

# White Paper: Massive Security Hole Ignored!

*Rev 1 - December 3, 2003*

Written by Philip Lieberman ([phil@lanicu.com](mailto:phil@lanicu.com))  
Lieberman Software Corporation  
<http://www.lanicu.com>

---

## **Abstract**

Even when administrators dutifully lockup their servers, apply patches, and use group policies to lock down workstation security, it only takes a few minutes for a hacker to unlock the keys to the kingdom (administrator accounts and passwords) with a quick search of the web. This paper will define this issue and offer possible solutions.

**Contents**

1. Introduction	3
2. Background	3
3. Distributed Administrative Credentials – the Hole that Cannot be Closed	3
4. Best Practices Workstations	4
5. Best Practices: Servers	4
6. Solution: Mass Management Tools—Save Money and Roll Your Own	4
7. Solution: Lieberman Software’s Mass Management Tools	6
8. Summary	7

## 1. Introduction

Most administrators dutifully lockup their servers, apply patches, and use group policies to lock down workstation security. Unfortunately, within just a few minutes any user can unlock the keys to the kingdom (administrator accounts and passwords) with a quick search of the web. This paper will define this issue and offer possible solutions.

## 2. Background



What would you say if I told you that I could break into all of your workstations (and probably your servers too) in a matter of minutes and there was nothing you could do about it? To make matters worse, I could accomplish this quickly and quietly without leaving a trace. How is this possible? Before revealing the details, let's review the basics of good security.

The most fundamental rule of security is that without physical security, there is no security. It is for that reason, most companies locate their servers in a secured location (the so called glass house where you can see the servers, but not touch them). Most companies go even further by incorporating software and hardware firewalls to block inappropriate traffic from attacking their servers from outside assaults.

The second rule of security is that servers and workstations must be kept up to date with patches. Out of date server software may contain security holes that can be exploited by hackers. So, for every exploit found, Microsoft has dutifully created patches and published best practices for how to protect your organization.

The third rule of security is that machines should be configured for the minimal level of functionality necessary to accomplish the job. This is accomplished quite nicely with Group Policies in Windows 2000 Active Directory. Group Policies allow for the configuration of workstation desktops, registry modifications, and access controls.

So, everything is locked down...or is it?

## 3. Distributed Administrative Credentials – the hole that cannot be closed



The problem that is rarely addressed is the existence of **distributed administrative credentials** stored in every machine on the network. If some or all of these credentials were to become known to an unauthorized user, they would have partial or complete administrative access to your entire domain.

Here is the list of credentials that can potentially become compromised:

- **Built-in administrator account on every machine** – Each machine has a local logon account that is created at the time the machine is built. The account and password is generally the same on every machine, so all that a hacker needs to do to become an administrator would be to crack the local administrator password. Cracking the local administrator common password can be done easily with tools such as L0phtCrack<sup>1</sup> and a boot floppy<sup>2</sup>. If all local machines and servers use the same built-in administrator account and password, once it has been compromised, an ordinary user will now have unfettered access to all systems.
- **Local Services that use Local or Domain Administrator account(s)** – Many machines use services that require either a local or domain administrator accounts. The bad news about services is that their account names and passwords are stored locally on every machine. Once a hacker has administrator access to a machine<sup>3</sup>, it is a simple matter to run a crack program such as LSADump2 to view the secrets area of a Windows NT or above system.
- **Scheduled Tasks located on a large group of systems that use local or domain credentials** – The Task Scheduler contained in every machine allows an administrator to schedule the periodic execution of program whether or not someone is logged on to the machine. The credentials for each task are stored locally on each machine. The administrator has a significant challenge if best practices specify that all domain administrator accounts must have a password change regularly. The reason for the challenge: it is tedious to change the account used by every task on every machine. Consequently, accounts used by Tasks are generally never changed.
- **MTS/COM+/DCOM components that use local or domain administrator accounts** - Microsoft's drive over the last 5 years to get developers to create n-tiered applications (also known as DNA or Digital Nervous System applications) has spawned a wide range of complex components that may use administrator account. Once the objects have been configured, the account information for the objects is stored uniquely on each machine. Determining which objects are using which accounts is virtually impossible due to the user interface provided and the vast number of mouse clicks/screens that must be viewed.

What this all means is simple: because of the nature of distributed credentials and the lack of any tools provided by Microsoft to manage this vast array of security information, most administrators choose to ignore the problem.

---

<sup>1</sup> L0phtCrack is now known as LC and is a commercial product available from @Stake ([www.atstake.com](http://www.atstake.com)).

<sup>2</sup> Using Winternals ([www.winternals.com](http://www.winternals.com)) NTFSDOS program a hacker can compromise the local operating system files so that the local password hashes are dumped at the time of the next system start.

<sup>3</sup> Gaining administrator access is much easier than cracking the password. There are numerous free and commercial utilities (see Locksmith from Winternals) that will reset the administrator password.

#### 4. Best Practices: Workstations

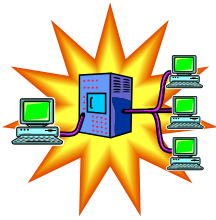
Since a curious user can easily and quietly penetrate the local security of their own machine and expose the stored credentials, there are many techniques to minimize the problem.



First, try to disable the introduction of hacking tools. With Group Policies in Windows 2000 you can attempt to disable registry editing tools and disable the running of hacking tools such as L0phtCrack. However, these policies are totally ineffective since the hacker can just boot to a diskette or CDROM and run their tools in DOS or in a second installation partition on the hard drive. You may consider removing or electrically disabling the floppy and CDROM drives. However, this can be compromised by the hacker opening the case and reconnecting the drives or by providing their own drives from home. The most insidious attack would be for the hacker to just make an image copy of the company hard drive and crack it at home at their leisure.

It seems that for every step an administrator takes to counter a hostile user from extracting sensitive information, there is a hacker workaround. This is completely true, so the only practical solution is to reduce the value of the information on each workstation. Reducing the value can be accomplished by making sure that all services, scheduled tasks, and COM+ type objects do not reference domain administrator accounts. Next, the local workstation administrator accounts must be changed on a regular basis. Even better, each machine should have its own unique password that is complex enough so that cracking it via L0phtCrack is not practical.

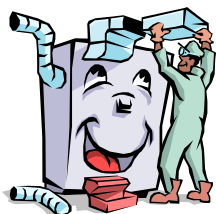
#### 5. Best Practices: Servers



When an administrator leaves the organization, they leave with the knowledge of all of the secret administrator accounts as well as the knowledge that the company that they left will be unable to change the credentials due to lack of tools. With a large organization there may be hundreds or thousands of servers with domain administrator accounts attached to services, scheduled tasks, COM+/DCOM/MTS objects, and local logon accounts. Any attempt to change domain administrator accounts will result in untold number of critical systems going off-line. Worse yet, if the account lockout policy is in effect, when some of the unchanged system objects continue to use the "old" password, the just changed account will be locked out and be unavailable to all of the just changed system objects.

As a consequence of the difficulty in finding ALL accounts used by domain administrator accounts, most organizations will neglect to change domain administrator account information. Because domain administrator accounts are generally valid on web servers, a disgruntled employee does not even need to visit their place of employment to cause damage.

#### 6. Solution: Mass Management Tools—Save Money and Roll Your Own



From what we have just discussed, the goal any security program is to stop or mitigate a problem. In the case of workstations we need some way of regularly changing the built-in administrator accounts and ideally make all of the passwords different. We also need some way of searching through all machines in the organization to find all instances of both local and domain administrator

accounts. Once all account usages are centralized we can embark on a regular program of changing the key account credentials on a regular basis as well as when key help desk or other administrators leave the organization.

The least expensive solution involves using the applets within the Resource Kit of Windows. With a little scripting and a bit of patience (and a good list of machines), many changes can be accomplished. Unfortunately, script based tools do not provide any database or GUI front end to perform management. They are also sorely lacking any ability to manage complex services, COM objects, randomization of passwords, or even scheduled tasks created by the GUI. If you have ever built a quick and dirty script, you know that the problem is not so much in writing it, as it is in documenting and supporting it.

What about using Group Policies? Unfortunately, Group Policies are a write-only solution with no ability to “aim before you shoot”. Group Policies are great for managing what is on a user’s desktop and do a great job locking out program, but they are not inherently intelligent and do not provide any reporting to the administrator.

Many administrators will write scripts that execute via Group Policies. However, this is a write-only solution with no inherent ability to feed back information on what was executed where and when. There is also an inherent delay as to when the script is actually run. The only sure way to assure that the script is run immediately is to set it up to execute on system reboot. This is not such a bad solution, but it is a dangerous one if it is a requirement for non-stop servers. Then there is the issue of how to reboot only the selected machines immediately. Also, you will need to get all of the applets distributed to all of the machines, or make them available via some sort of a common share (it could get kind of slow if all the machines attempt to use the same share at the same point).

Are “roll your own” solutions of scripts and/or Group Policies a bad solution? Not at all—you just need to keep in mind that there are significant limitations in capabilities, speed and the granularity of change. There is also the issue of what kind of time you have available to write and support the scripts and policies.

## 7. Solution: Lieberman Software’s Mass Management Tools

Lieberman Software Corporation (<http://www.lanicu.com>) has a complete suite of products that solve all of the problems just described. Lieberman Software Corporation has been developing commercial mass management tools to solve the problems outlined since 1997. All of the tools manage workstations and servers from Windows NT all the way to the most recent releases of Windows 2003 Server.



**User Manager Pro** – Removes the threat of a hostile user decrypting the local administrator account/password and gaining administrator access to all other machines with the same credentials. This tool is both a reporting and change tool for the mass management of workstations, servers and domain controllers. It manages all local accounts, groups and more on all machines simultaneously. With the optional **Random Password Generator** the program provides a continuous stream of complex passwords for each machine so that the compromise of a single machine will not allow access to all other machines in the network. The password generator maintains a local encrypted database of all current passwords so that the administrator can still gain access locally should it be necessary. The tool also has

the ability to intelligently strip out foreign accounts, groups and memberships so that all machines conform to the current IT standard.



**Service Account Manager** – With this tool you can regularly change the domain administrator accounts used by services distributed among machines in your organization. This program provides a single list of all services on all machines as well as the accounts being used. The service information can be sorted and used to generate reports as to account usage. When it comes time to change domain administrator accounts used by services, it is a simple matter of sorting on the account name field, highlighting all of the services to be changed, and clicking on the “Set” button within the program to make the changes on all machines at the same time. The program handles even the most complex services such as Veritas BackupExec and Microsoft Exchange. Going beyond what you might be able to program yourself, this program handles all service account members, rights and even the logon cache of each machine. Off-line machines are handled by an automatic retry mechanism that does not require any administrator intervention.



**Task Scheduler Pro** – One of the hardest security problems to solve is figuring out what accounts are being used by scheduled tasks. Using this program you can see all scheduled tasks running on all machines in a single sortable list. The list of tasks provides you with the accounts in use as well as the ability to do a mass change of the accounts used on any selected set of tasks within your organization. Without this tool, it is virtually impossible to get a global view of the working/damaged scheduled tasks within your organization.



**COM+ Manager** – Embedded in many servers are both commercial and custom build COM+ objects that use local and domain administrator accounts. Because there are so many objects and they are dispersed widely, the accounts used by the objects are virtually impossible to change in products. This tool gives you a single view of all COM+, MTS and DCOM objects on all machines at the same time within a single list. Using this tool you can see which objects are using which accounts. Once you have identified the objects that need account name/password changes, it only takes a few seconds to reconfigure the objects.

## 8. Summary

The greatest security threat to an organization is the wide distribution of administrator credentials in unprotected machines. In this paper you saw that to minimize the damage caused by this situation, an administrator must reduce local credentials to a minimum on each machine. Further, you saw that the only way to keep all machines from becoming hijacked was to put different credentials (passwords) on the built-in administrator account on each machine.

You also learned that credentials such as domain administrator accounts should be changed on a regular basis (at least every 60 days). This is frequently not done because the administrator accounts are buried in such multitude of places, (services, scheduled tasks, COM+, DCOM, MTS objects) manual search and replace techniques make it infeasible to accomplish the change in a timely manner. Consequently, credentials may be unchanged for years due to the difficulty in changing all the places the credentials are used.

Finally, you learned how you could use resource kit applets and scripts to accomplish some of the work, but that there specialized tools to easily handle the mass management of these distributed credentials. Whether you roll your own, or purchase a third party suite of products, you must actively manage your distributed credentials.

Failing to manage these risks means you don't care if former administrators can continue to have domain administrator privileges, and it is also inconsequential if a hostile user becomes an administrator of all your machines without your knowledge. In the real world, limiting administrator access is considered a smart thing to do.

**Our support staff is available to answer your technical questions whether you are a customer or not.**

**Voice: 800.829.6263 (USA/Canada) Voice: (01) 310.550.8575 (Worldwide) Fax: (01) 310.550.1152 (Worldwide)  
Web: [www.lanicu.com](http://www.lanicu.com) Email: [support@lanicu.com](mailto:support@lanicu.com)**

