and password
3. The Security Subsystem runs the authentication package.
4. The authentication package checks the local user account database and, if it isn't there, forwards the request to a remote server for validation.
5. Once the account is validated, SAM returns the user's security and group ID.
6. A logon session is created by the authentication package which passes both the logon session and the security IDs to the security subsystem.
7. If the security subsystem rejects the logon, the session is deleted, an error is flagged and a new logon process is started. If the logon is accepted, an access token is created containing the security IDs and returned to the logon process with a success flag.
8. The logon session then calls the Win32 subsystem to create a process and attach the access token to that process.
9. The Win32 subsystem will then start the desktop if an interactive session is required.

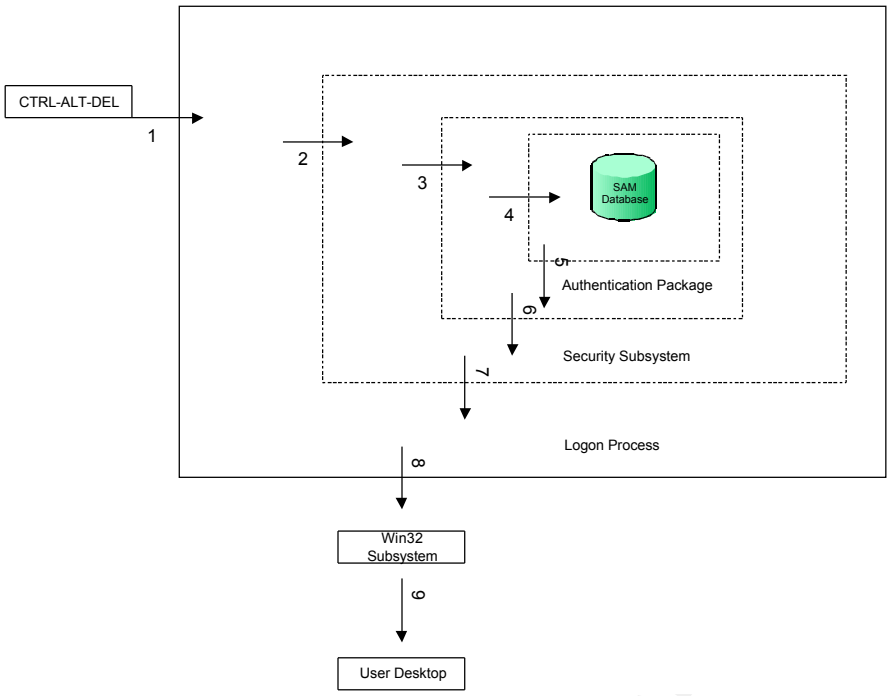

Figure III-1.

D. Narayanan of California Software Labs explains in his whitepaper titled Windows NT/2000 Security how the Windows logon process is executed.

> *Winlogon is the first process to run on a computer. The identification and authentication aspects of the winlogon are implemented as GINA (Graphical Identification and Authentication). The GINA process consists of the following steps for winlogon:*
>
> 1. *It creates a window station to represent keyboard, mouse and monitor.*
> 2. *It creates three desktops. An application desktop (used by the user), a winlogon desktop to display the login UI, and a screensaver desktop.*
> 3. *It registers a Secure Attention Sequence (SAS), a hot key sequence so that the keyboard hook handler is called whenever the SAS is entered.*
> 4. *Once the user enters the password, the winlogon sends the information to the Local Authority Server (LSA) which authenticates the password.*

More information about the GINA process can be obtained from from the California Software Laboratories. http://www.cswl.com/whiteppr/white/gina.html. More information about the local logon process for Windows 2000 can be obtained from the Microsoft KB Article Q231789 at http://support.microsoft.com.

Security Accounts Manager (SAM)

The SAM contains the usernames and encrypted passwords of all users on the local system, or the domain if the machine in question is a domain controller. In a Windows 2000 environment, Microsoft increased the functionality of the SAM by using a hashing algorithm left over from NT's LanManager roots. Although a newer NT-specific algorithm is available, the operating system must store the older LanMan hash along with the new to maintain compatibility with Windows 9x and Windows for Workgroups client. The biggest weakness in the SAM is the hashing methodologies of LanMan and NT hash. LM is separated into two seven-character halves. Cracking tools take advantage of this by simultaneously cracking both halves as if they were separate passwords.

The Administrators Best Friend/Enemy…….L0phtcrack v3.

L0phtcrack Version 3 is the only version of this program that runs cleanly on Windows 2000. It can extract unencrypted passwords hashes from systems that use Microsoft's SYSKEY protection, and it uses an updated packet sniffer that supports most Windows 2000 systems. It includes a 250,000 word English dictionary. This information was provided from L0phtcrack website. More indepth information can be obtained by visiting http://www.atstake.com/research/lc3/whatsnew.html. It is recommended that as an Administrator that you crack your networks passwords frequently to determine the strength of your admin and users passwords. Along with using L0phtcrack, in a Windows 2000 domain you will also have to use a program called PWDUMP3. Windows 2000, by default, enables SYSKEY. The following is an excerpt from the Pwdump3 product description found at http://www.ebiz-tech.com/html/pwdump.html. "Pwdump3 allows network administrators to retrieve hashes from a remote NT system. Administrators are no longer required to run the program directly on each machine. In addition, pwdump3 prints password hashes in upper case letters to ensure all hashes are interpreted correctly by L0pht Heavy Industries' L0phtcrack. Pwdump3 also correctly identifies accounts without passwords and allows administrators to enter a username if a connection to the remote machine does not exist, minimizing connection steps for the administrator." L0phtcrack in a W2K environment run against your hashed dump file will only reveal the Local Administrator and Guest accounts. The reason for this is Active Directory. W2K stores account information in Active Directory and, as a matter of fact, W2K doesn't even use the SAM on a W2K domain. The accounts you just extracted are the built-in accounts on the local machine. But don't forget about the backwards compatibility with NTLM for password hashes. One of the downfalls of L0phtcrack is that it can only crack 68 of the 256 possible characters in the ASCII character set. This enables the ability to create virtually "uncrackable" passwords.

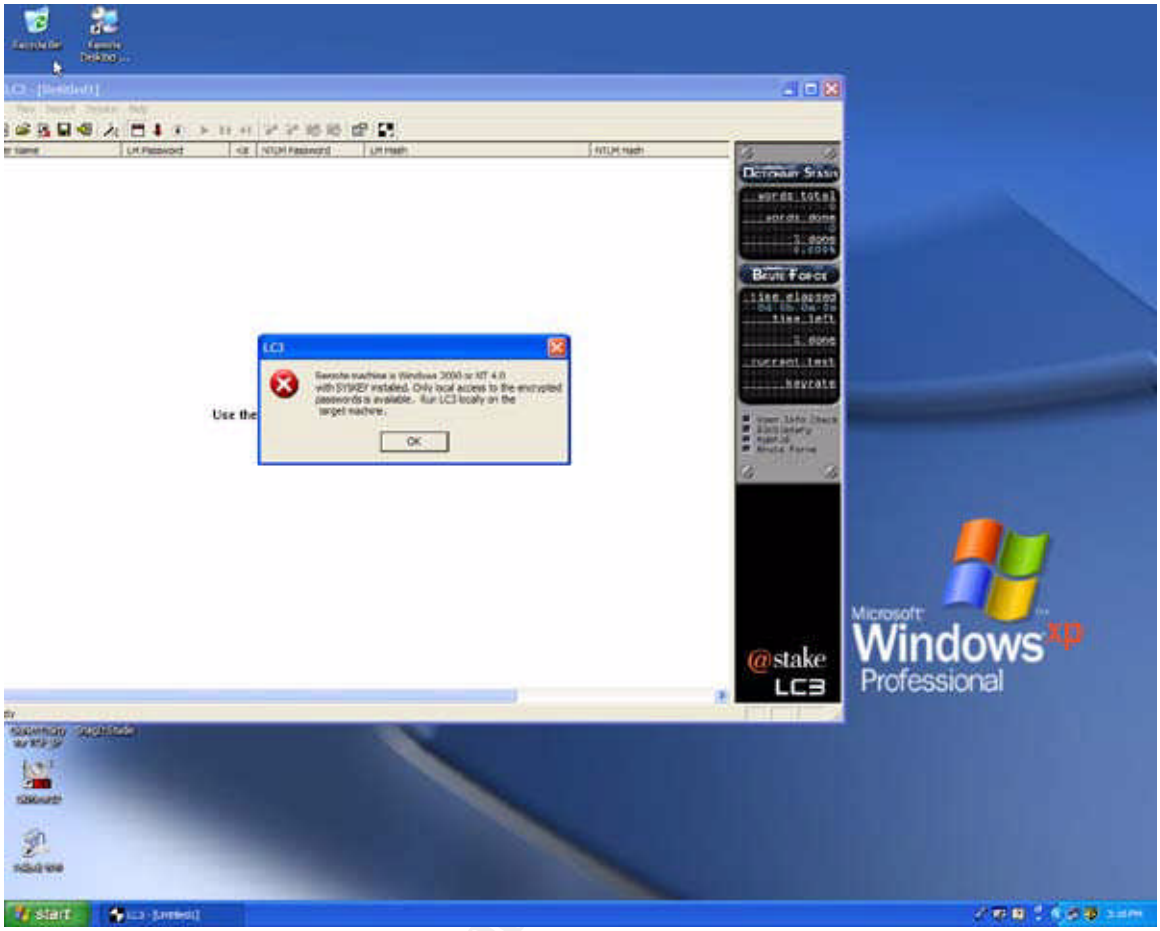

Figure V-1. Rejecting A Hash Not Obtained By A User With Admin Rights

There are some realities in this process. In order to effectively use pwdump3 against a W2K domain controller the user must have administrative rights or the request to extract the SAM will be rejected. An example can be seen in Figure V-1.

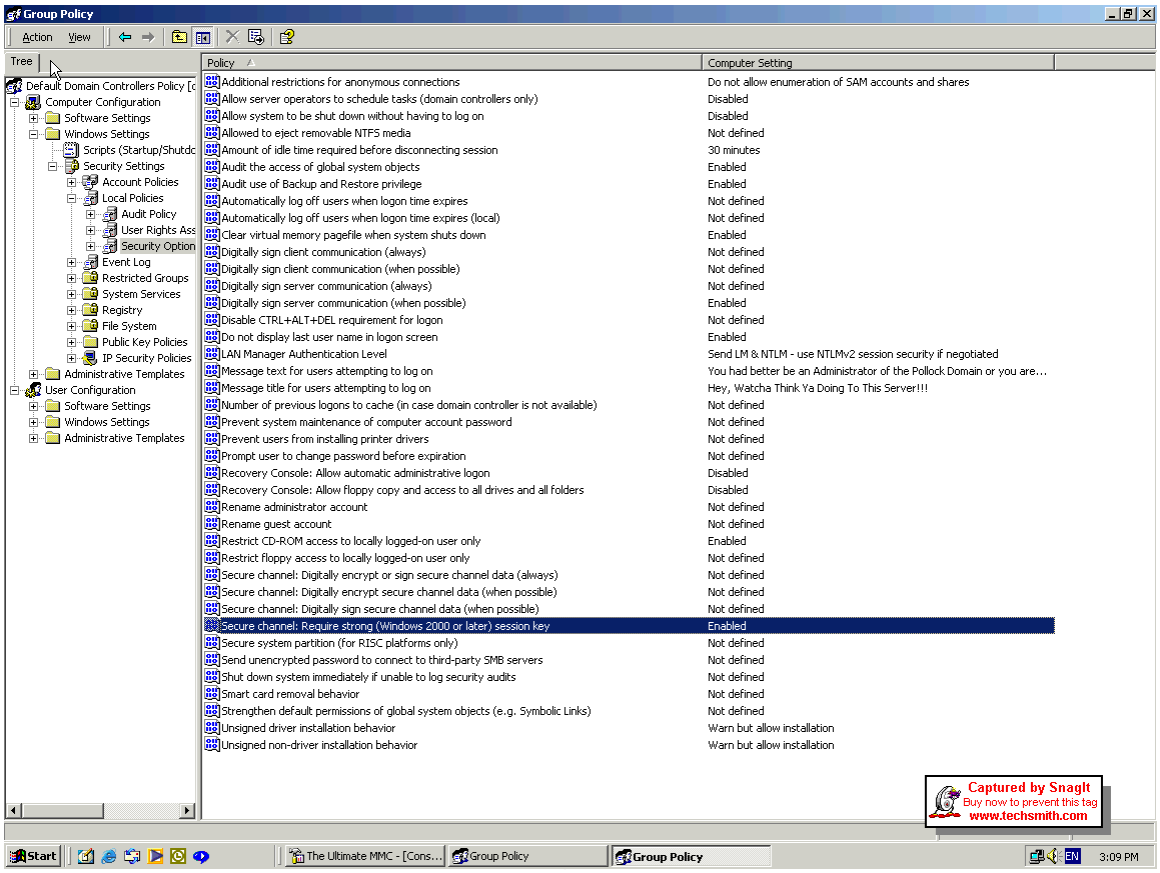

Figure VI-1. Setting NTLM Settings and Restricting Anonymous Connections In A GPO

There are several settings in your Microsoft Management Console (MMC) that you want set in your Default Domain Policy. The first of which is for Anonymous connections. Set "Do Not Allow Enumeration of SAM Accounts and Shares" and make it applicable for not only domain controllers but for all computers and laptops in the domain. The GPO will cache to the local machine. Furthermore, do not allow local user accounts on the local machine except Local Administrator and Guest. Users should log in with their domain accounts on and offline and this account should not have administrative access to the local machine. This allows you to control the user's abilities to perform functions locally as stipulated by the GPO for the Domain or a GPO generated for a particular OU or group.

The second setting set should be LAN Manager Authentication Level. Set "Send LM&NTLM – use NTLMv2 session security if negotiated". If you cannot get rid of NTLM out of your organization then this level will provide adequate security in a native Windows 2000 domain. For additional information on how to restrict Anonymous connections in Windows 2000 refer to the Microsoft KB Q246261.

Defensive Strategy II

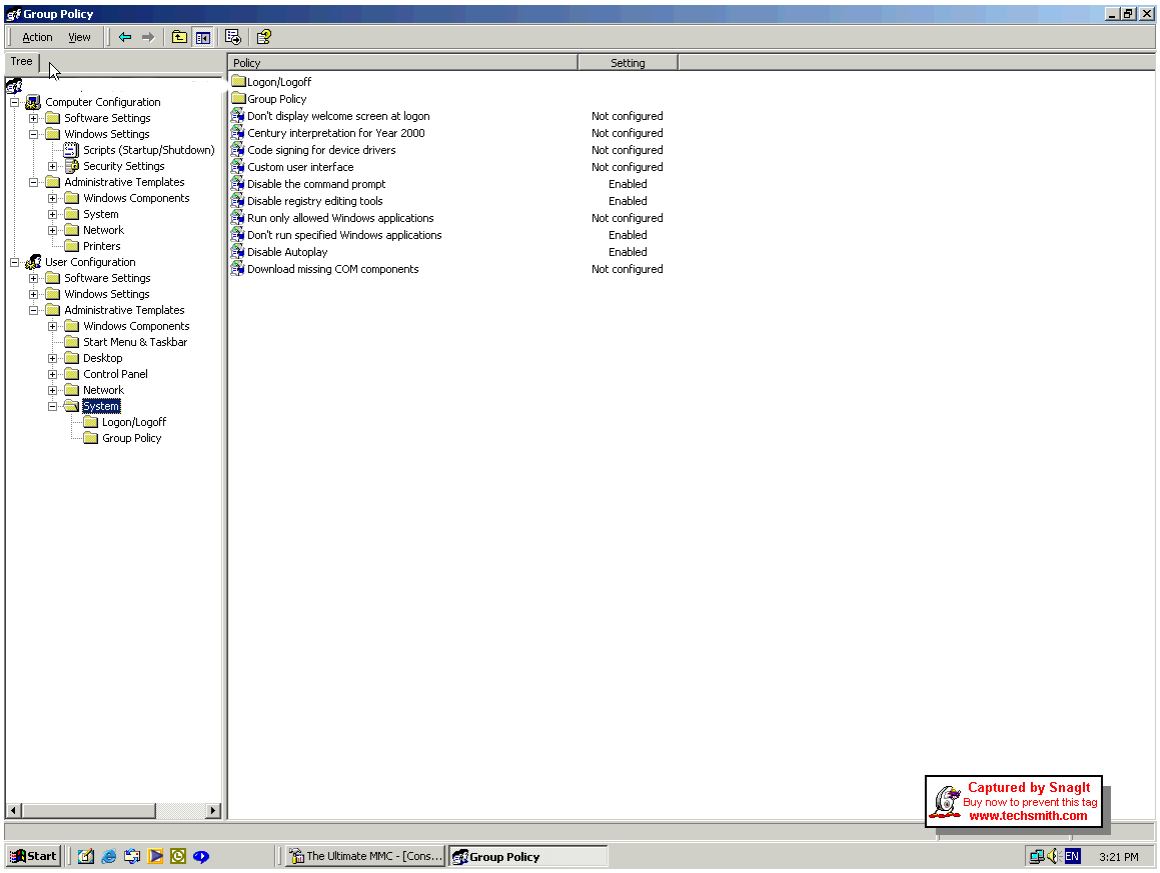

Figure VII-1. Disabling Registry Editing Tools and Command Prompt In A GPO

In your Microsoft Management Console (MMC) do not allow the registry editing tools to be enabled and if your corporate policy permits, do not even allow the run command. The environment that could be considered ideal is to not allow floppy drives or CD-ROM devices on local workstations. Exceptions should be closely monitored.

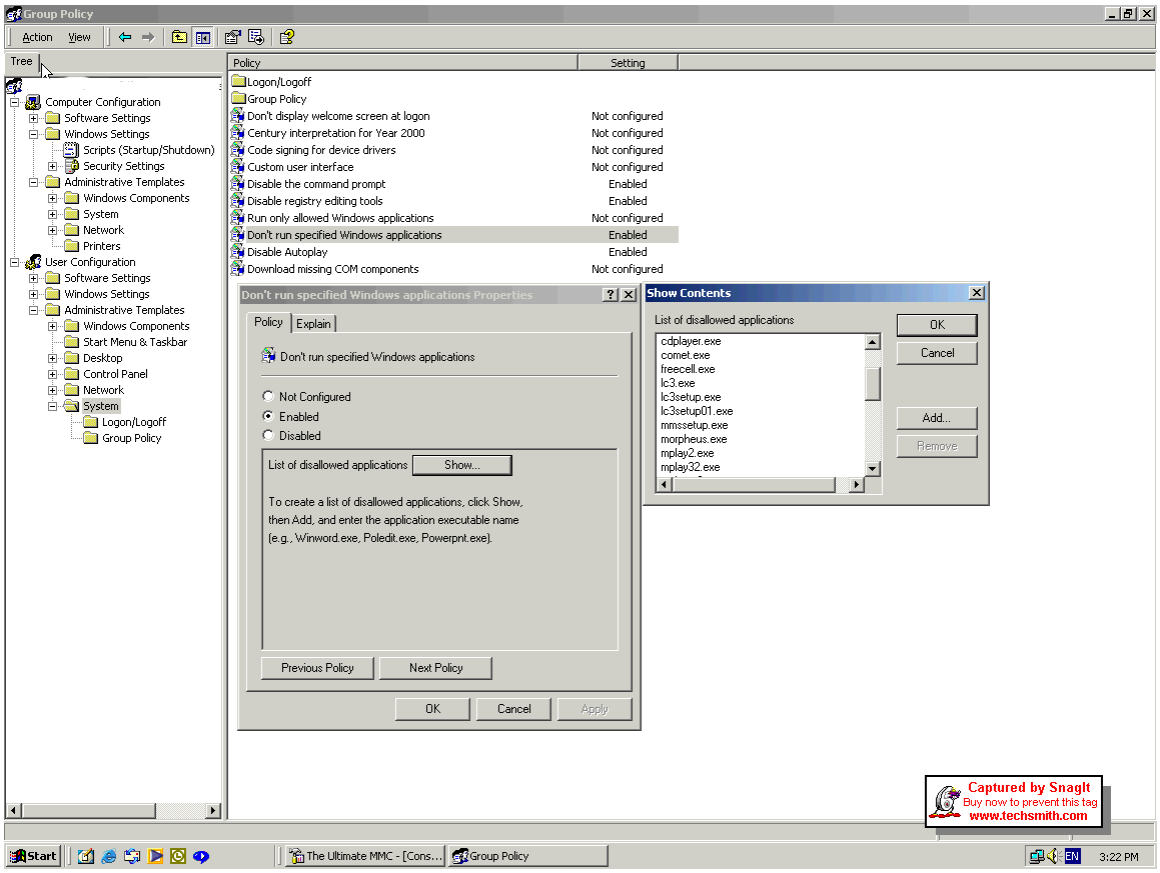

Figure VII-2. Disallowing Specific Applications In A GPO

Another good practice is to disallow the running or installation of L0phtcrack at the Domain level in the Group Policy Object. Disallowing the execution of lc3.exe, lc3setup.exe, and lc3setup01.exe initially proves to be effective. Making sure that you have enterprise auditing software like TrackIT from Blue Ocean Software or NetInventory by Bindview will notify of any unknown and known software in an organization just in case a user decides to rename the executable.

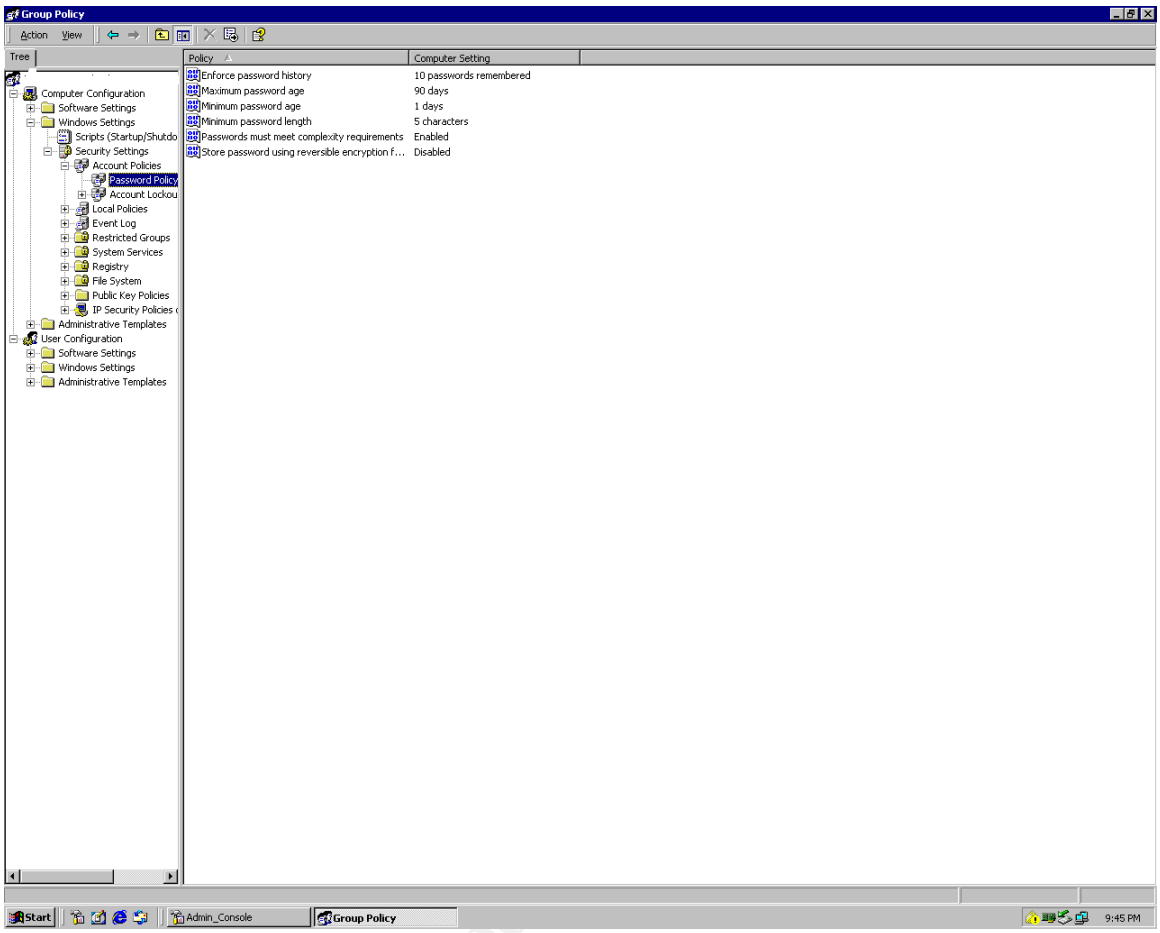

Figure VII-3. Password Settings in a GPO

Another GPO setting that should be utilized is the Password settings under Computer Configuration section. Enforcing password history and password age will also enhance the effectiveness of password security on a domain wide level.

The Administrator Account

Special attention needs to be paid to the Administrator account. The Windows 2000 Server Baseline Security Checklist located at the following URL, http://www.microsoft.com/technet/security/tools/w2ksvrcl.asp?frame=true, offers the following guidelines for establishing and maintaining the Administrator account.

> *"Windows 2000 allows passwords up to 127 characters. In general, longer passwords are stronger than shorter ones, and passwords with several character types (letters, numbers, punctuation marks, and nonprinting ASCII characters generated by using the ALT key and three-digit key codes on the numeric keypad) are stronger than alphabetic or alphanumeric-only passwords. For maximum protection, make sure the Administrator account password is at least nine characters long and that it includes at least one punctuation mark or nonprinting ASCII character in the first seven characters. In addition, the Administrator account password should not be synchronized across multiple servers. Different*

passwords should be used on each server to raise the level of security in the workgroup or domain."

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= £	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= °	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= £		
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		

L0phtcrack v3 is a tool that is utilized by hackers and administrators alike. L0phtcrack's capabilities and its effectiveness can enhance the security of your network if used correctly and with managerial approval. The flipside of this coin is if the program is introduced into your network maliciously it can cause embarrassment and damage. Gaining an understanding of the Windows 2000 logon process, Windows 2000 authentication methodologies, and the fundamental capabilities of L0phtcrack v3 is just as important as any other Defense in Depth concept. At the conclusion of the referenced Password survey by Sunbelt Software the author, Stu, concludes the following concerning password effectiveness:

> *Publishing a stricter written company policy does not prevent users from selecting those same vulnerable passwords. The native NT/W2K tools do not enforce effective enough restrictions on passwords to defeat these "dictionary attacks." Running a password hacking tool to identify the weak passwords still will not stop your users from falling back and using passwords that are "easy to remember." The only answer is to enforce an effective password policy when it counts, before the password is used.*

List of References and Sources:

Books:

Cole, Eric. SANS Security Essentials V: Windows Basics. SANS Security Boot camp 2001, San Diego, California

Dr-K,, A Complete H@ckers Handbook. Reading: Carlton Books. 2000 : 116-117

Scambray, Joel. HACKING EXPOSED SECOND EDITION. Reading: Osborne/McGraw-Hill. 2001 : 156-157

Internet:

@stake.com. "LC3: What's New." Nov 2001.
URL: http://www.atstake.com/research/lc3/whatsnew.html

Ebiz-tech.com. "Pwdump3 Product Description." Nov 2001.
URL: http://www.ebiz-tech.com/html/pwdump.html

Narayanan, D. "Windows NT/2000 Login Security – Whitepaper." 21 Mar 2001
URL: http://www.cswl.com/whiteppr/white/gina.html

Smith, Randy. "Cracking User Passwords in Windows 2000." 6 July 2000.
URL: http://ntsecurity.net/Articles/Index.cfm?ArticleID=9186

Kleppinger, Joel. "How to Make Windows 2000 and NT 4 Passwords Uncrackable." 3 Jan 2001. URL: http://sysopt.earthweb.com/articles/win2kpass/index2.html

Microsoft. "How to Use the RestrictAnonymous Registry Value in Windows 2000." 17 October 2001. URL: http://support.microsoft.com/support/kb/articles/Q246/2/61.asp

Microsoft. "Local Logon Process for Windows 2000." 1 Jan 2000.
URL: http://support.microsoft.com/support/kb/articles/q231/7/89.asp

Microsoft. "Windows 2000 Kerberos Authentication." 9 July 1999
URL: www.microsoft.com/windows2000/techinfo/howitworks/security/kerberos.asp

Microsoft. "Enabling Strong Password Functionality in Windows 2000." 1 Jan 2000
URL: http://support.microsoft.com/support/kb/articles/Q225/2/30.ASP

"The Weak Security-Link: Passwords." W2Knews Electronic Newsletter 19 Nov 2001. Vol. 6, #89 – Nov 19, 2001 – Issue #324 http://www.w2knews.com