Massive Security Hole Ignored!

Even when administrators dutifully lock up their servers, apply patches, and use group policies to lock down server and workstation security, with a quick search of the web, it only takes a few minutes for a hacker to unlock the keys to the kingdom: administrator accounts and passwords.

Table of Contents

Microsoft GOLD CERTIFIED Partner

www.liebsoft.com | P 800.829.6263 (USA/Canada) P (01) 310.550.8575 (Worldwide) F (01) 310.550.1152 | 1900 Avenue of the Stars, Suite 425, Los Angeles, CA 90067

Massive Security Hole Ignored!

White Paper

Introduction

Anyone with a little bit of initiative can break into your systems in a matter of minutes, quietly, and without leaving a trace.

The most fundamental rule of security is that without physical security, there is no security. It is for that reason that 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.

The most fundamental rule of security is that without physical security, there is no security.

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 Out-of-date server software may contain security holes that can be exploited by hackers.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 an organization.

The third rule of security is that machines should be configured for the minimum level of functionality required to accomplish the job. This is accomplished to a large extent with group policies in Active Directory. Group policies allow for the configuration of workstation and server desktops, registry permissions, and other access controls.

So, everything is locked down…or is it?

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 the entire domain.

The administrator has a significant challenge if security requirements dictate that all accounts must have a password change regularly. The reason for the challenge: it is tedious to update the local accounts as well as accounts used by every task, service, and COM object on every machine. **Consequently, local accounts as well as accounts used by tasks, services, and COM objects are generally never changed**.

Following is a list of credentials that can potentially become compromised:

- **Built-in administrator account on every machine:**
  Every machine has a local logon account that is created at the time the machine is built. The account name and password is usually the same on every system. This means all a hacker has to do to become an administrator is to crack the local administrator password (remember — all of the systems have the same username and password). Cracking the local administrator common password can be done in seconds using rainbow tables[1] and a boot floppy[2]. If all local machines and servers use the same built-in administrator account and password, once a single machine has been compromised, an ordinary user will now have unfettered access to all systems.

- **Local servers that use local or domain administrator accounts:**
  Many machines use services that require either a local or domain administrator account to run. 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[3], it is a simple matter to run a password cracking program such as rainbow tables or login recovery to view the secrets area of a Windows NT or newer 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 a program whether or not someone is logged onto the machine. The credentials for each task are stored locally on each machine.

- **MTS/COM+/DCOM components that use local or domain administrator accounts:**
  Microsoft's initiative since Windows NT4 has been for developers to create n-tiered applications (also known as DNA or Digital Nervous System applications). This has spawned a wide range of complex components that typically use administrative accounts. 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 amount of layers which must be excavated to locate this information.

…because of the nature of distributed credentials and the lack of tools provided by Microsoft to manage this vast array of security information, most administrators choose to ignore the problem.

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

Best Practices: Workstations

Since curious users can easily and quietly penetrate the local security of their own machines 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 Microsoft's Active Directory, the registry editing tool and hacking tools, can be disabled. However, these policies are totally ineffective since hackers can just boot to a diskette or CDROM and run their tools in DOS. Another option is to remove or electronically disable the floppy and CDROM drives, which will be effective — until a determined person gets into the case or BIOS and re-enables the devices. The most insidious attack would be for the hacker to simply copy the information or image the machine to a location you do not control and crack it at their leisure.

It seems that for every step an administrator takes to counter a hostile user from extracting sensitive information, there is a workaround. **This means that 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 have their passwords changed on a regular basis. Even better, each machine should have its own unique password that is complex and long enough so that cracking the password is not practical.

Best Practices: Servers

When administrators leave an organization, they leave with the knowledge of all secret administrator accounts as well as the knowledge that the organization they left will be unable to change (or be complacent about changing) credentials due to lack of tools and time. Within a large organization there may be hundreds or thousands of servers with domain administrator accounts running as services, scheduled tasks, MTS/COM+/DCOM objects, and local logon accounts. Any attempt to change the credentials of these accounts will result in an 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" credentials, the just-changed account will be locked out and be unavailable to all of the just-changed system objects.

Due to the difficulty of finding ALL objects used by domain and local administrator accounts, most organizations will neglect to update this information with any kind of regularity.

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

The goal of any security program is to stop or mitigate a problem. In the case of workstations there needs to be a way to regularly change the built-in administrator accounts and ideally make all of the passwords unique. There also needs to be a way of searching through all of the machines in an organization to find all instances of both local and domain administrator accounts. Once this information is gathered, it must be updated regularly. The credentials of those accounts must also be regularly updated, and as personnel leave the organization.

Due to the difficulty of finding ALL objects used by domain and local administrator accounts, most organizations will neglect to update this information with any kind' of regularity.

The least expensive solution (in terms of initial cash outlay) involves using applets within the resource kits, a fair bit of scripting, a lot of patience, and an up-to-date list of systems. Unfortunately, script-based tools do not provide any database or GUI front end to perform management. They also sorely lack any ability to manage complex services, COM objects, true randomization of passwords, or even scheduled tasks created via the GUI. The problem is not so much in writing the script as it is in testing, troubleshooting, documenting, supporting, and updating, as well as providing adequate security in the script.

Group policies are a write-only solution with no inherent intelligence. They have no reporting capabilities and rely on the workstation to request an update. This means there can be a lag in time of hours from the application of the group policy in Active Directory to the application of that same group policy on a system — if it works.

Many administrators will write scripts that execute via group policies. However, this is a write-only solution with no inherent ability to feed information back on what was executed where and when. Timing is another important issue. The only way to ensure that the script will run in this scenario is to configure it as a startup or shutdown script — this is an implausible solution for servers needing to run 24 hours per day, 365 days per year.

"Roll your own" solutions utilizing scripts and group policies are not necessarily bad solutions — they simply exhibit severe functional limitations, speed, and granularity. Then there is the issue of availability to write and support these scripts and policies.

Solution: Lieberman Software's Mass Management Tools

Since 1997, Lieberman Software Corporation (http://www.liebsoft.com) has developed commercial mass management tools to solve all of the problems just described. All of the tools manage workstations and servers from Windows NT to the most recent releases of Windows.

Each tool is written to function without the use of agents, thus reducing the cost of deployment and management. Each tool is designed so that a single administrator can function as many administrators — able to touch hundreds or thousands of machines in a single key stroke. Because these products operate in parallel (instead of sequentially, like scripts), this means that a single (or multiple) machine will have no affect on the rest of the machines receiving the necessary changes.

- **Random Password Manager**™ is a stand-alone and feature complete rendition of the Random Password Generator found in User Manager Pro Suite. Building on the concept of continuously and automatically updating each system with a completely unique password, this tool adds additional levels of encryption, automatic re-randomization following a period of time, password vault, recovery notifications, password verification, and password history. In addition to managing Windows and Active Directory account passwords, Random Password Manager can also be used to manage SQL Server, Linux, and Unix account information.

- **Enterprise Random Password Manager**™ builds on Random Password Manager's foundation of continuously and automatically updating each system in the network with a completely unique password. It seeks seek out all accounts, and every place the accounts can be used in the environment - including services, tasks, COM/DCOM/MTS, IIS, and other locations. When a password change is implemented, Enterprise Random Password Manager updates the account information in every place it is used. In addition to managing Windows and Active Directory account passwords, it can also manage SQL Server, Linux, and Unix account information. Enterprise Random Password Manager, just like Random Password Manager, has also been provided an extensible programmable interface to allow for management of items such as switches, routers, and other applications.

- **User Manager Pro Suite**™ removes the threat of a hostile user decrypting the local administrator account/password and gaining access to all other machines with the same credentials. In addition to being a complete reporting tool, User Manager Pro Suite also provides for mass management of workstations, servers, and domain controllers. It manages all local accounts, groups, registries, files, and more on all machines simultaneously. The Suite's Random Password Generator™ tool 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 gain access locally should it be necessary. The tool also has the ability to intelligently remove foreign accounts, groups, and memberships so that all machines conform to the current IT standard.

- **Service Account Manager**™ regularly change the account information used by the services distributed among the machines throughout an 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 for account usage. When it comes time to change the credentials used by services, it is a simple matter of selecting the services and clicking the "SET" button within the program to make these changes. The program handles the most complex services such as Veritas BackupExec and Microsoft Exchange. This program is also able to handle rights and the logon cache of each machine, ensuring that all services can always start.

- **Task Scheduler Pro**™ can regularly change the account information used by the scheduled tasks distributed among the machines throughout an organization. This program provides a single list of all scheduled tasks on all machines as well as the accounts, and other information being used. With this information, administrators can quickly and accurately update all scheduled tasks; ensuring items such as antivirus are always up to date.

- **COM+ Manager**™ arms administrators with the information about the MTS/COM+/DCOM objects on all managed systems. Because there are so many objects that are widely dispersed and obfuscated behind poorly documented programming and user interfaces, it becomes virtually impossible to see which objects are using which accounts. Once the administrator identifies objects that need account information updates, it is only a matter of selecting the option to "Set Identity".

LIEBERMANSOFTWARE™

Massive Security Hole Ignored!

White Paper

Summary

The greatest security threat to an organization is the wide distribution of administrator credentials in unprotected machines. This paper demonstrated that to minimize the damage caused by this situation, an administrator must reduce local credentials to a minimum on each machine. This is achieved through monitoring and regularly changing local and domain account passwords, and updating everywhere those accounts are used.

Organizations that neglect these security best practices leave themselves open to risks such as former administrators continuing to have domain wide privileges and users gaining access to all systems. In the world of regulatory compliance and governance, this is a dangerous thing to do.

The greatest security threat to an organization is the wide distribution of administrator credentials in unprotected machines.

For more information on how Lieberman Software can help secure your enterprise, email **sales@liebsoft.com** or call **800-829-6263** (US and Canada or **(01) 310-550-8575** (Worldwide).

1 Rainbow tables are precompiled tables of LM, NTLM, MD5, and other hash types. Rainbow tables are distributed freely across the internet as are the tools which generate them.
2 Using the login recovery tool (http://www.loginrecovery.com) is as easy as rebooting the system with a boot floppy. In most cases, the tool can tell you the current password within minutes.
3 Many utilities are available free to download to reset any account including the built-in administrator. Such utilities include John the Ripper (http://www.openwall.com/john/) and EBCD (http://ebcd.pcministry.com/).