



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 permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Auditing Systems, Applications, and the Cloud (Audit 507)"
at <http://www.giac.org/registration/gсна>

Auditing User Accounts in a Windows 2000/2003 (Active Directory) Domain

GSNA Practical v4.0

Option # 1
Topic 1 – “Testing”

Charlie Clauss
4/1/2005

Abstract

The use of a Windows 2000/2003 Active Directory Domain has become an industry standard. The domain user authentication process is relied upon to protect the information assets stored on the servers (and workstations) within the enterprise or organization. In many cases it is the only level of authentication that is in use.

This paper describes some of the vulnerabilities that may be present due to a combination of mis-configured security settings, weak or missing passwords, and poor attention to user management. The purpose is to then describe several of the risks associated with these combinations, detail the tests that can be performed to measure the extent of the risk, and show the results of actual tests performed.

© SANS Institute 2005, Author retains full rights.

Table of Contents

Abstract.....	2
Table of Contents.....	3
1: Identification.....	4
2: Risk Analysis.....	7
2.1 Review User Accounts and Groups.....	9
2.2 Review Group Policy Objects and Assignment.....	10
2.3 Review Password Strength.....	12
2.4 Risk Summary.....	12
3: Testing.....	13
3.1 Review User Accounts and Groups.....	13
3.2 Review Group Policy Objects and assignment.....	23
3.3 Review Password Strength.....	28
4: Audit.....	39
4.1 Review User Accounts and Groups.....	39
4.2 Review Group Policy Objects and Assignment.....	53
4.3 Review Password Strength.....	57
4.4 Institution Policies related to passwords and users.....	62
4.4 Conclusions.....	64
References.....	65

© SANS Institute 2005, Author retains full rights.

1: Identification

The specific system used in this audit process and results is a Windows 2000 domain in a regional financial institution. All names and addresses have been changed or obscured for privacy purposes. The domain consists of approximately fourteen (14) servers and one hundred (100) workstations on a “flat” Wide Area Network of eight (8) locations. Each location has its own Domain Controller and there are two (2) DC's at the operations center where the onsite portion of this audit took place.

While the results shown here are specific to the financial institution in question, experience has shown that the elements of the audit are representative of most small organizations using the Windows 2000/2003 Domain model. It should be noted that the introduction of multiple domains with trust relationships significantly (possibly exponentially) increases the complexity of audit. The complex system is not addressed in this paper, but the concepts and tests used are most certainly applicable.

The following is a diagram of the network in which the Active Directory domain exists:

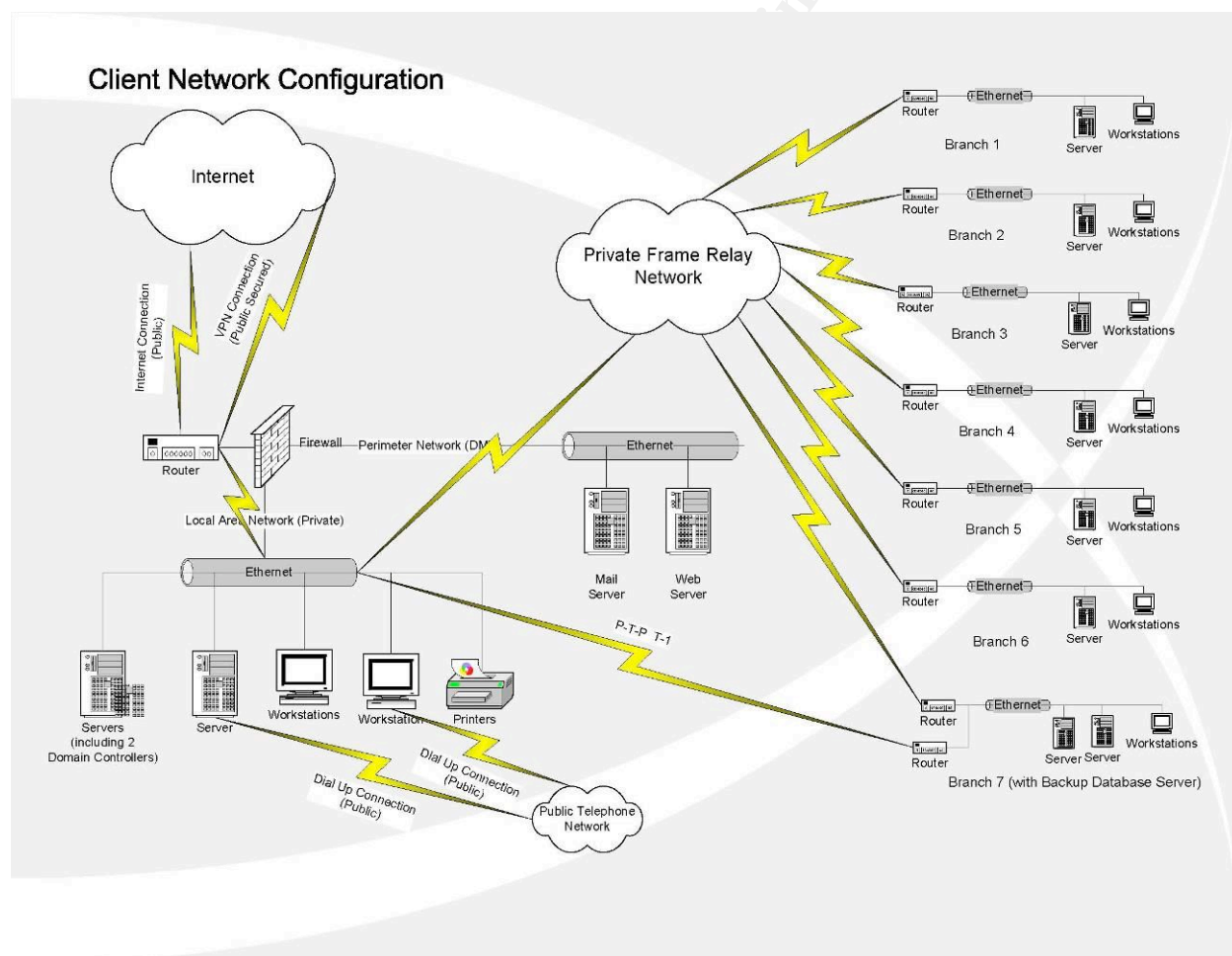


Figure 1.1 Network Diagram

This domain protects the institution's confidential information including, but not limited to, customer name, address, driver's license images, and other personal data, proprietary institution processes and financial information, and employee personal information such as name, address, social security number, family data, and limited medical information. Impact on the institution of a compromise and unauthorized access to this information is shown in the chart below:

Unauthorized access to:	Possible Result	Possible Consequence
Customer Information	Identity theft Lawsuit	Public Relations and stock value risk Officer liability under Sarbanes Oxley Gramm-Leach-Bliley Act violation FDIC insurability issue
Financial Information	Sold to competitor	Profit impact Stock value risk
Employee Information	Identity theft Lawsuit	Possible HIPPA violation

Figure 1.2 Chart of Risks

The scope of this audit is limited to the single domain, a representative Domain Controller, and associated domain users and groups. There are several ways that domain authentication could be compromised:

Access method	Causal Weaknesses	Method
Hack from Public side of firewall	<ul style="list-style-type: none"> • Weak firewall • Domain controller accessible from public side 	<ul style="list-style-type: none"> • Buffer overflows • Scans
Hack from network	<ul style="list-style-type: none"> • Most likely vulnerability • Physical access to network switches weak • Wireless access available • Hubs rather than switches • Physical access to workstations not protected 	<ul style="list-style-type: none"> • Scanner sniffing passwords • Key loggers • "Shoulder surfing"
Hack directly on domain controller	<ul style="list-style-type: none"> • Physical security weak 	<ul style="list-style-type: none"> • Scanner sniffing passwords • Key loggers
Valid user probing the network	<ul style="list-style-type: none"> • Configuration of user / group assignment • Group Policy configuration error • Failure to maintain old user accounts 	<ul style="list-style-type: none"> • User discovers elevated rights either purposely or accidentally • User attempts access with another user's credentials

Figure 1.3 Chart of Vulnerabilities

There are many resources that discuss best practices in setting up security on a Windows 2000/2003 domain. One example that is clear and concise is University of Washington School of Medicine's Security procedures¹. These should, of course, be adjusted to fit the organization's overall Risk Assessment and Mitigation strategy. Another good source on best practice is Kathy Ivens' "Getting Started with Windows Administration"². Financial institutions should insure that Operating System access meets or exceeds the guidelines set forth in the FFIEC Information Security - IT Examination Handbook³. Lastly, one of the primary reasons for detailed auditing of the Windows 2000/2003 domain user accounts comes from Microsoft TechNet's "10 Immutable Laws of Security"⁴:

Law #5: Weak passwords trump strong security

The purpose of having a logon process is to establish who you are. Once the operating system knows who you are, it can grant or deny requests for system resources appropriately. If a bad guy learns your password, he can log on as you. In fact, as far as the operating system is concerned, he is you. Whatever you can do on the system, he can do as well, because he's you. Maybe he wants to read sensitive information you've stored on your computer, like your e-mail. Maybe you have more privileges on the network than he does, and being you will let him do things he normally couldn't. Or maybe he just wants to do something malicious and blame it on you. In any case, it's worth protecting your credentials.

Always use a password—it's amazing how many accounts have blank passwords. And choose a complex one. Don't use your dog's name, your anniversary date, or the name of the local football team. And don't use the word "password"! Pick a password that has a mix of upper- and lower-case letters, number, punctuation marks, and so forth. Make it as long as possible. And change it often. Once you've picked a strong password, handle it appropriately. Don't write it down. If you absolutely must write it down, at the very least keep it in a safe or a locked drawer—the first thing a bad guy who's hunting for passwords will do is check for a yellow sticky note on the side of your screen, or in the top desk drawer. Don't tell anyone what your password is. Remember what Ben Franklin said: two people can keep a secret, but only if one of them is dead.

Finally, consider using something stronger than passwords to identify yourself to the system. Windows 2000, for instance, supports the use of smart cards, which significantly strengthens the identity checking the system can perform. You may also want to consider biometric products like fingerprint and retina scanners.⁴

¹ <https://security.uwmedicine.org/Docs/Procs/MSWebsiteWin2000ServerSecurity.htm>

² <http://www.windowsitpro.com/Windows/Article/ArticleID/40721/40721.html>

³ http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#infosec

⁴ <http://www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.msp>

2: Risk Analysis

In Calculating Your Security Risk, Peter Tippet, Chief Technology Officer of Reston, Virginia-based TruSecure™ Corp. defines Risk as “Threat Times Vulnerability Times Cost”⁵.

A comprehensive guide to Risk Assessment methodology can be found in Microsoft Corporation’s Security Risk Management Guide Chapter 4: Assessing Risk⁶, and defines risk in a similar fashion.

The structure of the risk assessment, no matter the source, is very similar:

- Identify and rate the potential threat
- Identify and rate the potential vulnerability
- Identify and rate the cost of loss or compromise of the asset that would be exposed

If any of the three are zero, the risk becomes zero. An unpatched Web server connected directly to the Internet, a situation that seems to be very risky, can still have zero if there is no data stored on the server and it is the only device connected. (One could argue that there is still the risk of legal responsibility for its use in a distributed attack, or the cost of having to rebuild the server, but that would be stretching it a bit). The point is that all three must exist for risk to be present, and the magnitude of the risk is directly related to the magnitude of the three elements- Threat, Vulnerability, and Cost. The definition of each element follows.

A **threat** is an event that may “negatively impact an asset, represented by loss of confidentiality, integrity, or availability of the asset”⁶. It is always associated with some frequency of likelihood of occurrence, and because of that is more easily measured. It does not have to be an overt attempt at intrusion. Unintentional use of a mis-configured system or an employee’s naïve curiosity or ignorance also poses threats.

A **vulnerability** is a weakness that has the potential to be exploited affecting an asset in some way. Its magnitude can be measured as the likelihood of success of a threat or attack. Negative impact on an asset may be in the form of:

- A competitive advantage obtained
- A legal liability situation
- A regulatory compliance issue
- Influence on the availability of the asset thus affecting revenue or productivity
- Impact on Business or Organizational reputation
- Actual damage to the asset requiring repair or replacement

The magnitude of the vulnerability is related to the following factors:

- Attacker population- The probability of exploit normally increases as the attacker population increases in size and technical skill level.
- Remote vs. local access- The probability normally increases if a vulnerability can be exploited remotely.
- Visibility of exploit- The probability normally increases if an exploit is well known and publicly available.

⁵ http://www.theciostore.com/watchit_product.asp?id=196

⁶ <http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/srsgch04.mspx#EAAA>

- Automation of exploit- The probability normally increases if an exploit can be programmed to automatically seek out vulnerabilities across large environments.

Microsoft suggests the following rating system based on the probability of vulnerability:

Probability Definitions for Vulnerabilities	
High	
<i>Large attacker population- "script-kiddie"/hobbyist</i>	
<i>Remotely executable</i>	
<i>Anonymous privileges needed</i>	
<i>Externally-published exploitation method</i>	
<i>Automated</i>	
"5" if any apply	
Medium	
<i>Medium attacker population - expert/specialist</i>	
<i>Non-remotely executable</i>	
<i>User level privileges required</i>	
<i>Not publicly-published exploitation method</i>	
<i>Non-automated</i>	
"3" if any apply	
Low	
<i>Small attacker population - insider knowledge</i>	
<i>Non-remotely executable</i>	
<i>Administrator level privileges required</i>	
<i>Not publicly-published exploitation method</i>	
<i>Non-automated</i>	
"1" if all apply	

Figure 4.15 Risk Analysis Worksheet: Evaluating Vulnerability (SRMGTool3) ⁶

The **cost** is the estimate of the consequences of a successful exploit (threat to a vulnerability). Direct costs would be the replacement of the damaged information, hardware, and software. Also included in direct cost would be the actual cost of lost business, remediation of the exploit, legal ramifications due to lawsuits or regulatory sanctions, repair to customer or stockholder relations by the Public Relations department. Indirect or difficult to measure costs would be those associated with lost productivity, stockholder and customer confidence, and future business opportunities.

In the Information Technology world, **risk** is therefore **highest** when there is a potentially frequent threat on a system with known, easily and automatically exploited vulnerabilities, holding (information) assets that are valuable and sensitive to the business or organization responsible for them. Rarely, if ever, will we be able to assess the risk as zero. Some risk must be present if there are assets of value stored on our network where there are multiple people with legitimate access requirements. Risks should be mitigated in a fashion appropriate to their magnitude.

In applying this concept of risk to user accounts in a Windows 2000/2003 domain, we find there are some serious risks associated with users with elevated or mis-configured rights. In figures 1.2 and 1.3 we reviewed the potential risks and vulnerabilities to the financial institution regarding a compromise to their Windows 2000/2003 domain. Those risks could have a serious and detrimental effect on the business. Breach of Gramm-Leach-Bliley and Sarbanes-Oxley could have personal liability repercussions to the officers and Board members. This has a way of making the security of the Windows 2000/2003 domain a very personal issue to the management of the institution.

Three selected impacts and vulnerabilities for testing and audit are as follows:

- 1- Employees with either inappropriate access configured for their own user ID or knowledge of another (possibly terminated) employee's password.
- 2- Improperly configured Group Policy Objects could inadvertently apply rights to users or workstations that yield undesired elevated rights.
- 3- A valid user, or other person with access to the physical network, could attempt to crack the user IDs and passwords of other users.

Industry experts say that between 60 and 80 percent of exploits occur from inside the network. We spend tens of thousands of dollars (and more) on firewalls and Intrusion Detection and Intrusion Prevention systems (IDS/IPS), and very little on simple review of internal network configurations.

Windows 2000 and Windows 2003 are built on a domain authentication scheme that is solid in its foundation. Security related improvements have been significant from the Windows NT 4.0 days, and they continue to improve. Each of these impacts revolves around the underlying data held on the network servers and workstations of the institution. Each vulnerability is caused by a different set of circumstances.

2.1 Review User Accounts and Groups

First, user access to the network information store is limited based upon the user ID and associated group memberships of that user. Rights of all kinds are assigned either directly to a user or to a group of users. Rights are either to resources on a particular computer, or globally on the domain (all member machines). Typically, the local Administrator group and the Domain Administrator group are the groups with the most authority to access and change the underlying security framework of the network. Other groups have either more (as in the Enterprise Admin or Schema Admin group) or less (as in the Everyone group) authority to access and change the rights.

Periodic reviews of user accounts on the domain are essential to maintaining a good security framework. Even if an organization has an extremely tight, rigorous audited process of adding, deleting, and changing users and definition and assignment of authority to users and groups, it is important to review the current status of users and group assignments periodically.

The accounting corollary is that of the difference between a P&L and balance sheet. We can have a great P&L, where our sales are through the roof, but the balance sheet shows that all sales are going into Accounts Receivable (and are not being collected). The balance sheet shows that we have a problem. Review of the user accounts can

show a problem that is not evident by reviewing the user, group, and rights assignment processes. Too many user accounts with Domain Admin rights or Dial-In rights, old accounts that were set up as application service accounts and never deleted, users that are simply no longer using the system (and therefore, possibly shouldn't have an account), accounts that were simply missed or mis-keyed in the entry of the add, delete, or change are all examples of issues that can be caught in a user/group review.

The current policies for user logon windows, remote access, password change frequency, and add/delete/change users should be the backdrop of this review. They will, presumably, define the appropriate risk mitigation strategy for these areas.

2.2 Review Group Policy Objects and Assignment

Included within all Active Directory networks, beginning with Windows 2000, is Microsoft's Change and Configuration Management (CCM) system for Windows. The central component of this system is the Group Policy, which is managed by configuring Group Policy Objects (GPOs). Group Policy Objects are collections of Group Policy settings. GPO's are stored at the domain level, and they affect users and computers that are contained in sites, domains, and organizational units. In addition, each computer has exactly one group of policy settings stored locally, called the local Group Policy object. The Group Policy Object Editor is the Microsoft Management Console (MMC) snap-in that is used to edit Group Policy objects (GPOs). The two kinds of Group Policy objects are local and nonlocal.⁷

Microsoft defines GPO's as follows:

*"The infrastructure within Active Directory directory service that enables directory-based change and configuration management of user and computer settings, including security and user data. You use Group Policy to define configurations for groups of users and computers. With Group Policy, you can specify policy settings for registry-based policies, security, software installation, scripts, folder redirection, remote installation services, and Internet Explorer maintenance. The Group Policy settings that you create are contained in a Group Policy object (GPO). By associating a GPO with selected Active Directory system containers--sites, domains, and organizational units--you can apply the GPO's policy settings to the users and computers in those Active Directory containers. To create an individual GPO, use the Group Policy Object Editor. To manage Group Policy objects across an enterprise, you can use the Group Policy Management console."*⁸

⁷ http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/gpe_gpo.asp

⁸ <http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Storage.asp>

Local Group Policy objects are stored on individual computers. Only one local Group Policy object exists on a computer. Local Group Policy object settings can be overwritten by nonlocal settings if they are in conflict; otherwise, both groups of settings apply. Nonlocal Group Policy objects, which are stored on a domain controller, are available only in an Active Directory environment. An organizational unit (OU) is the smallest scope to which a Group Policy object (GPO) can be linked, or over which administrative authority can be delegated. (An organizational unit is an Active Directory logical container into which users, groups, computers, and other organizational units are placed.)⁷ The Group Policies are applied in a layered effect, with deny restrictions taking precedence. Group Policy Inheritance can be blocked, so the actual resulting Group Policies that affect a user can become quite complex.

Group Policy objects, other than the local Group Policy object, are virtual objects. The policy setting information of a GPO is actually stored in two locations: the Group Policy container and the Group Policy template. The Group Policy container is an Active Directory container that stores GPO properties, including information on version, GPO status, and a list of components that have settings in the GPO. The Group Policy template is a folder structure within the file system that stores Administrative Template-based policies, security settings, script files, and information regarding applications that are available for Group Policy Software Installation. The Group Policy container is a directory service object. It includes sub-containers for computer and user Group Policy information. The Group Policy container contains the following data:

- Version information- Used to verify that the information is synchronized with Group Policy template information.
- Status information- Indicates whether the Group Policy object is enabled or disabled for this site
- List of components- Specifies which extensions to Group Policy have settings in the Group Policy object.

The Group Policy template folder contains subfolders, including, but not limited to, the following:

- Adm- Contains all the .adm files for this Group Policy template.
- Scripts- Contains all the scripts and related files for this Group Policy template.
- User- Includes a Registry.pol file that contains the registry settings that are to be applied to users. When a user logs on to a computer, this Registry.pol file is downloaded and applied to the HKEY_CURRENT_USER portion of the registry. The User folder contains an Applications subfolder.
- User\Applications-Contains the application advertisement script files (.aas) that are used by the operating system-based installation service. These files are applied to users.
- Machine- Includes a Registry.pol file that contains the registry settings that are to be applied to computers. When a computer initializes, this Registry.pol file is downloaded and applied to the HKEY_LOCAL_MACHINE portion of the registry. The Machine folder contains an Applications subfolder.
- Machine\Applications- Contains the .aas files that are used by the operating system-based installation service. These files are applied to computers.⁹

⁹ Microsoft Corporation

As you may imagine, the use of Group Policy Objects can get quite complex. In fact, the lack of a way to view which Group Policy actually delivered a particular setting to a user or workstation was a serious shortcoming (certainly for auditors) in Windows 2000. With the introduction of Windows XP and Windows 2003 came the Group Policy Management Console which “allows management of Group Policy across sites, domains, and organizational units within one or more forests”⁹ It installs on a Windows XP or 2003 workstation or server and can review the effects of all GPO

We will focus here on the two possible errors in administration that affect the GPO delivered to a particular user- A mis-configuration of a GPO that delivers incorrect rights to a user, or an assignment of an incorrect GPO to an unauthorized user. It is possible that a more restrictive GPO is delivered to a user than is authorized. Usually, this is discovered because the user is denied access to a file or service required to perform his/her job. It is highly unusual for a user to highlight the fact that he/she has been granted rights to which he/she is not authorized. The latter is the true risk of GPO mis-configuration.

2.3 Review Password Strength

Any person with physical access to the network has a window to crack the passwords of the domain. Most small to mid-sized organizations are not sophisticated enough to have the controls in place to prevent or foil such an attempt. A process can be added to any computer that captures keystrokes as they occur, a program can be loaded and run that will attempt to crack the domain passwords just by pointing it at a domain controller.

So, our security mission is twofold. We need to put controls into place to reduce the possibility of key logger and cracking programs being introduced to our network. Testing for this particular vulnerability is not addressed in this paper.

Secondly, we need to insure that our passwords are strong enough to withstand a cracking attempt for a period of time. The length of time that any password needs to be capable of withstanding an attack is the maximum amount of time between forced changes of passwords, or until the attack is detected, isolated, and stopped.

(Vulnerability window = Identification time + Remediation time). The password policy, the implementation of password security (password length, complexity, and change frequency), and the testing of passwords should all be reviewed to determine risk.

2.4 Risk Summary

Since we initially began this section defining risk as $\text{Threat} \times \text{Vulnerability} \times \text{Cost}$, our three impacts all have high risk. While the organization and its Information Services staff may argue that the threats and vulnerabilities associated with the three impacts- user and/or group mis- configuration, Group Policy Object mis-configuration, and password hacking, are mitigated in some way, it cannot be argued that the cost of potential loss or compromise of the assets on the network make this a very important audit area.

3: Testing

This section presents testing for the three areas of impact selected above. It assumes a certain level of familiarization with installing programs, working with users and groups, and Active Directory concepts.

3.1 Review User Accounts and Groups

A review of the users and groups defined on the domain can be undertaken using the following steps:

- Use a tool to capture user and group information from the domain controller
- Organize the output for ease of analysis
- Identify the users with elevated rights (Remote Access, etc.) and verify authority
- Identify users belonging to groups with elevated rights and verify authority

The simplest tools for reviewing users and groups are Somarsoft's DUMPSEC (formerly DUMPACL) and Hyena. The 2.8.2 version of DUMPSEC was used for this testing.

Preparation:

- Use a workstation or laptop with network access to the domain controller
- Insure you have administrative access to the domain (either as a Domain Admin or have the step of data collection performed by a Domain Admin under your supervision)
- Download and install DUMPSEC from the systemtools.com site¹⁰
- Insure a copy of Microsoft Excel is available for the analysis of collected data
- A fairly advanced knowledge of Excel (or a staff member who can assist) is very helpful.

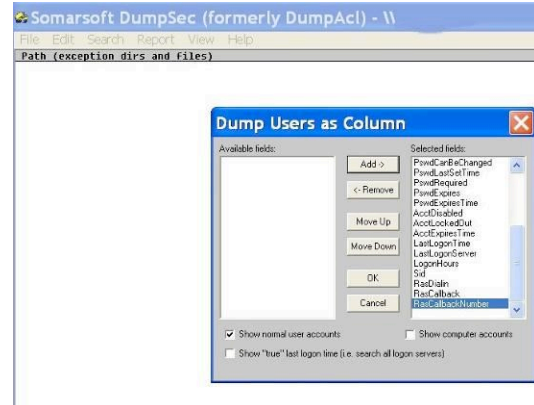
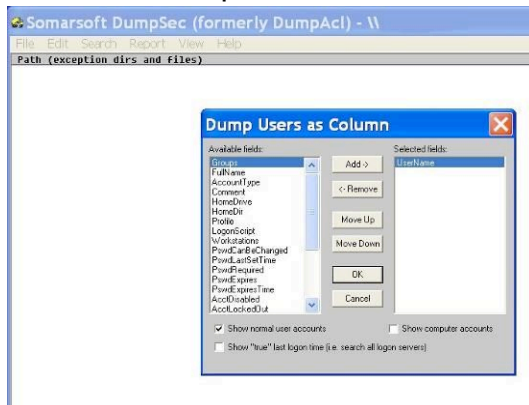
Data Collection

- Launch DUMPSEC
- Using the Report "Select a Computer" type the name of the domain controller (e.g. \\dc1)



¹⁰ Copyright 1994-1998 Somarsoft, Inc., Distribution point <http://www.systemtools.com/somarsoft>

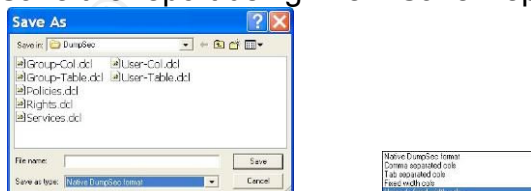
- Select Dump Users as column



- Highlight the Groups field in Available fields and press Add->. This will move it to the Selected field column. Repetitively press the Add-> key until all fields have been selected. Then press OK. The report should populate:

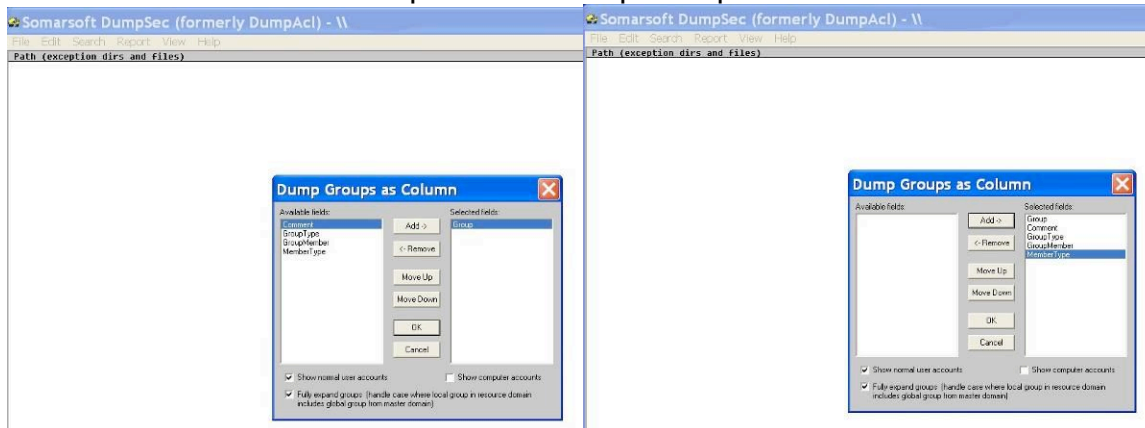
Administrator	
Groups	Administrators (Local, Administrators have complete and unrestricted access to the computer/domain)
FullName	
AccountType	User
Comment	Built-in account for administering the computer/domain
HomeDrive	
HomeDir	
Profile	
LogonScript	
Workstations	
PwdCanBeChanged	Yes
PwdLastSetTime	7/22/2004 2:58 PM
PwdRequired	Yes
PwdExpires	No
PwdExpiresTime	Never
AcctDisabled	No
AcctLockedOut	No
AcctExpiresTime	Never
LastLogonTime	1/20/2005 1:59 PM
LastLogonServer	bucg-102
LogonHours	All
Sid	S-1-5-21-1399190424-3886189598-1179759684-500
RasDialin	No
RasCallback	None
RasCallbackNumber	
ASP.NET	
Groups	Users (Local, Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified
FullName	ASP.NET Machine Account
AccountType	User
Comment	Account used for running the ASP.NET worker process (aspnet_wp.exe)
HomeDrive	
HomeDir	
Profile	
LogonScript	
Workstations	
PwdCanBeChanged	No
PwdLastSetTime	3/24/2005 3:50 PM
PwdRequired	No
PwdExpires	No
PwdExpiresTime	Never
AcctDisabled	No
AcctLockedOut	No
AcctExpiresTime	Never
LastLogonTime	Never
LastLogonServer	bucg-102
LogonHours	All
Sid	S-1-5-21-1399190424-3886189598-1179759684-1006
RasDialin	No

- Save the report using File Save Report As



It is a good idea to save each report as Native DumpSec format first. This will preserve the report so that it can be accessed later as required. Also, save the report in Comma Separated Cols- it will be used in Excel for analysis and presentation.

- Perform the same steps for the Dump Groups as column....



Both the User report and the Group report can be printed directly from DUMPSEC. However, review of the printed documents is extremely difficult since the key items are potentially spread throughout hundreds of pages of output. Analysis of the results is simplified with the use of Excel or another spreadsheet program.

The key elements of the user file that should be captured are:

- User
- FullName
- AcctDisabled
- PswdExpiresTime
- PswdLastSetTime
- LogonHours
- LastLogonTime
- RasDialin

The key elements of the group file that should be captured are:

- Group Type
- Group Name
- User

Opening the user file (user-col.txt) in Excel yields the following view:





1/28/2005 10:11 AM - Somarsoft DumpSec (formerly DumpAcl) - \\han			
1	UserName		
2			
3	rc=1355 RasAdminUserGetInfo		
4	Administrator		
5	Administrator		
6	Group	Administrators (Global)	Members can fully administer the computer (Members)
7	Group	Backup Operators (Global)	Members can backup the security to back up files
8	Group	Domain Admins (Global)	Designated administrators of the domain
9	Group	Domain Users (Global)	All domain users
10	Group	Enterprise Admins (Global)	Designated administrators of the enterprise
11	Group	Group Policy Creator Owners (Global)	Members in this group can modify group policy for the domain
12	Group	Schema Admins (Global)	Designated administrators of the schema
13	Group	Schemas Admins (Global)	Designated administrators of the schema
14	FullControl	Administrators	
15	AccountType	User	
16	Comment	Build or account for administering the computer (Members)	
17	HomeDir		
18	HomeDr		
19	Profile		
20	LoginScript	login.bat	
21	Workstation		
22	PowerShellChange	Yes	
23	PowerShellTime		7/24/2007 13:45
24	PowerShellTime	Yes	
25	PowerShellTime	No	
26	PowerShellTime	None	
27	PowerShellTime	No	
28	PowerShellTime	No	
29	PowerShellTime	None	
30	PowerShellTime		10/20/05 9:17
31	PowerShellTime	All	
32	PowerShellTime	All	
33	PowerShellTime	5-11-21-189622-02-021037454-30024121037454	
34	PowerShellTime	Yes	
35	PowerShellTime	None	
36	PowerShellTime		
37	PowerShellTime		
38	PowerShellTime		
39	PowerShellTime		
40	PowerShellTime	Domain Guests (Global)	All domain guests
41	PowerShellTime		
42	PowerShellTime	User	
43	PowerShellTime	Build or account for guest access to the computer (Members)	
44	PowerShellTime		
45	PowerShellTime		
46	PowerShellTime		
47	PowerShellTime		
48	PowerShellTime		
49	PowerShellTime		
50	PowerShellTime		
51	PowerShellTime		
52	PowerShellTime		
53	PowerShellTime		
54	PowerShellTime		
55	PowerShellTime		
56	PowerShellTime		
57	PowerShellTime		
58	PowerShellTime		
59	PowerShellTime		
60	PowerShellTime		
61	PowerShellTime		
62	PowerShellTime		
63	PowerShellTime		
64	PowerShellTime		
65	PowerShellTime		
66	PowerShellTime		
67	PowerShellTime		
68	PowerShellTime		
69	PowerShellTime		
70	PowerShellTime		
71	PowerShellTime		
72	PowerShellTime		
73	PowerShellTime		
74	PowerShellTime		
75	PowerShellTime		
76	PowerShellTime		
77	PowerShellTime		
78	PowerShellTime		
79	PowerShellTime		
80	PowerShellTime		
81	PowerShellTime		
82	PowerShellTime		
83	PowerShellTime		
84	PowerShellTime		
85	PowerShellTime		
86	PowerShellTime		
87	PowerShellTime		
88	PowerShellTime		
89	PowerShellTime		
90	PowerShellTime		
91	PowerShellTime		
92	PowerShellTime		
93	PowerShellTime		
94	PowerShellTime		
95	PowerShellTime		
96	PowerShellTime		
97	PowerShellTime		
98	PowerShellTime		
99	PowerShellTime		
100	PowerShellTime		

The information in this tab now needs to be manipulated with some formulas and copying (Edit Copy and Edit Paste Special Values- which is similar to a standard copy/paste except formulas are translated into their corresponding values).

By creating a worksheet that refers to the Users-DUMPACL sheet, a final row can be developed that refers to all of the required information needed.

Record	User	Fullname	AccDisabled	PwdExpireTime	PwdLastSetTime	LogonHours	LastLogonTime	RasDialin
1	Administrator	Administrator	✓					
2	Administrator	Administrator	✓					
3	Administrator	Administrator	✓					
4	Administrator	Administrator	✓					
5	Administrator	Administrator	✓					
6	Administrator	Administrator	✓					
7	Administrator	Administrator	✓					
8	Administrator	Administrator	✓					
9	Administrator	Administrator	✓					
10	Administrator	Administrator	✓					
11	Administrator	Administrator	✓					
12	Administrator	Administrator	✓					
13	Administrator	Administrator	✓					
14	Administrator	Administrator	✓					
15	Administrator	Administrator	✓					
16	Administrator	Administrator	✓					
17	Administrator	Administrator	✓					
18	Administrator	Administrator	✓					
19	Administrator	Administrator	✓					
20	Administrator	Administrator	✓					
21	Administrator	Administrator	✓					
22	Administrator	Administrator	✓		7/24/03 10:45 AM			
23	Administrator	Administrator	✓		7/24/03 10:45 AM			
24	Administrator	Administrator	✓		7/24/03 10:45 AM			
25	Administrator	Administrator	✓		7/24/03 10:45 AM			
26	Administrator	Administrator	✓		7/24/03 10:45 AM			
27	Administrator	Administrator	✓		7/24/03 10:45 AM			
28	Administrator	Administrator	✓		7/24/03 10:45 AM			
29	Administrator	Administrator	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	
30	Administrator	Administrator	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	
31	Administrator	Administrator	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	
32	Administrator	Administrator	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	
33	Administrator	Administrator	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
34	Administrator	Administrator	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
35	Administrator	Administrator	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
36	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
37	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
38	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
39	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
40	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
41	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
42	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
43	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
44	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
45	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
46	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
47	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
48	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
49	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
50	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
51	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
52	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
53	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
54	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
55	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
56	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes
57	Guest	Guest	✓		7/24/03 10:45 AM		1/29/06 9:17 AM	Yes

Each column's formula refers to the detail worksheet with the actual file from DUMPSEC in such a way that the line with Record = 1 has the complete information about the user as follows:

- A =IF(LEFT('Users-Full'!A37,1)<>"",1,"")
- B =IF(LEFT('Users-Full'!A36,1)<>"", 'Users-Full'!A36,B34)
- C =IF('Users-Full'!\$A36=C\$1, 'Users-Full'!\$B36,C34)
- D =IF('Users-Full'!\$A36=D\$1, 'Users-Full'!\$B36,D34)
- E =IF('Users-Full'!\$A36=E\$1, 'Users-Full'!\$B36,E34)
- F =IF('Users-Full'!\$A36=F\$1, 'Users-Full'!\$B36,F34)
- G =IF('Users-Full'!\$A36=G\$1, 'Users-Full'!\$B36,G34)
- H =IF('Users-Full'!\$A36=H\$1, 'Users-Full'!\$B36,H34)
- I =IF('Users-Full'!\$A36=I\$1, 'Users-Full'!\$B36,I34)

We can now simply copy the entire sheet, paste special values into a WorkArea sheet, and then sort on the Record column. The rows with the "1" will have all the user data required for analysis.

Another technique used here is to create duplicate worksheets with the same data. They are created in pairs. One that holds the raw information and is sorted in a particular sequence, and the other that points to the relevant information on an underlying sorted sheet. Each raw data sheet is then sorted into the sequence appropriate to the analysis being performed. This allows us to create very professional looking presentation sheets simply, quickly, and as a by-product (rather than an additional effort) of the analysis.

Four sets of sheets are created:

- User Statistics- all users are presented for review
- Disabled Users- to review those accounts that may require deletion
- Dial-In- To review user accounts that allow remote access to the network
- Password Age- To review the oldest accounts and consequently most susceptible to unauthorized access.

Each is created by copying the main user statistics sheet, sorting it into the appropriate sequence, and then limiting the printed document to the pertinent information.

Perform a similar analysis for the user groups. Open the Groups-col.txt file in Excel (using commas as delimiters). Create a sheet that points to the worksheet with the actual file from DUMPSEC. The columns and their formulas are as follows:

Group Type	=IF(LEFT('Groups-Full'!\$A4,1)<>" ",IF('Groups-Full'!\$C4="Global","Global",IF('Groups-Full'!\$C4="Local","Local","error")),A1)
Group Name	=IF(LEFT('Groups-Full'!\$A4,1)=" ",B1,'Groups-Full'!\$A4)
User	=IF(LEFT('Groups-Full'!\$A4,1)=" ",RIGHT('Groups-Full'!\$A4,LEN('Groups-Full'!\$A4)-3),""))
GroupName	=+A2&" - "&B2

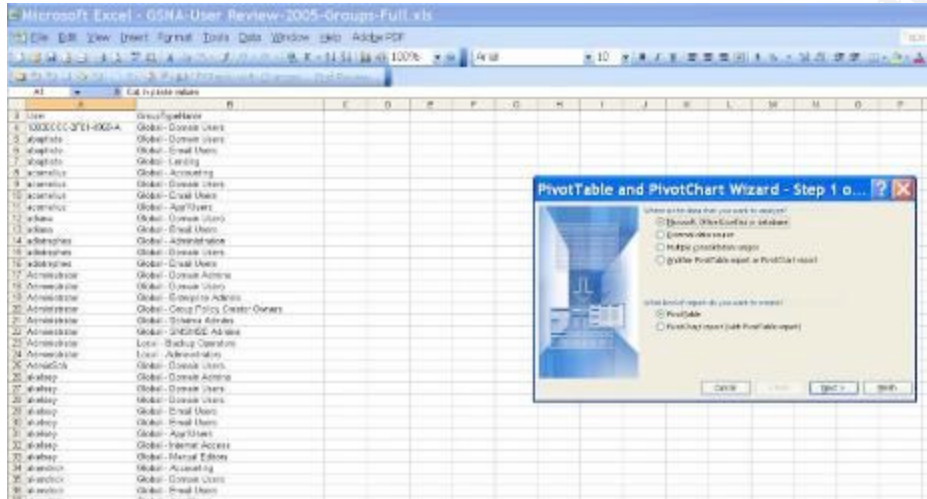
This creates two columns that contain the user and a grouptypename (which is the group type (“Local” or “Global” concatenated with the actual group name). This will allow for an Excel PivotTable function to be performed and the counts of each group to be easily calculated automatically. Cut and Paste Special Values the User and GroupTypeName columns into a worksheet, and then sort to get the blank user names out of the analysis. Using a presentation sheet, as before, makes a good management overview table.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS	AT	AU	AV	AW	AX	AY	AZ	BA	BB	BC	BD	BE	BF	BG	BH	BI	BJ	BK	BL	BM	BN	BO	BP	BQ	BR	BS	BT	BU	BV	BW	BX	BY	BZ	CA	CB	CC	CD	CE	CF	CG	CH	CI	CJ	CK	CL	CM	CN	CO	CP	CQ	CR	CS	CT	CU	CV	CW	CX	CY	CZ	DA	DB	DC	DD	DE	DF	DG	DH	DI	DJ	DK	DL	DM	DN	DO	DP	DQ	DR	DS	DT	DU	DV	DW	DX	DY	DZ	EA	EB	EC	ED	EE	EF	EG	EH	EI	EJ	ЕК	EL	EM	EN	EO	EP	EQ	ER	ES	ET	EU	EV	EW	EX	EY	EZ	FA	FB	FC	FD	FE	FF	FG	FH	FI	FJ	FK	FL	FM	FN	FO	FP	FQ	FR	FS	FT	FU	FV	FW	FX	FY	FZ	GA	GB	GC	GD	GE	GF	GG	GH	GI	GJ	GK	GL	GM	GN	GO	GP	GQ	GR	GS	GT	GU	GV	GW	GX	GY	GZ	HA	HB	HC	HD	HE	HF	HG	HH	HI	HJ	HK	HL	HM	HN	HO	HP	HQ	HR	HS	HT	HU	HV	HW	HX	HY	HZ	IA	IB	IC	ID	IE	IF	IG	IH	II	IJ	IK	IL	IM	IN	IO	IP	IQ	IR	IS	IT	IU	IV	IW	IX	IY	IZ	JA	JB	JC	JD	JE	JF	JG	JH	JI	IJ	JK	KL	KM	KN	KO	KP	KQ	KR	KS	KT	KU	KV	KW	KX	KY	KZ	LA	LB	LC	LD	LE	LF	LG	LH	LI	LJ	LK	LL	LM	LN	LO	LP	LQ	LR	LS	LT	LU	LV	LW	LX	LY	LZ	MA	MB	MC	MD	ME	MF	MG	MH	MI	MJ	MK	ML	MM	MN	MO	MP	MQ	MR	MS	MT	MU	MV	MW	MX	MY	MZ	NA	NB	NC	ND	NE	NF	NG	NH	NI	NJ	NK	NL	NM	NN	NO	NP	NQ	NR	NS	NT	NU	NV	NW	NX	NY	NZ	OA	OB	OC	OD	OE	OF	OG	OH	OI	OJ	OK	OL	OM	ON	OO	OP	OQ	OR	OS	OT	OU	OV	OW	OX	OY	OZ	PA	PB	PC	PD	PE	PF	PG	PH	PI	PJ	PK	PL	PM	PN	PO	PP	PQ	PR	PS	PT	PU	PV	PW	PX	PY	PZ	QA	QB	QC	QD	QE	QF	QG	QH	QI	QJ	QK	QL	QM	QN	QO	QP	QQ	QR	QS	QT	QU	QV	QW	QX	QY	QZ	RA	RB	RC	RD	RE	RF	RG	RH	RI	RJ	RK	RL	RM	RN	RO	RP	RQ	RR	RS	RT	RU	RV	RW	RX	RY	RZ	SA	SB	SC	SD	SE	SF	SG	SH	SI	SJ	SK	SL	SM	SN	SO	SP	SQ	SR	SS	ST	SU	SV	SW	SX	SY	SZ	TA	TB	TC	TD	TE	TF	TG	TH	TI	TJ	TK	TL	TM	TN	TO	TP	TQ	TR	TS	TT	TU	<th>TW</th> <th>TX</th> <th>TY</th> <th>TZ</th> <th>UA</th> <th>UB</th> <th>UC</th> <th>UD</th> <th>UE</th> <th>UF</th> <th>UG</th> <th>UH</th> <th>UI</th> <th>UJ</th> <th>UK</th> <th>UL</th> <th>UM</th> <th>UN</th> <th>UO</th> <th>UP</th> <th>UQ</th> <th>UR</th> <th>US</th> <th>UT</th> <th>UU</th> <th>UV</th> <th>UW</th> <th>UX</th> <th>UY</th> <th>UZ</th> <th>VA</th> <th>VB</th> <th>VC</th> <th>VD</th> <th>VE</th> <th>VF</th> <th>VG</th> <th>VH</th> <th>VI</th> <th>VJ</th> <th>VK</th> <th>VL</th> <th>VM</th> <th>VN</th> <th>VO</th> <th>VP</th> <th>VQ</th> <th>VR</th> <th>VS</th> <th>VT</th> <th>VU</th> <th>VV</th> <th>VW</th> <th>VX</th> <th>VY</th> <th>VZ</th> <th>WA</th> <th>WB</th> <th>WC</th> <th>WD</th> <th>WE</th> <th>WF</th> <th>WG</th> <th>WH</th> <th>WI</th> <th>WJ</th> <th>WK</th> <th>WL</th> <th>WM</th> <th>WN</th> <th>WO</th> <th>WP</th> <th>WQ</th> <th>WR</th> <th>WS</th> <th>WT</th> <th>WU</th> <th>WV</th> <th>WW</th> <th>WX</th> <th>WY</th> <th>WZ</th> <th>XA</th> <th>XB</th> <th>XC</th> <th>XD</th> <th>XE</th> <th>XF</th> <th>XG</th> <th>XH</th> <th>XI</th> <th>XJ</th> <th>XK</th> <th>XL</th> <th>XM</th> <th>XN</th> <th>XO</th> <th>XP</th> <th>XQ</th> <th>XR</th> <th>XS</th> <th>XT</th> <th>XU</th> <th>XV</th> <th>XW</th> <th>XX</th> <th>XY</th> <th>XZ</th> <th>YA</th> <th>YB</th> <th>YC</th> <th>YD</th> <th>YE</th> <th>YF</th> <th>YG</th> <th>YH</th> <th>YI</th> <th>YJ</th> <th>YK</th> <th>YL</th> <th>YM</th> <th>YN</th> <th>YO</th> <th>YP</th> <th>YQ</th> <th>YR</th> <th>YS</th> <th>YT</th> <th>YU</th> <th>YV</th> <th>YW</th> <th>YX</th> <th>YZ</th> <th>ZA</th> <th>ZB</th> <th>ZC</th> <th>ZD</th> <th>ZE</th> <th>ZF</th> <th>ZG</th> <th>ZH</th> <th>ZI</th> <th>ZJ</th> <th>ZK</th> <th>ZL</th> <th>ZM</th> <th>ZN</th> <th>ZO</th> <th>ZP</th> <th>ZQ</th> <th>ZR</th> <th>ZS</th> <th>ZT</th> <th>ZU</th> <th>ZV</th> <th>ZW</th> <th>ZX</th> <th>ZY</th> <th>ZZ</th> <th>AA</th> <th>AB</th> <th>AC</th> <th>AD</</th>	TW	TX	TY	TZ	UA	UB	UC	UD	UE	UF	UG	UH	UI	UJ	UK	UL	UM	UN	UO	UP	UQ	UR	US	UT	UU	UV	UW	UX	UY	UZ	VA	VB	VC	VD	VE	VF	VG	VH	VI	VJ	VK	VL	VM	VN	VO	VP	VQ	VR	VS	VT	VU	VV	VW	VX	VY	VZ	WA	WB	WC	WD	WE	WF	WG	WH	WI	WJ	WK	WL	WM	WN	WO	WP	WQ	WR	WS	WT	WU	WV	WW	WX	WY	WZ	XA	XB	XC	XD	XE	XF	XG	XH	XI	XJ	XK	XL	XM	XN	XO	XP	XQ	XR	XS	XT	XU	XV	XW	XX	XY	XZ	YA	YB	YC	YD	YE	YF	YG	YH	YI	YJ	YK	YL	YM	YN	YO	YP	YQ	YR	YS	YT	YU	YV	YW	YX	YZ	ZA	ZB	ZC	ZD	ZE	ZF	ZG	ZH	ZI	ZJ	ZK	ZL	ZM	ZN	ZO	ZP	ZQ	ZR	ZS	ZT	ZU	ZV	ZW	ZX	ZY	ZZ	AA	AB	AC	AD</
--	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	--	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	------

- Perform the Data PivotTable



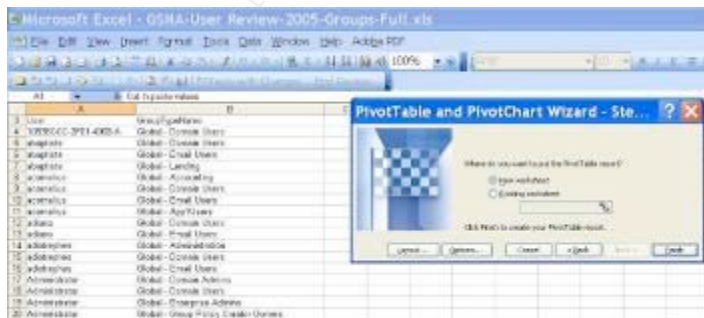
Data PivotTable



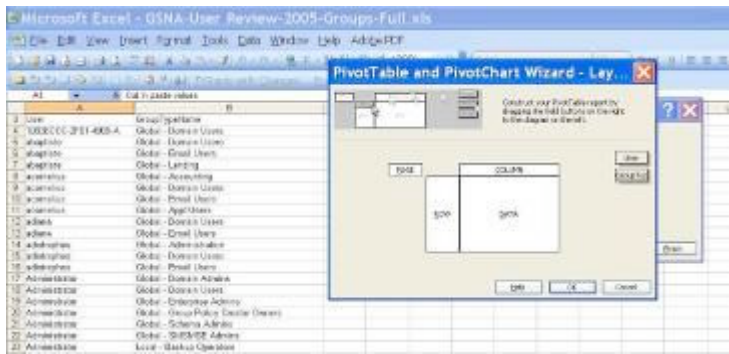
Next



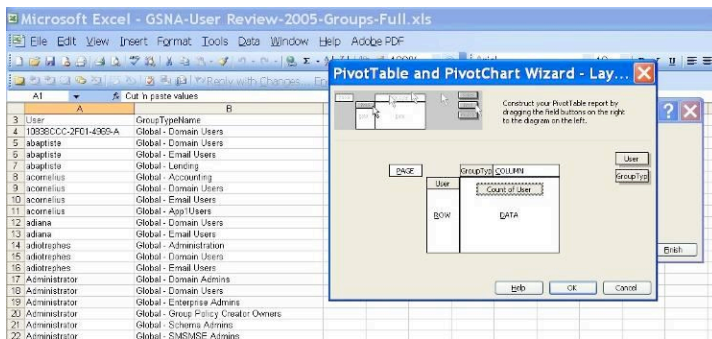
Highlight the data table, Next



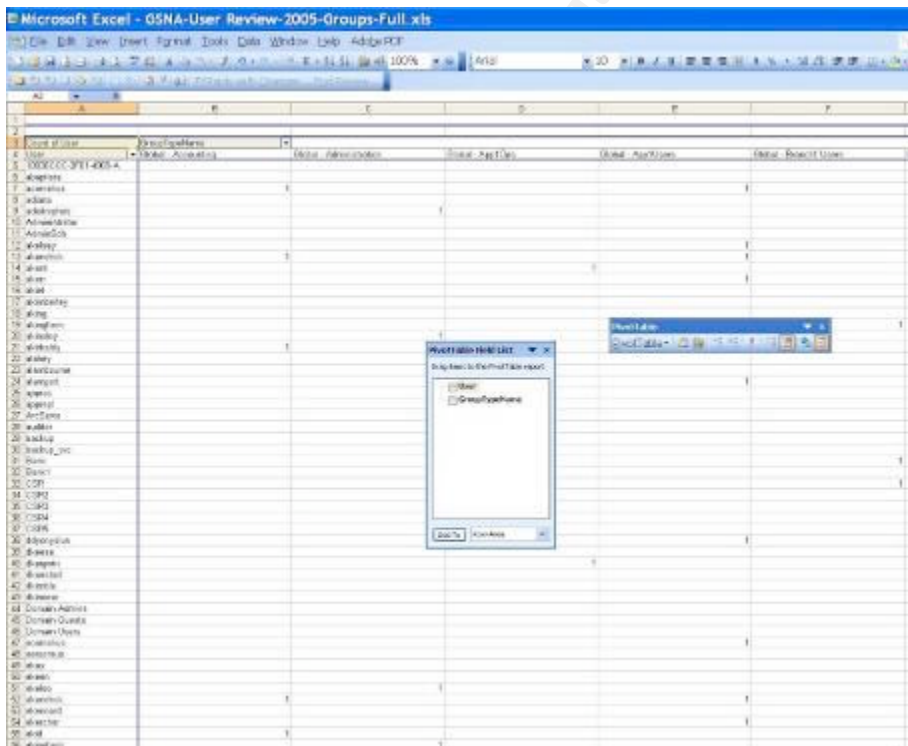
Select Layout



Click and drag the fields on the right to the table image:



OK



Data analysis couldn't be simpler, thanks to the Excel PivotTable !

AT	A	B	C	D	E	F	G	H	I	J
1										
2	Count of sites	23000000								
3	Count of sites	23000000								
4	Count of sites	23000000								
5	Count of sites	23000000								
6	Count of sites	23000000								
7	Count of sites	23000000								
8	Count of sites	23000000								
9	Count of sites	23000000								
10	Count of sites	23000000								
11	Count of sites	23000000								
12	Count of sites	23000000								
13	Count of sites	23000000								
14	Count of sites	23000000								
15	Count of sites	23000000								
16	Count of sites	23000000								
17	Count of sites	23000000								
18	Count of sites	23000000								
19	Count of sites	23000000								
20	Count of sites	23000000								
21	Count of sites	23000000								
22	Count of sites	23000000								
23	Count of sites	23000000								
24	Count of sites	23000000								
25	Count of sites	23000000								
26	Count of sites	23000000								
27	Count of sites	23000000								
28	Count of sites	23000000								
29	Count of sites	23000000								
30	Count of sites	23000000								
31	Count of sites	23000000								
32	Count of sites	23000000								
33	Count of sites	23000000								
34	Count of sites	23000000								
35	Count of sites	23000000								
36	Count of sites	23000000								
37	Count of sites	23000000								
38	Count of sites	23000000								
39	Count of sites	23000000								
40	Count of sites	23000000								
41	Count of sites	23000000								
42	Count of sites	23000000								
43	Count of sites	23000000								
44	Count of sites	23000000								
45	Count of sites	23000000								
46	Count of sites	23000000								
47	Count of sites	23000000								
48	Count of sites	23000000								
49	Count of sites	23000000								
50	Count of sites	23000000								
51	Count of sites	23000000								
52	Count of sites	23000000								

Date		A		B		C		D		E	
1	Building Fund										
2	Am Bank										
3	Groups										
4	Local - Accounting									Global - General Users	
5	Global - Administration									Global - Email Users	
6	Global - App Users									Global - App Users	
7	Global - Admin									Global - Admin	
8	Global - General Users									Global - General Users	
9	Global - General Admin									Global - General Admin	
10	Global - General Users									Global - General	
11	Global - General Users									Global - General Users	
12	Global - General Users									Global - Accounting	
13	Global - General Admin									Global - Admin Users	
14	Global - General Users									Global - App Users	
15	Global - General Admin									Global - Admin	
16	Global - General Users									Global - General Users	
17	Global - General Admin									Global - General Admin	
18	Global - General Users									Global - General Users	
19	Global - General Admin									Global - General Admin	
20	Global - General Users									Global - General Users	
21	Global - General Admin									Global - General Admin	
22	Global - General Users									Global - General Users	
23	Global - General Admin									Global - General Admin	
24	Global - General Users									Global - General Users	
25	Global - General Admin									Global - General Admin	
26	Global - General Users									Global - General Users	
27	Global - General Admin									Global - General Admin	
28	Global - General Users									Global - General Users	
29	Global - General Admin									Global - General Admin	
30	Global - General Users									Global - General Users	
31	Global - General Admin									Global - General Admin	
32	Global - General Users									Global - General Users	
33	Global - General Admin									Global - General Admin	
34	Global - General Users									Global - General Users	
35	Global - General Admin									Global - General Admin	
36	Global - General Users									Global - General Users	
37	Global - General Admin									Global - General Admin	
38	Global - General Users									Global - General Users	
39	Global - General Admin									Global - General Admin	
40	Global - General Users									Global - General Users	
41	Global - General Admin									Global - General Admin	
42	Global - General Users									Global - General Users	
43	Global - General Admin									Global - General Admin	
44	Global - General Users									Global - General Users	
45	Global - General Admin									Global - General Admin	
46	Global - General Users									Global - General Users	
47	Global - General Admin									Global - General Admin	
48	Global - General Users									Global - General Users	
49	Global - General Admin									Global - General Admin	
50	Global - General Users									Global - General Users	
51	Global - General Admin									Global - General Admin	
52	Global - General Users									Global - General Users	
53	Global - General Admin										

[illegible]

- Review the Disabled users to see how long they have been disabled (last login). Determine if the reason for the account's existence is legitimate. It should be understood that the existence of a disabled account, while potentially legitimate, needs to be reviewed (especially if it is given elevated rights of any kind). It would be possible to enable the account, perform activities under that account login, and then return the account to a seemingly innocuous disabled state. Also, the existence of too many disabled users might indicate an issue with the add/delete/change user account process that you may wish to investigate.
- Review the Dial-in accounts and their last login in light of the organization's Remote Access policy. Determine if there is a legitimate reason for the account and if the last login seems reasonable. These accounts allow remote access to the network (thus extending the network beyond its physical borders). Again, if elevated rights exist in combination with Dial-In, the account should be scrutinized.
- Review the password age and analyze the last login in light of the organization's password change policy. Determine if it appears to comply with policy and if any anomalies exist.
- Finally, review the entire account list (usually in conjunction with the group analysis). This review is usually best done in conjunction with an operational manager, familiar with the employee population. Review the log on hours at this time, as well.
- Review the members of the groups with elevated security permissions, like Domain Admins and Enterprise Admins. Insure they are, indeed, authorized the associated access.
- Review the need for the number of accounts with high-level authorization. Most organizations have far too many Administrative-level accounts.

3.2 Review Group Policy Objects and assignment

Group Policy Objects (GPO) are a very powerful configuration structure. They allow policies of all types to be applied to Active Directory Organizational Units (OU). This means that groups or classes of users and workstations can have policies set so that each individual object doesn't need to be fully configured itself. It can merely be associated with an OU that has a GPO set for it. Prior to Windows 2003, it was very difficult to audit GPOs since they are cumulative in effect. A particular user logging on to a particular workstation could have GPOs applied from the OU of the user (and the GPO of any parent container of that user OU) and a GPO from the OU of the workstation (and the GPO of any parent container of that workstation OU). With the introduction of Windows XP and 2003, Microsoft simplified this task by including the Group Policy Management Console.

The Group Policy Management Console (GPMC) is a Microsoft Management Console (MMC) snap-in and provides a single solution for managing all Group Policy-related activities. It also includes a set of "scriptable" interfaces for automating GPO tasks.

The good news is that it also works with Windows 2000. It does, however, require a Windows XP or 2003 machine to run the GPMC snap-in. The only limitation is that the advanced modeling feature is not available on Windows 2000. This means that any user that has already logged on to a workstation can have the resultant GPO reviewed on a Windows 2000 machine. Modeling can be used in Windows 2003 to see the resultant GPO set that would be applied if a particular user logged on to a particular computer- a very powerful auditing tool.

From the GPMC help file is a simple description of this powerful tool:

New ways to do familiar tasks

The following table lists common Group Policy tasks. Using Group Policy Management Console (GPMC), the procedures for performing these tasks are different from the way you performed these tasks in the past, without the Group Policy Management snap-in. Previously Administrators used Active Directory Users and Computers and Active Directory Sites and Services to manage Group Policy. Now you use GPMC to perform all Group Policy-related tasks.

If you want to	On a computer without GPMC	With Group Policy Management snap-in
Create a Group Policy object (GPO) and a link to it	On the Group Policy tab for a site, domain, or organizational unit, click New .	In GPMC, right-click the relevant site, domain, or organizational unit and then click Create and link a GPO here . For more information, see Create or delete a Group Policy object and Link a Group Policy object.
Create an unlinked GPO	Navigate to the Group Policy properties tab for a site, domain, or organizational unit, click Add . On the All tab, right-click, and then click New .	In GPMC, navigate to Group Policy Objects , right-click it, and then click New . For more information, see Create or delete a Group Policy object.
Edit a GPO	Navigate to the Group Policy properties tab for a site, domain, or organizational unit, select the GPO, and then click Edit . This opens Group Policy Object Editor.	In GPMC, navigate to Group Policy Objects , right-click the GPO, and then click Edit . For more information, see Edit a Group Policy object.

• Group Policy Object Editor MMC snap-in

		is still used to edit GPOs and is opened when you click Edit in GPMC.
Link an existing GPO to a site, domain, or organizational unit	Navigate to the Group Policy properties tab for a site, domain, or organizational unit, click Add , and then select a GPO.	In GPMC, navigate to a site, domain, or organizational unit, right-click it, and then click Link an existing GPO here . For more information, see Link a Group Policy object.
Use security groups to filter the scope of policy	Edit the access control entry (ACE) permission option for Apply Group Policy on the Security tab in the Properties dialog box for the GPO.	In GPMC, click a GPO or GPO Link, select the Scope tab, and then use the Add and Remove buttons to control the groups, users, and computers on which the GPO applies. For more information, see Filter using security groups.
Delegate permissions on GPOs	Navigate to the properties of a GPO, click Permissions for Authenticated Users , and select the check boxes that correspond to the permissions you want to give.	In GPMC, click the GPO, click the Delegation tab, and then click the Add or Remove buttons. For more information, see Delegate Group Policy tasks.
Determine Resultant Set of Policy with Group Policy Results (logging mode)	In Resultant Set of Policy snap-in, right-click Resultant Set of Policy , and then click Generate RSoP Data . Select Logging Mode in the Resultant Set of Policy Wizard.	In GPMC, right-click Group Policy Results , and then click Group Policy Results Wizard . For more information, see Determine Resultant Set of Policy with Group Policy Results.
Simulate Resultant Set of Policy using Group Policy Modeling	In Resultant Set of Policy snap-in, right-click Resultant Set of Policy , and then click Generate RSoP Data . Select Planning Mode in the Resultant Set of Policy Wizard.	In GPMC, right-click Group Policy Modeling , and then click Group Policy Modeling Wizard . For more information, see Simulate Resultant Set of Policy using Group Policy Modeling.
Add a WMI filter	Navigate to the Properties of a Group Policy object, and click the WMI Filter tab.	In GPMC, right-click WMI Filters and click New . For more information, see Create, import, export, copy, and paste WMI filters.

11

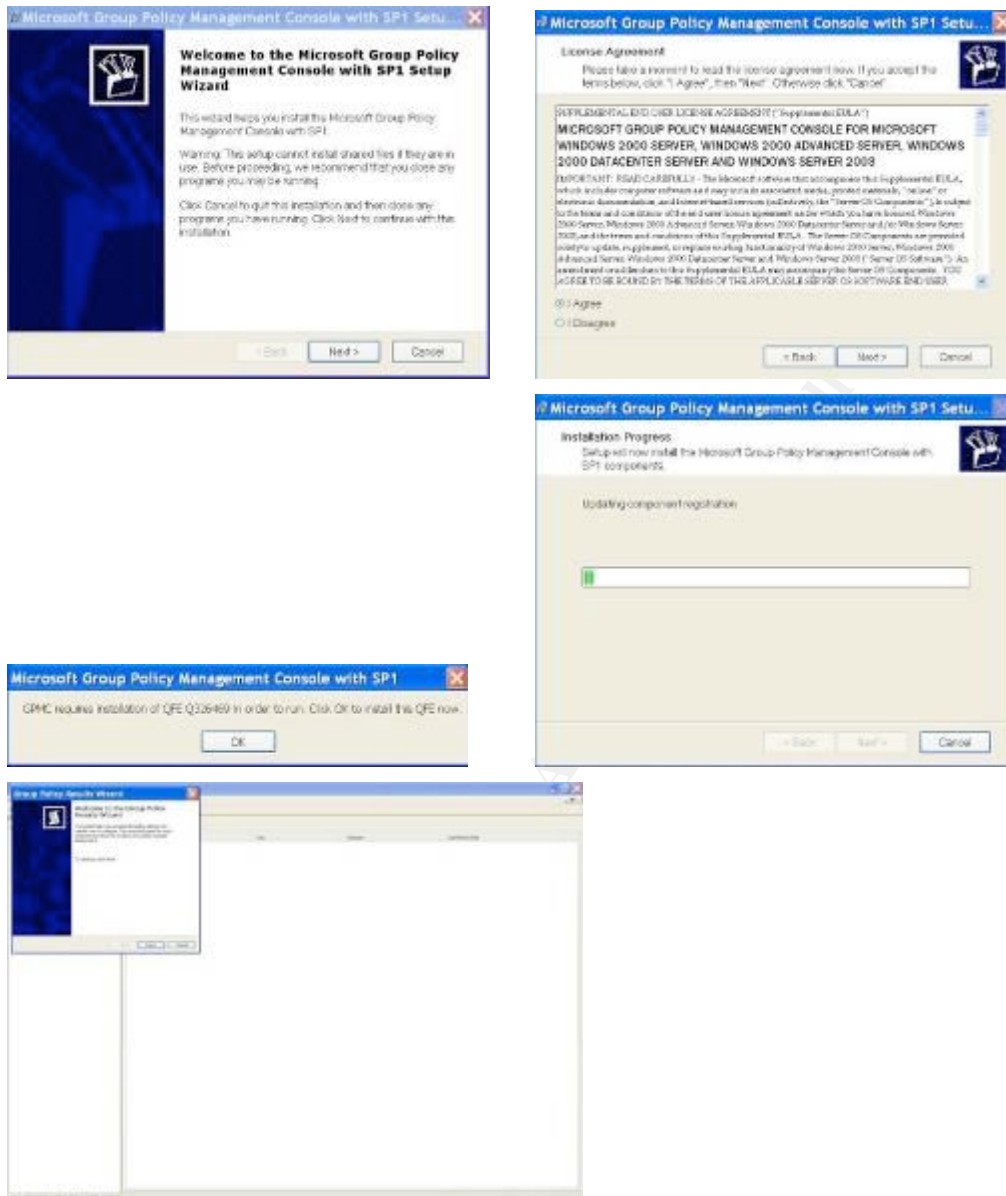
A review of the GPO applied to selected users at selected workstations can be undertaken using the following steps:

- Use the GPMC to access the user and workstation
- Print the result for documentation of the test
- Analyze the resultant GPOs applied in the area of concern (security, internet access, etc.)
- Report on any suspicious areas

Preparation:

- Use a workstation or laptop with network access to the domain with Windows XP installed.
- Select the representative users and workstations to be reviewed. This selection should be from selected groups of users. The intent is to see if a user with restricted network access has the correct GPOs applied.
- Download and install GPMC from the Microsoft site (certain XP service packs may be required prior to installation):

11 Microsoft Corporation, Group Policy Management Console- Help Text



Data Collection:

- Start GPMC (version 1.0.2 used here)
- Select the Domain
- Select a user and a workstation
- Save the resultant file

- Print and review the output (display with browser):

Default Settings Policy				Index of
General				Index
General				100
<p>Policy Name: General</p> <p>Policy ID: 100</p> <p>Policy Description: General settings for the system.</p> <p>Policy Status: Enabled</p> <p>Policy Owner: System Administrator</p> <p>Policy Version: 1.0</p> <p>Policy Last Modified: 11/02/2025 11:02 AM</p>				
Settings				101
Location	Address	Link Status	Path	
100	100	100	100	
<p>The link status is the status of the link.</p> <p>The path is the path to the link.</p>				
Security Settings				102
<p>The settings in the GPO can only apply to the following groups, users, and computers.</p> <p>Group: Group Name</p> <p>User: User Name</p> <p>Computer: Computer Name</p>				
Link Filtering				103
Link Filter Name	Link Filter Description	Link Filter Status	Link Filter Path	
100	100	100	100	
Link Filtering				104
<p>These groups and users have the specified permission for the GPO.</p> <p>Group: Group Name</p> <p>User: User Name</p> <p>Computer: Computer Name</p>				
Computer Configuration (Enabled)				105
System Settings				106
Security Settings				107
Account Policies/Password Policy				108
Policy	Setting	Value	Link	
100	100	100	100	
<p>Policy Name: Password Policy</p> <p>Policy ID: 100</p> <p>Policy Description: Password policy for the system.</p> <p>Policy Status: Enabled</p> <p>Policy Owner: System Administrator</p> <p>Policy Version: 1.0</p> <p>Policy Last Modified: 11/02/2025 11:02 AM</p>				
Account Policies/Maximum Password Age				109
Policy	Setting	Value	Link	
100	100	100	100	
<p>Policy Name: Maximum Password Age</p> <p>Policy ID: 100</p> <p>Policy Description: Maximum password age for the system.</p> <p>Policy Status: Enabled</p> <p>Policy Owner: System Administrator</p> <p>Policy Version: 1.0</p> <p>Policy Last Modified: 11/02/2025 11:02 AM</p>				
Account Policies/Maximum Password Age				110
Policy	Setting	Value	Link	
100	100	100	100	
<p>Policy Name: Maximum Password Age</p> <p>Policy ID: 100</p> <p>Policy Description: Maximum password age for the system.</p> <p>Policy Status: Enabled</p> <p>Policy Owner: System Administrator</p> <p>Policy Version: 1.0</p> <p>Policy Last Modified: 11/02/2025 11:02 AM</p>				
Account Policies/Maximum Password Age				111
Policy	Setting	Value	Link	
100	100	100	100	
<p>Policy Name: Maximum Password Age</p> <p>Policy ID: 100</p> <p>Policy Description: Maximum password age for the system.</p> <p>Policy Status: Enabled</p> <p>Policy Owner: System Administrator</p> <p>Policy Version: 1.0</p> <p>Policy Last Modified: 11/02/2025 11:02 AM</p>				
Account Policies/Maximum Password Age				112
Policy	Setting	Value	Link	
100	100	100	100	
<p>Policy Name: Maximum Password Age</p> <p>Policy ID: 100</p> <p>Policy Description: Maximum password age for the system.</p> <p>Policy Status: Enabled</p> <p>Policy Owner: System Administrator</p> <p>Policy Version: 1.0</p> <p>Policy Last Modified: 11/02/2025 11:02 AM</p>				
Account Policies/Maximum Password Age				113
Policy	Setting	Value	Link	
100	100	100	100	
<p>Policy Name: Maximum Password Age</p> <p>Policy ID: 100</p> <p>Policy Description: Maximum password age for the system.</p> <p>Policy Status: Enabled</p> <p>Policy Owner: System Administrator</p> <p>Policy Version: 1.0</p> <p>Policy Last Modified: 11/02/2025 11:02 AM</p>				
Account Policies/Maximum Password Age				114
Policy	Setting	Value	Link	
100	100	100	100	
<p>Policy Name: Maximum Password Age</p> <p>Policy ID: 100</p> <p>Policy Description: Maximum password age for the system.</p> <p>Policy Status: Enabled</p> <p>Policy Owner: System Administrator</p> <p>Policy Version: 1.0</p> <p>Policy Last Modified: 11/02/2025 11:02 AM</p>				
Account Policies/Maximum Password Age				115
Policy	Setting	Value	Link	
100	100	100	100	
<p>Policy Name: Maximum Password Age</p> <p>Policy ID: 100</p> <p>Policy Description: Maximum password age for the system.</p> <p>Policy Status: Enabled</p> <p>Policy Owner: System Administrator</p> <p>Policy Version: 1.0</p> <p>Policy Last Modified: 11/02/2025 11:02 AM</p>				
Account Policies/Maximum Password Age				116
Policy	Setting	Value	Link	
100	100	100	100	
<p>Policy Name: Maximum Password Age</p> <p>Policy ID: 100</p> <p>Policy Description: Maximum password age for the system.</p> <p>Policy Status: Enabled</p> <p>Policy Owner: System Administrator</p> <p>Policy Version: 1.0</p> <p>Policy Last Modified: 11/02/2025 11:02 AM</p>				
Account Policies/Maximum Password Age				117
Policy	Setting	Value	Link	
100	100	100	100	
<p>Policy Name: Maximum Password Age</p> <p>Policy ID: 100</p> <p>Policy Description: Maximum password age for the system.</p> <p>Policy Status: Enabled</p> <p>Policy Owner: System Administrator</p> <p>Policy Version: 1.0</p> <p>Policy Last Modified: 11/02/2025 11:02 AM</p>				
Account Policies/Maximum Password Age				118
Policy	Setting	Value	Link	
100	100	100	100	
<p>Policy Name: Maximum Password Age</p> <p>Policy ID: 100</p> <p>Policy Description: Maximum password age for the system.</p> <p>Policy Status: Enabled</p> <p>Policy Owner: System Administrator</p> <p>Policy Version: 1.0</p> <p>Policy Last Modified: 11/02/2025 11:02 AM</p>				
Account Policies/Maximum Password Age				119
Policy	Setting	Value	Link	
100	100	100	100	
<p>Policy Name: Maximum Password Age</p> <p>Policy ID: 100</p> <p>Policy Description: Maximum password age for the system.</p> <p>Policy Status: Enabled</p> <p>Policy Owner: System Administrator</p> <p>Policy Version: 1.0</p> <p>Policy Last Modified: 11/02/2025 11:02 AM</p>				
Account Policies/Maximum Password Age				120
Policy	Setting	Value	Link	
100	100	100	100	
<p>Policy Name: Maximum Password Age</p> <p>Policy ID: 100</p> <p>Policy Description: Maximum password age for the system.</p> <p>Policy Status: Enabled</p> <p>Policy Owner: System Administrator</p> <p>Policy Version: 1.0</p> <p>Policy Last Modified: 11/02/2025 11:02 AM</p>				
Account Policies/Maximum Password Age				121
Policy	Setting	Value	Link	

This is an example of the format of the output from the tool. The actual result will contain the GPOs applied to the particular user and computer being reviewed. It is important to understand the sections specific to your purpose. In this particular case we are reviewing the Account Policies being applied.

A review of the resultant output should include looking for any delegated administrative control or elevated rights (allowing the ability to enable and disable GPO inheritance). Look for anything that blocks policy inheritance also. If a mis-configuration, or intentional deny of policy inheritance exists, it may allow a user to perform actions that the higher-level Group Policy is preventing. This is a double negative: we want to insure that the policy is being applied to the lower level object, therefore we want to make sure the policy inheritance is not denied.

© SANS Institute 2005, Author retains full rights.

3.3 Review Password Strength

There are several tools available to assess password strength. @Stake's L0phtCrack™ and Open Source John the Ripper are two very popular password "cracking" programs. It is essential that it is understood that the legitimate uses of these two programs are twofold:

- Assess password strength so that the result may be documented, compared to the organization's policy, and appropriate remediation steps put into action.
- Recover lost or unavailable passwords when no other alternative method is possible.

@Stake's LC4 was used for this testing (LC5 is the current version). In addition, there are basically two options for assessing password strength. The program can be set to run against the Windows Domain Controller directly, passwords can be captured by "sniffing" on the network, or the "SAM" file (Windows Security Accounts Manager file) can be captured with a utility program (pwdump3) and assessed offline. *Regardless of the method used, it must be assumed that the passwords have been compromised and appropriate actions taken.* The utility program is method in the testing process used here.

A review of the password strength can be undertaken using the following steps:

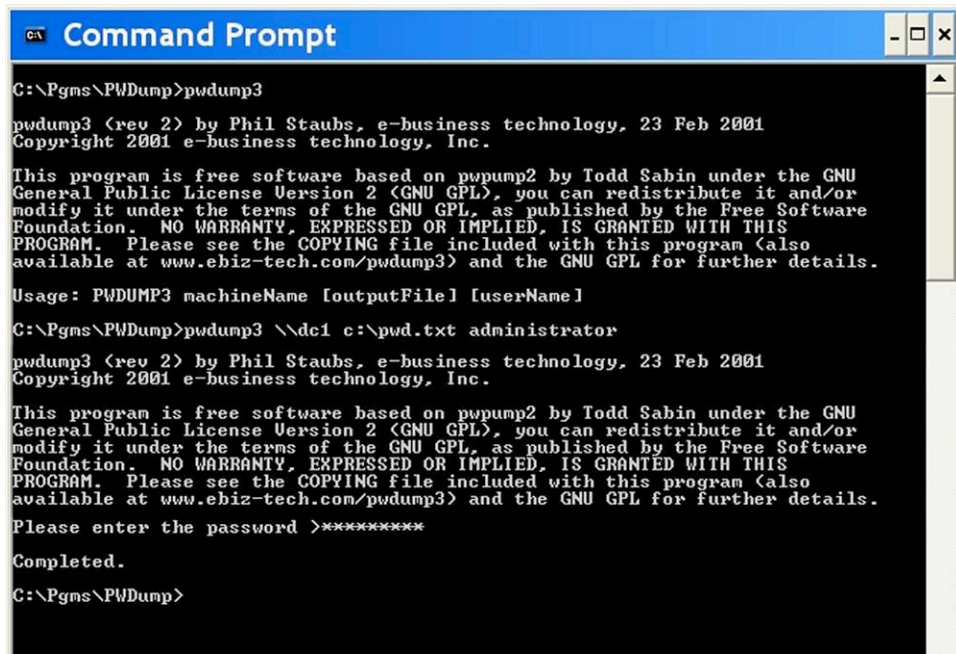
- Review the organization's Password Policy (if it exists)
- Use a tool (pwdump3) to capture SAM file from a Domain Controller
- Use a stand-alone computer with L0phtCrack™ installed to perform the password vulnerability assessment
- Export the resultant "cracked" file
- Organize the output for ease of analysis
- Prepare presentation of user list with "cracking statistics"
- Prepare summary presentation of "cracking statistics"

Preparation:

- Use a workstation or laptop with network access to a Domain Controller
- A Domain Administrator's account and password must be available for the utility used to capture the SAM file.
- A secured method of transport and, preferably, a secured stand-alone workstation with the L0phtCrack™ program installed should be used for password vulnerability testing.
- Download the pwdump3 utility
- Insure a copy of Microsoft Excel is available for the analysis of collected data
- A fairly advanced knowledge of Excel (or a staff member who can assist) is very helpful.

Data Collection:

- Run pwdump3 as follows. The resultant file in this example is pwd.txt in the root of C:\



```
C:\Pgms\PWDump>pwdump3

pwdump3 (rev 2) by Phil Staubs, e-business technology, 23 Feb 2001
Copyright 2001 e-business technology, Inc.

This program is free software based on pwpump2 by Todd Sabin under the GNU
General Public License Version 2 (GNU GPL), you can redistribute it and/or
modify it under the terms of the GNU GPL, as published by the Free Software
Foundation. NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS
PROGRAM. Please see the COPYING file included with this program (also
available at www.ebiz-tech.com/pwdump3) and the GNU GPL for further details.

Usage: PWDUMP3 machineName [outputFile] [userName]

C:\Pgms\PWDump>pwdump3 \\\\dc1 c:\\pwd.txt administrator

pwdump3 (rev 2) by Phil Staubs, e-business technology, 23 Feb 2001
Copyright 2001 e-business technology, Inc.

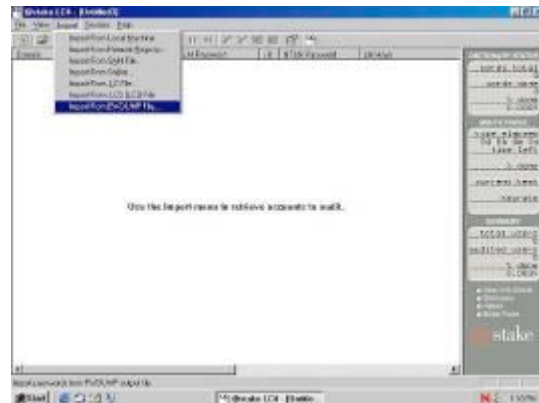
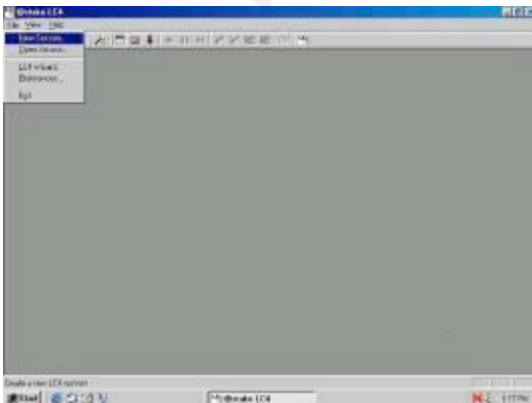
This program is free software based on pwpump2 by Todd Sabin under the GNU
General Public License Version 2 (GNU GPL), you can redistribute it and/or
modify it under the terms of the GNU GPL, as published by the Free Software
Foundation. NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS
PROGRAM. Please see the COPYING file included with this program (also
available at www.ebiz-tech.com/pwdump3) and the GNU GPL for further details.

Please enter the password >*****

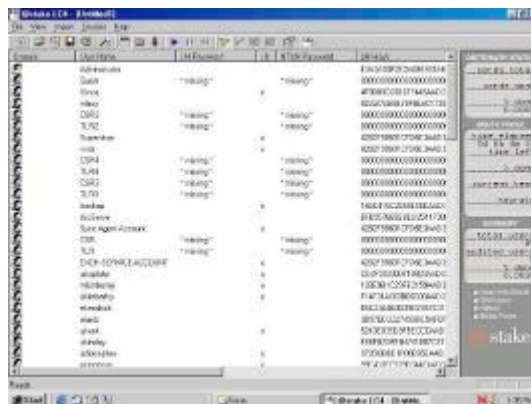
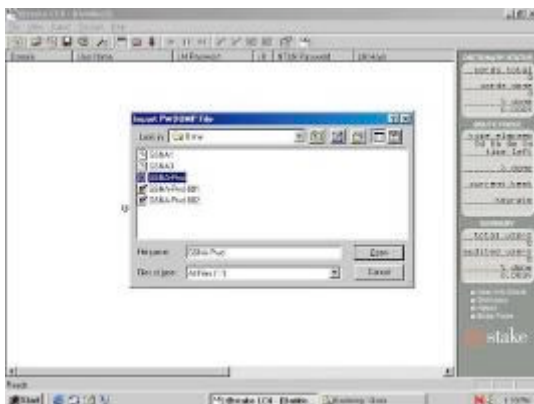
Completed.

C:\Pgms\PWDump>
```

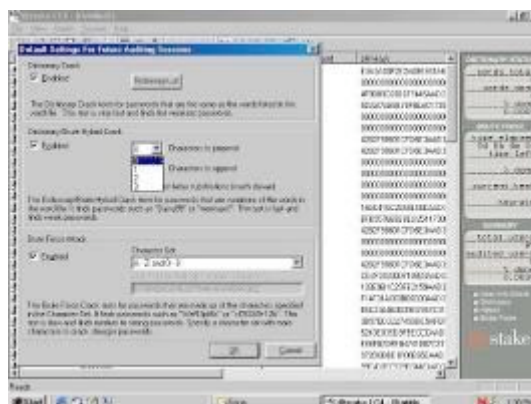
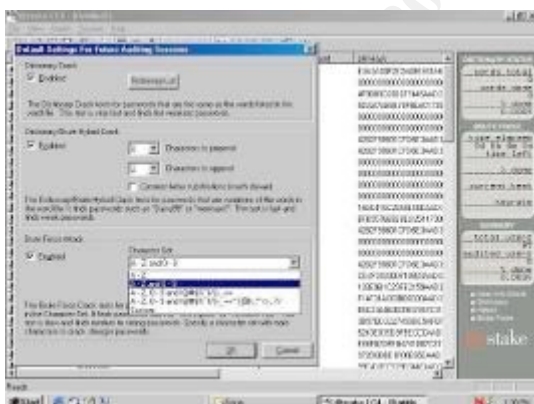
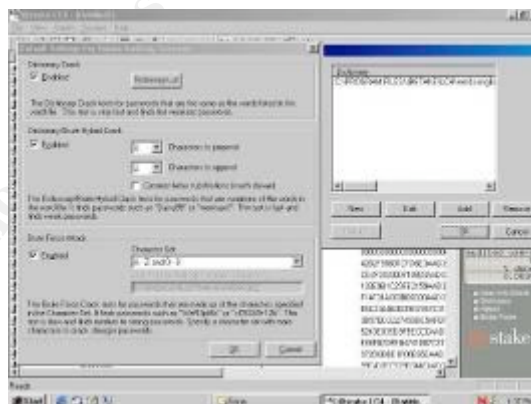
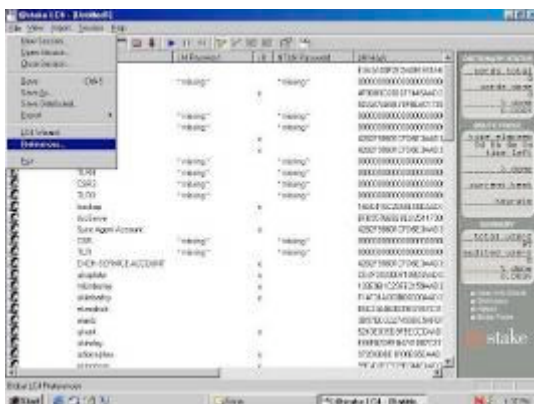
- NOTE: If the program fails, the most common reason is that the administrative share (ADMIN\$) has been disabled. Several “workarounds” exist (including creating the share, running the program, and deleting the share), but are outside the scope of this document.
- Secure the file (in a password protected zip file, for example), delete it from the local machine, and transport it to the computer where the L0pht program will be run.
- Place the file on the L0pht computer and Begin a new session



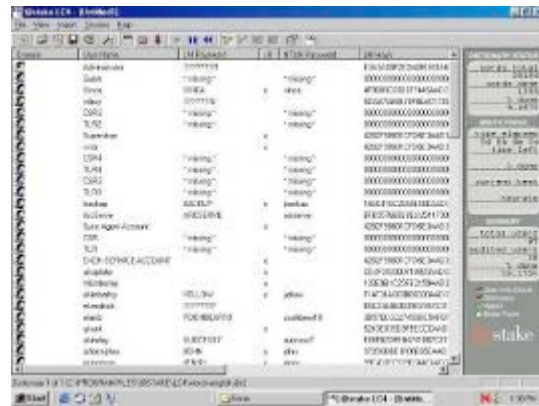
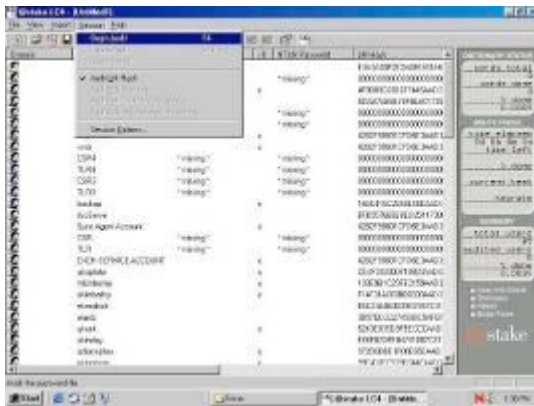
- Import the file



- Set the session preferences. Here is where you can try different settings to see how they affect the speed and cracking capabilities of the program.



- Begin the Audit

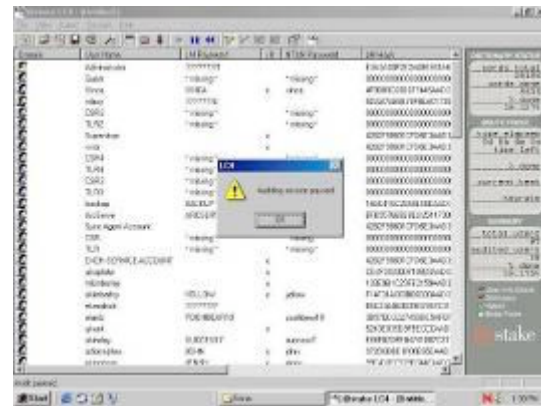
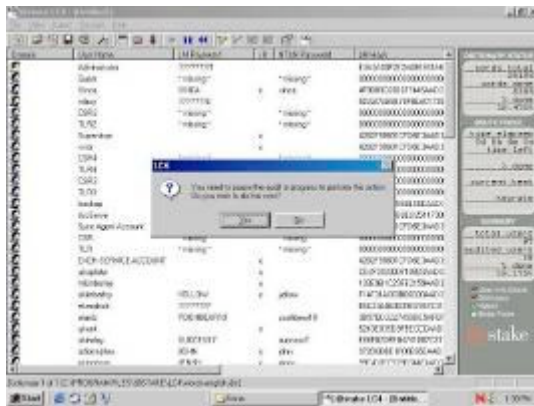


© SANS Institute 2005, Author retains full

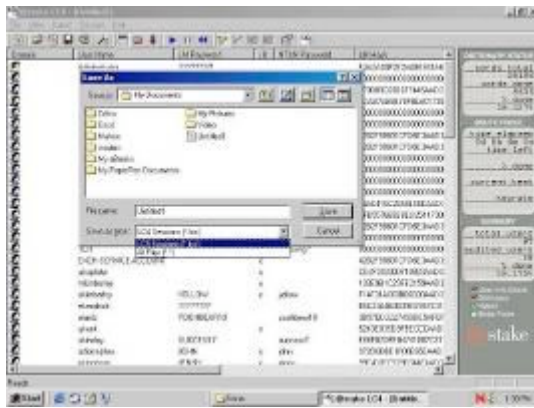
- Scroll up and down until the majority of the passwords have been cracked, or the time permitted has been reached (this one ran for approximately 4 days):



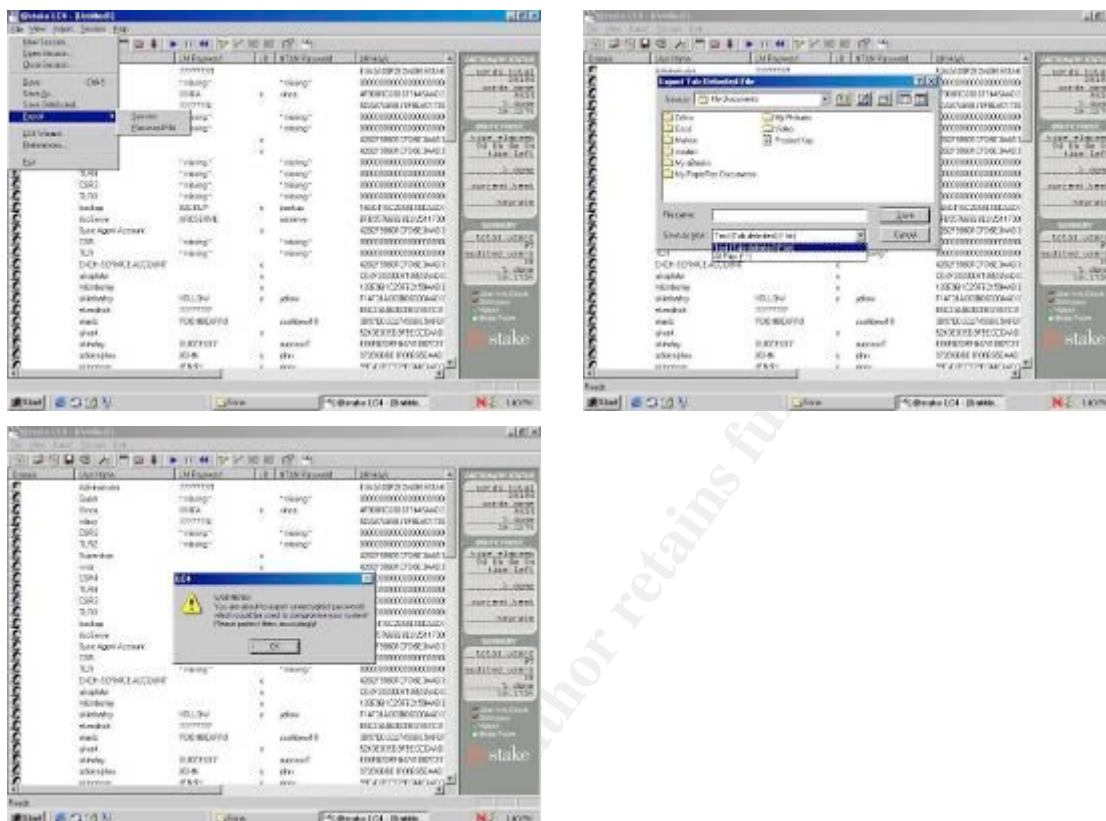
- “File Save As” will prompt to pause the session.



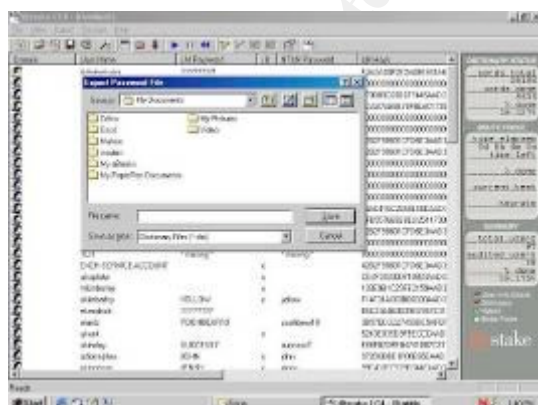
- This will save the session as it exists (to allow a restart).



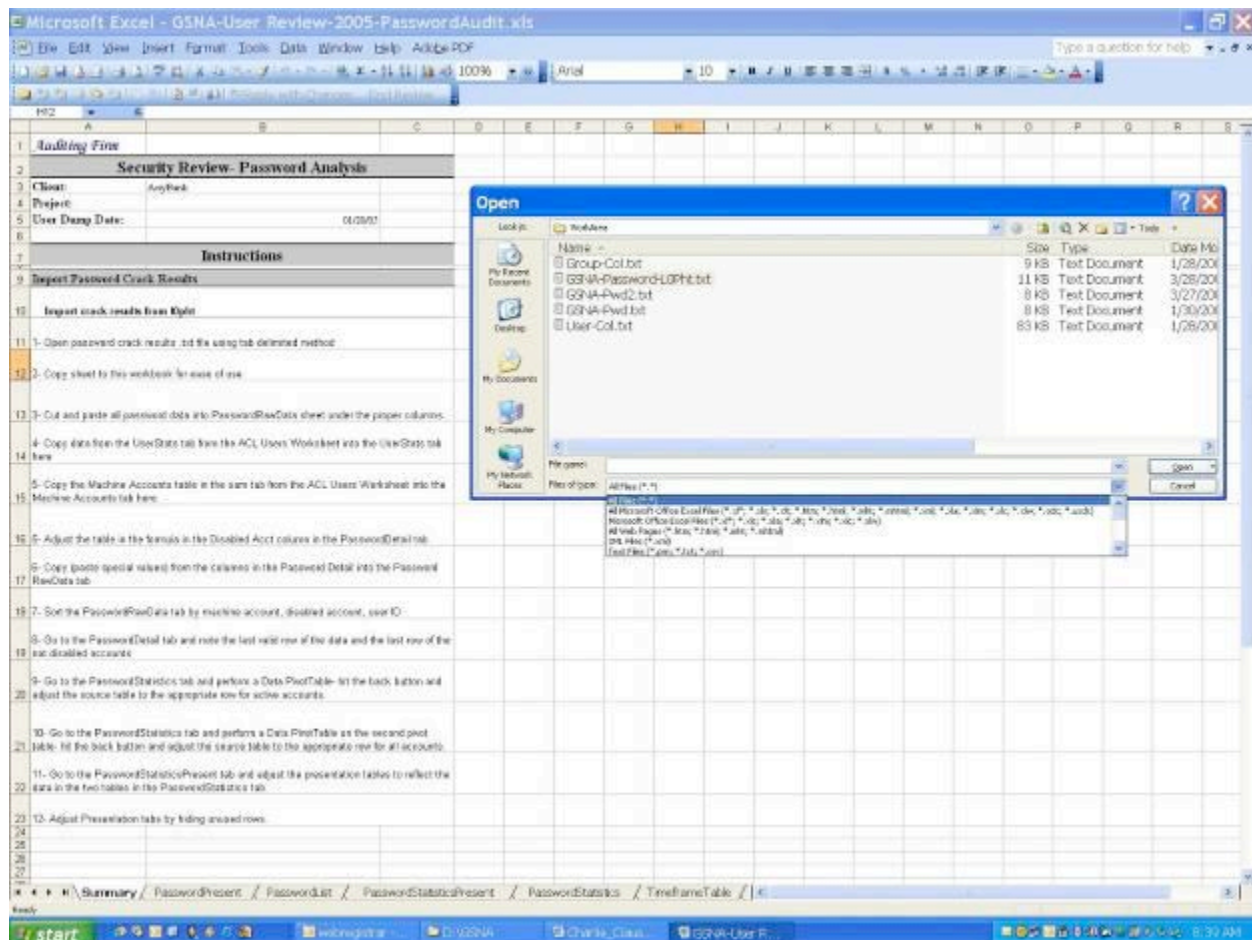
- “File Export Session” will present the same prompts to pause the session, and allow the results of the session to be saved in a txt file for analysis:



- “File Export Password File” will present the same prompts to pause the session, and allow the results of the session to be saved as a dictionary file for later use in sources for password cracking:



- Import the password file into an Excel spreadsheet.



The results can be analyzed using several techniques. A summary of the number of passwords cracked by each method is an impressive presentation for management. It really shows the results in a meaningful way. In order to do this, each account's time to crack should be categorized in groups similar to the following:

- Page 36 of 65

- h- 3-4 days
- i- 4-5 days
- j- 5-6 days
- k- 6-7 days
- l- over 7 days

Combine this with the L0pht categories of cracking:

- Brute Force
- Dictionary
- Hybrid
- User Info
- Not Cracked

And a table of meaningful results can be presented:

	A	B	C	D	E	F	G	H
1	<i>Auditing Firm</i>						01/28/05	
2	AnyBank							
3	Password Cracking Statistics							
4								
5	All User Accounts							
6	Crack Method							
7	TimeFrame	Brute Force	Dictionary	Hybrid	User Info	N/A	Grand Total	
8	N/A							
9	a- Under 1 minute							
10	b- Under 1 hour							
11	c- Under 4 hours							
12	d- Under 8 hours							
13	e- Under 24 hours							
14	f- 1-2 days							
15	g- 2-3 days							
16	h- 3-4 days							
17	i- 4-5 days							
18	j- 5-6 days							
19	k- 6-7 days							
20	l- over 7 days							
21	Grand Total							
28								
29								
30								

© SANS Ins

The detailed user list can be presented as follows:

Auditing Firm					
A	B	C	D	I	J
1	Auditing Firm				
2	AnyBank				
3	Password List				
5	Seq	Username	LANMAN Password	Less Than Eight	Method
6	1	Administrator	PASSWORD		Hybrid
7	2	mlacy	PECANPIE		Brute Force
8	3	ArcServe	ARCserve		User Info
9	4	akiel	LEE12134		Brute Force
10	5	backup	BACKUP	x	User Info
11	6	backup_svc	REFIP	x	Brute Force
12	7	ekay	DAISY	x	Dictionary
13	8	eerasmus	TRUSTY	x	Dictionary
14	9	ekipp	PS14310	x	Brute Force
15	10	ekinghorn	JENNY	x	Dictionary
16	11	mkinston	HARLEY	x	Dictionary
17	12	mkimberley	CONRS	x	Brute Force
18	13	adiana	MUFFIN	x	Dictionary
19	14	ekercher	PASSWORD		Dictionary
20	15	ekennard	BLIZZARD		Dictionary
21	16	CSR	* missing *		N/A
22	17	CSR2	* missing *		N/A
23	18	CSR3	* missing *		N/A
24	19	CSR4	* missing *		N/A
25	20	CSR5	* missing *		N/A
26	21	mdiodorus	PSALM333		Hybrid
27	22	dkeese	CORABA	x	Brute Force
28	23	eken	DIANE	x	Dictionary
29	24	mkierman	WINTER	x	Dictionary
30	25	akerr	OUTBACK	x	Brute Force
31	26	akent	DSKDSK4	x	Brute Force
32	27	mkennicot	CLOCKS	x	Brute Force
33	28	mkinsley	PASSWORD		Dictionary
34	29	ddyonysius	SNOWMOBILE		Dictionary
35	30	akinghorn	BOZOB	x	Brute Force
36	31	mkelly	GIRLY	x	Brute Force
37	32	emailad	TRUSTY	x	Dictionary
38	33	emaildump	EMAILDUMP		User Info
39	34	adiotrephe	JOHN	x	Dictionary
40	35	exch-backup-agent	PASSWORD		Hybrid
41	36	exch-nav-agent	REFIP	x	Brute Force
42	37	EXCH-SERVICE-ACCOUNT	REFIP	x	Brute Force
43	38	aking	STUPID381		Hybrid
44	39	Bank	HSB	x	User Info
45	40	Bank1	HSB1	x	User Info
46	41	finloan	HSBLOAN	x	User Info
47	42	Internal	* missing *		N/A
48	43	alambourne	ZANEA	x	Brute Force
49	44	mkirkaldy	HOLIDAYS		Dictionary
50	45	mkinsley	HUNTING	x	Dictionary
51	46	mkent	GRACIE	x	Brute Force
52	47	dkinnear	KIOSK	x	User Info
53	48	mkimberley	LIPPY	x	Brute Force
54	49	abaptiste	120665	x	Brute Force

The table combined with the user list allows the auditor to review the actual password cracking times against the password policy to see if the organizations' security goals are being met. In addition, this review, combined with the user and group review above allows the auditor to review the highest risk group (usually Domain and Enterprise Admins) in more detail.

4: Audit

The results presented here are from an actual review of a financial institution's Active Directory Domain. All domain names, users, groups and other identifying characteristics have been changed (a considerable effort), but recommendations have been developed based on the results shown here.

4.1 Review User Accounts and Groups

The DUMPACL utility was used to create a user-col.txt and group-col.txt file from the Domain Controller following the steps outlined in 3.1. The detailed results are as follows:

DumpACL - Summary of Group Policy Objects (GPOs) - Summary									
Group Policy Objects (GPOs)									
1	Group	Administrators (Local)							
2	Group	Domain Admins (Global)							
3	Group	Domain Users (Global)							
4	Group	Domain Computers (Global)							
5	Group	Domain Controllers (Global)							
6	Group	Enterprise Admins (Global)							
7	Group	Group Policy Creator Owners (Global)							
8	Group	Schema Admins (Global)							
9	Group	Enterprise Admins (Global)							
10	Group	Administrators (Global)							
11	AccountType	User							
12	Comment	Default account for administrative access to the computer domain							
13	HomeDir								
14	Profile								
15	LogonScript	login.bat							
16	Workstation								
17	PowerShellEnabled	Yes							
18	PowerShellPath	Yes	3000,4000						
19	PowerShellExe	No							
20	PowerShellExePath	None							
21	AccDisabled	No							
22	AccLockedOut	No							
23	AccExpiresTime	None							
24	LogonTime		3000,3000						
25	LogonScript	login.bat							
26	LogonScriptPath	login.bat							
27	LogonScriptExe	login.bat							
28	LogonScriptExePath	login.bat							
29	LogonScriptExePath	login.bat							
30	LogonScriptExePath	login.bat							
31	LogonScriptExePath	login.bat							
32	LogonScriptExePath	login.bat							
33	LogonScriptExePath	login.bat							
34	LogonScriptExePath	login.bat							
35	LogonScriptExePath	login.bat							
36	LogonScriptExePath	login.bat							
37	LogonScriptExePath	login.bat							
38	LogonScriptExePath	login.bat							
39	LogonScriptExePath	login.bat							
40	LogonScriptExePath	login.bat							
41	LogonScriptExePath	login.bat							
42	LogonScriptExePath	login.bat							
43	LogonScriptExePath	login.bat							
44	LogonScriptExePath	login.bat							
45	LogonScriptExePath	login.bat							
46	LogonScriptExePath	login.bat							
47	LogonScriptExePath	login.bat							
48	LogonScriptExePath	login.bat							
49	LogonScriptExePath	login.bat							
50	LogonScriptExePath	login.bat							
51	LogonScriptExePath	login.bat							
52	LogonScriptExePath	login.bat							
53	LogonScriptExePath	login.bat							
54	LogonScriptExePath	login.bat							
55	LogonScriptExePath	login.bat							
56	LogonScriptExePath	login.bat							
57	LogonScriptExePath	login.bat							
58	LogonScriptExePath	login.bat							
59	LogonScriptExePath	login.bat							
60	LogonScriptExePath	login.bat							

All - Layouts										
	A	B	C	D	E	F	G	H	I	J
1	Layouts									
2	Ref	S:1521-100002107-362-807404-2025415-80-000								
3	RefDate	No								
4	RefCallBack	No								
5	RefCallBackNumber									
6	Group	Domain Users (Global)								
7	Fullname									
8	AccountType	User								
9	Comment	Very Distributed Code Service Account								
10	HomeDir									
11	Profile									
12	LogonScript									
13	Workstations									
14	PowerShellChanged	Yes								
15	PowerShellTime									
16	PowerShell	Yes								
17	PowerShellTime									
18	PowerShellTime	Yes								
19	PowerShellTime	Yes								
20	PowerShellTime	Yes								
21	PowerShellTime	Yes								
22	PowerShellTime	Yes								
23	PowerShellTime	Yes								
24	PowerShellTime	Yes								
25	PowerShellTime	Yes								
26	PowerShellTime	Yes								
27	PowerShellTime	Yes								
28	PowerShellTime	Yes								
29	PowerShellTime	Yes								
30	PowerShellTime	Yes								
31	PowerShellTime	Yes								
32	PowerShellTime	Yes								
33	PowerShellTime	Yes								
34	PowerShellTime	Yes								
35	PowerShellTime	Yes								
36	PowerShellTime	Yes								
37	PowerShellTime	Yes								
38	PowerShellTime	Yes								
39	PowerShellTime	Yes								
40	PowerShellTime	Yes								
41	PowerShellTime	Yes								
42	PowerShellTime	Yes								
43	PowerShellTime	Yes								
44	PowerShellTime	Yes								
45	PowerShellTime	Yes								
46	PowerShellTime	Yes								
47	PowerShellTime	Yes								
48	PowerShellTime	Yes								
49	PowerShellTime	Yes								
50	PowerShellTime	Yes								
51	PowerShellTime	Yes								
52	PowerShellTime	Yes								
53	PowerShellTime	Yes								
54	PowerShellTime	Yes								
55	PowerShellTime	Yes								
56	PowerShellTime	Yes								
57	PowerShellTime	Yes								
58	PowerShellTime	Yes								
59	PowerShellTime	Yes								
60	PowerShellTime	Yes								
61	PowerShellTime	Yes								
62	PowerShellTime	Yes								
63	PowerShellTime	Yes								
64	PowerShellTime	Yes								
65	PowerShellTime	Yes								
66	PowerShellTime	Yes								
67	PowerShellTime	Yes								
68	PowerShellTime	Yes								
69	PowerShellTime	Yes								
70	PowerShellTime	Yes								
71	PowerShellTime	Yes								
72	PowerShellTime	Yes								
73	PowerShellTime	Yes								
74	PowerShellTime	Yes								
75	PowerShellTime	Yes								
76	PowerShellTime	Yes								
77	PowerShellTime	Yes								
78	PowerShellTime	Yes								
79	PowerShellTime	Yes								
80	PowerShellTime	Yes								
81	PowerShellTime	Yes								
82	PowerShellTime	Yes								
83	PowerShellTime	Yes								
84	PowerShellTime	Yes								
85	PowerShellTime	Yes								
86	PowerShellTime	Yes								
87	PowerShellTime	Yes								
88	PowerShellTime	Yes								
89	PowerShellTime	Yes								
90	PowerShellTime	Yes								
91	PowerShellTime	Yes								
92	PowerShellTime	Yes								
93	PowerShellTime	Yes								
94	PowerShellTime	Yes								
95	PowerShellTime	Yes								
96	PowerShellTime	Yes								
97	PowerShellTime	Yes								
98	PowerShellTime	Yes								
99	PowerShellTime	Yes								
100	PowerShellTime	Yes								

All - Layouts (Current and Future)										
	A	B	C	D	E	F	G	H	I	J
1	Layouts									
2	Ref	S:1521-100002107-362-807404-2025415-80-000								
3	RefDate	No								
4	RefCallBack	No								
5	RefCallBackNumber									
6	Group	Domain Users (Global)								
7	Fullname									
8	AccountType	User								
9	Comment	Very Distributed Code Service Account								
10	HomeDir									
11	Profile									
12	LogonScript									
13	Workstations									
14	PowerShellChanged	Yes								
15	PowerShellTime									
16	PowerShell	Yes								
17	PowerShellTime									
18	PowerShellTime	Yes								
19	PowerShellTime	Yes								
20	PowerShellTime	Yes								
21	PowerShellTime	Yes								
22	PowerShellTime	Yes								
23	PowerShellTime	Yes								
24	PowerShellTime	Yes								
25	PowerShellTime	Yes								
26	PowerShellTime	Yes								
27	PowerShellTime	Yes								
28	PowerShellTime	Yes								
29	PowerShellTime	Yes								
30	PowerShellTime	Yes								
31	PowerShellTime	Yes								
32	PowerShellTime	Yes								
33	PowerShellTime	Yes								
34	PowerShellTime	Yes								
35	PowerShellTime	Yes								
36	PowerShellTime	Yes								
37	PowerShellTime	Yes								
38	PowerShellTime	Yes								
39	PowerShellTime	Yes								
40	PowerShellTime	Yes								
41	PowerShellTime	Yes								
42	PowerShellTime	Yes								
43	PowerShellTime	Yes								
44	PowerShellTime	Yes								
45	PowerShellTime	Yes								
46	PowerShellTime	Yes								
47	PowerShellTime	Yes								
48	PowerShellTime	Yes								
49	PowerShellTime	Yes								
50	PowerShellTime	Yes								
51	PowerShellTime	Yes								
52	PowerShellTime	Yes								
53	PowerShellTime	Yes								
54	PowerShellTime	Yes								
55	PowerShellTime	Yes								
56	PowerShellTime	Yes								
57	PowerShellTime	Yes								
58	PowerShellTime	Yes								
59	PowerShellTime	Yes								
60	PowerShellTime	Yes								
61	PowerShellTime	Yes								
62	PowerShellTime	Yes								
63	PowerShellTime	Yes								
64	PowerShellTime	Yes								
65	PowerShellTime	Yes								
66	PowerShellTime	Yes								
67	PowerShellTime	Yes								
68	PowerShellTime	Yes								
69	PowerShellTime	Yes								
70	PowerShellTime	Yes								
71	PowerShellTime	Yes								
72	PowerShellTime	Yes								
73	PowerShellTime	Yes								
74	PowerShellTime	Yes								
75	PowerShellTime	Yes								
76	PowerShellTime	Yes								
77	PowerShellTime	Yes								
78	PowerShellTime	Yes								
79	PowerShellTime	Yes								
80	PowerShellTime	Yes								
81	PowerShellTime	Yes								
82	PowerShellTime	Yes								
83	PowerShellTime	Yes								
84	PowerShellTime	Yes								
85	PowerShellTime	Yes								
86	PowerShellTime	Yes								
87	PowerShellTime	Yes								
88	PowerShellTime	Yes								
89	PowerShellTime	Yes								
90	PowerShellTime	Yes								
91	PowerShellTime	Yes								
92	PowerShellTime	Yes								
93	PowerShellTime	Yes								
94	PowerShellTime	Yes								
95	PowerShellTime	Yes								
96	PowerShellTime	Yes								
97	PowerShellTime	Yes								
98	PowerShellTime	Yes								
99	PowerShellTime	Yes								
100	PowerShellTime	Yes								

A	B	C	D	E	F	G	H	I
57	USER_Serve9	Internet Guest Account	No	Never	37641.5 All		Never	No
58	1 MAM_DC1	Internet Guest Account	No	Never	37642.60139 All		36376.37069	No
59	1 MAM_Serve2	Internet Guest Account	No	Never	38379.38125 All		Never	No
60	1 MAM_Serve3	Web Application Manager account	No	Never	38446.67272 All		Never	No
61	1 MAM_Serve4	Web Application Manager account	No	Never	38906.6826 All		Never	No
62	1 MAM_Serve5	Launch IIS Process Account	No	Never	39215.68403 All		Never	No
63	1 MAM_Serve6	Internet Guest Account	No	Never	37541.47917 All		Never	No
64	1 MAM_Serve7	Internet Guest Account	No	Never	37335.77351 All		Never	No
65	1 MAM_Serve8	Internet Guest Account	No	Never	38307.4 All		Never	No
66	1 MAM_Serve9	Internet Guest Account	No	Never	37641.5 All		Never	No
67	1 lamblane	Allan Lamborne	No	Never	38446.33364	38395.29397 All	36379.29306	No
68	1 mickkady	March Kirkaldy	No	38427.36667	38337.36667 All		36372.36319	No
69	1 mimsley	Miles Kinsley	No	38417.35903	38327.35903 All		36380.35486	No
70	1 mirst	Mark Kirt	No	38462.36782	38362.36525 All		36384.36139	No
71	1 dkinneer	Douglas Kinneer	No	Never	37790.72290 All		36387.36675	No
72	1 mkinberley	Martin Kimberley	No	38432.37014	38342.37014 All		36380.36044	No
73	1 kldgt	Yes	37673.63472	37593.63472 All		Never	No	No
74	1 apudite	Alfred Baptiste	No	38487.71119	38377.71119 All		36383.36782	No
75	1 mkinncot	Martin Kennicot	No	38389.34375	38339.34375 All		36373.36181	No
76	1 kalsley	Alan Kalsley	No	38419.67669	38329.67569 All		36343.36389	No
77	1 elvato	Edward Kelso	No	38410.30333	38300.30333 All		36377.32163	No
78	1 kkimberley	Alban Kimberley	No	38452.40069	38362.35903 All		36379.36235	No
79	1 lamport	Egbert Lamport	No	38403.40764	38313.40764 All		36379.56069	No
80	1 lamport	Manuel Lamport	No	38466.36528	38376.32351 All		36370.36684	No
81	1 leat	Ernie Gill	No	38400.57078	38310.57078 All		36380.31380	No
82	1 dkinble	Desmond Kinble	No	38427.42986	38337.42986 All		36379.39514	No
83	1 dkinneer	Durley Kinneer	No	38433.375	38343.375 All		36380.42163	No
84	1 mimsy	Mona Kips	No	38424.34722	38334.34722 All		36380.34614	No
85	1 appras	App RAS account	No	Never	38334.65833 All		37979.38868	Yes
86	1 apprep1	App Replication Account	No	Never	37772.99583 All		Never	No
87	1 vndr	App Vendor	Yes	Never	38106.43125 All		Never	Yes
88	1 vndr	Application Vendor	Yes	Never	37562.63975 All		Never	Yes
89	1 kirkaldy	Anthony Kirkaldy	No	38427.36872	38337.36872 All		36380.31319	No
90	1 mkinham	Martin Kisham	No	38432.65278	38342.65278 All		36380.36722	No
91	1 kinsley	Argus Kinsley	No	Never	38337.34881 All		36380.33164	No
92	1 kinsley	Argus Kinsley	No	38411.27292	38321.27292 All		36378.69722	No
93	1 kinsley	Durley Kinsley	No	38466.45625	38376.41659 All		36380.31644	No
94	1 kinsley	Alastair Laney	No	38425.37047	38345.37047 All		36373.68861	No
95	1 kinsley	test	No	Never	38425.65278 All		36343.65266	No
96	1 mkinmpster	Mona Kinspster	No	38468.38066	38378.33889 All		36379.33642	No
97	1 kinsley	Allen Kinsley	No	38366.33472	38336.33472 All		36380.34583	No
98	1 mkinham	Martin Kisham	No	38393.63869	38303.63869 All		36379.47647	No
99	1 ecomellus	Ephraim Comellus	No	38401.36006	38311.36006 All		36328.36444	No
100	1 kalsley	Andrew Kalsley	No	38410.34742	38320.34742 All		36379.76403	No
101	1 dkinneer	Sharon Kins	No	Never	38370.38472 All		Never	No
102	1 Supervisor	Supervisor	Yes	Never	38104.63881 All		Never	No
103	1 dkinneer	Don Kinsley	No	38358.35764	38308.35764 All		36379.42059	No
104	1 lamport	Alan Lamport	No	38411.37639	38321.37639 All		36377.36161	No
105	1 kinsley	Eric Kinsley	No	38447.37163	38357.37163 All		36380.31468	No
106	1 Sync Agent Account	Sync Agent Account	No	Never	38166.425 All		Never	No
107	1 kinsley	Edgar Key	No	38445.37639	38355.37472 All		36380.36164	No
108	1 kinsley	Edwin Kinsley	No	38432.31736	38342.31736 All		36377.36275	No
109	1 TLR	Teller branch 1	No	Never	36202.76270 Sun(5-24)Mon(5-24)Tue(5-24)Wed(5-24)Thu(5-24)Fri(5-24)Sat(5-16)		36380.31069	No
110	1 TLR2	Teller branch 2	No	Never	36104.65764 Mon(5-24)Tue(5-24)Wed(5-24)Thu(5-24)Fri(5-24)Sat(5-14)		36380.30319	No
111	1 TLR3	Teller branch 3	No	Never	36115.73917 Mon(5-24)Tue(5-24)Wed(5-24)Thu(5-24)Fri(5-24)Sat(5-16)		36380.36235	No
112	1 TLR4	Teller branch 4	No	Never	36116.66181 Mon(5-24)Tue(5-24)Wed(5-24)Thu(5-24)Fri(5-24)Sat(5-16)		36377.36568	No

- Copy to a new sheet, sort by Disabled account, and delete the remainder.

A	B	C	D	E	F	G	H	I
1	Disabled User	Fulltime	AccDisabled	PinLastUpdateTime	PinLastUpdateTime	LogonTime	LastLogonTime	PinDate
2	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No
3	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No
4	System(Admin)	System(Admin)	Yes	37673.63472	37593.63472 All	38446.67272 All	37979.38868	No
5	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No
6	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No
7	System(Admin)	System(Admin)	Yes	37673.63472	37593.63472 All	38446.67272 All	37979.38868	No
8	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No
9	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No
10	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No
11	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No
12	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No

- Copy to a new sheet, sort by DialIn account, and delete the remainder.

A	B	C	D	E	F	G	H	I
1	Disabled User	Fulltime	AccDisabled	PinLastUpdateTime	PinLastUpdateTime	LogonTime	LastLogonTime	PinDate
2	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No
3	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No
4	System(Admin)	System(Admin)	Yes	37673.63472	37593.63472 All	38446.67272 All	37979.38868	No
5	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No
6	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No
7	System(Admin)	System(Admin)	Yes	37673.63472	37593.63472 All	38446.67272 All	37979.38868	No
8	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No
9	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No
10	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No
11	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No
12	System(Admin)	System(Admin)	Yes	Never	Never	AB	Never	No

- Copy to a new sheet, sort by Password Expires (primary sort) and Password Last Set Time (secondary sort).

Username	Full Name	Account Type	Password Expires	Password Last Set	Logon Hours	Last Logon Time	Function
10838CCC-2F01-4969-A	SystemMailbox{10838CCC-2F01-4969-A51C-EEDB7CFDF74F}	System Mailbox	Never	Never	All	Never	No
AdminSch	Microsoft Schedule+ Free/Busy Connector	System Mailbox	Never	Never	All	Never	No
auditor	Auditors	User	12/18/03 9:31 AM	9/19/03 10:31 AM	Mon(5-24)Tue(10/7/03 3:31 PM	No
Fedline	Fedline Machine	User	Never	2/13/99 1:23 PM	All	Never	No
Gnost		User	Never	3/7/00 9:50 AM	All	Never	No
kbrtgt		User	2/21/03 3:14 PM	11/23/02 3:14 PM	All	Never	No
Supervisor	Supervisor	User	Never	11/5/98 3:17 PM	All	Never	No
vendor	Application Vendor	User	Never	11/23/02 12:54 PM	All	Never	Yes
vndr	App Vendor	User	Never	11/6/98 10:21 AM	All	Never	Yes

- The presentation Sheets contain formulas that point to the underlying raw data sheets.

Auditing Firm

AnyBank Disabled Users							
Information as of:		28-Jan-06					
Seq	User	FullName	Password Expires	Pwd Last Set	Logon Hours	Last Logon	Dial in ?
1	10838CCC-2F01-4969-A	SystemMailbox{10838CCC-2F01-4969-A51C-EEDB7CFDF74F}	?Unknown	Never	All	Never	No
2	AdminSch	Microsoft Schedule+ Free/Busy Connector	?Unknown	Never	All	Never	No
3	auditor	Auditors	12/18/03 9:31 AM	9/19/03 10:31 AM	Mon(5-24)Tue(10/7/03 3:31 PM	No
4	Fedline	Fedline Machine	Never	2/13/99 1:23 PM	All	Never	No
5	Gnost		Never	3/7/00 9:50 AM	All	Never	No
6	kbrtgt		2/21/03 3:14 PM	11/23/02 3:14 PM	All	Never	No
7	Supervisor	Supervisor	Never	11/5/98 3:17 PM	All	Never	No
8	vendor	Application Vendor	Never	11/23/02 12:54 PM	All	Never	Yes
9	vndr	App Vendor	Never	11/6/98 10:21 AM	All	Never	Yes

Observations on Disabled Users:

- Guest account has been disabled, not deleted
- It appears that two vendor accounts are present, but disabled
- An auditor account is present, but disabled
- A Fedline user account is disabled
- It appears that each of these accounts is manually controlled with no password expiration.
- Purpose for each account should be determined to see if they are consistent with the institution's policies.

Auditing Firm

AnyBank Dial In Users								
Information as of:		28-Jan-05						
Seq	User	FullName	Disabled ?	Password Expires	Pwd Last Set	Logon Hours	Last Logon	Dial in ?
1	Administrator	Administrator	No	Never	7/24/03 10:45 AM	All	1/28/05 9:17 AM	Yes
2	appras	App RAS account	No	Never	12/3/04 1:24 PM	All	12/24/03 9:21 AM	Yes
3	Internal		No	Never	9/9/02 11:03 AM	All	Never	Yes
4	mlacy	Malcolm Lacy	No	4/18/05 9:12 AM	1/18/05 8:12 AM	All	1/27/05 10:58 AM	Yes
5	vendor	Application Vendor	Yes	Never	11/23/02 12:54 PM	All	Never	Yes
6	vndr	App Vendor	Yes	Never	11/6/98 10:21 AM	All	Never	Yes
7								

Observations on Dial In Users:

These are the most dangerous accounts since they have authority to access the system remotely. The first four are active accounts that should be scrutinized.

- Administrator account has not been renamed
- Appras and Internal accounts appear to be generic account (generic user accounts are not good practice. They evade tracking individual responsibility for events in a forensic audit.)

Auditing Firm

AnyBank Password Age								
Information as of:		28-Jan-05						
Seq	User	FullName	Password Expires	Pwd Last Set	Logon Hours	Last Logon	Dial in ?	
1	CSR2	CSR's Branch 2	Never	11/5/98 3:46 PM	All	12/9/04 8:49 AM	No	
2	TLR2	Teller branch 2	Never	11/5/98 3:47 PM	Mon-Sat 9:19 AM	No		
3	CSR4	CSR's Branch 4	Never	11/9/98 3:53 PM	All	12/13/04 8:58 AM	No	
4	TLR4	Teller branch 4	Never	11/9/98 3:53 PM	Mon-Sat 9:21 AM	No		
5	CSR3	CSR's Branch 3	Never	11/6/98 5:30 PM	All	1/28/05 7:35 AM	No	
6	TLR3	Teller branch 3	Never	11/6/98 5:30 PM	Mon-Sat 9:21 AM	No		
7	backup	Backup for servers	Never	11/5/98 12:29 PM	All	Never	No	
8	AcServe	AcServe Account	Never	12/30/98 11:32 AM	All	Never	No	
9	Vinea	Vinea Login	Never	12/30/98 11:53 PM	All	Never	No	
10	Sysc Agent Account	Sysc Agent Account	Never	1/5/99 10:12 AM	All	Never	No	
11	CSR	CSR's Branch 1	Never	2/11/99 5:59 PM	All	1/28/05 7:34 AM	No	
12	TLR	Teller branch 1	Never	2/11/99 6:04 PM	Sat-Sun 9:19 AM	No		
13	Recep	Receptionist	Never	6/16/99 8:18 AM	All	1/28/05 7:58 AM	No	
14	IUSR_Server3	Internet Guest Account	Never	10/13/99 4:07 PM	All	Never	No	
15	IWAM_Server3	Web Application Manager account	Never	10/13/99 4:08 PM	All	Never	No	
16	Bank	Bank	Never	3/16/00 9:36 AM	All	1/25/05 10:55 AM	No	
17	IUSR_Server4	Internet Guest Account	Never	3/23/00 3:53 PM	All	Never	No	
18	IWAM_Server4	Web Application Manager account	Never	3/23/00 3:54 PM	All	Never	No	
19	VBE ADMIN		Never	4/5/00 11:26 AM	All	8/18/04 4:45 PM	No	
20	EXCH-SERVICE-ACCOUNT	NAV for Microsoft Exchange	Never	12/24/00 5:35 PM	All	1/28/05 10:05 AM	No	
21	backup ave	backup ave	Never	1/19/01 2:28 PM	All	Never	No	
22	TLR5	Teller branch 5	Never	5/16/01 8:31 AM	Mon-Sat 9:21 AM	12/8/01 8:52 AM	No	
23	CSR5	CSR's Branch 5	Never	5/16/01 8:33 AM	All	1/26/05 7:46 AM	No	
24	Internal		Never	9/9/02 11:03 AM	All	Never	Yes	
25	TsInternetUser	TsInternetUser	Never	11/23/02 2:57 PM	All	Never	No	
26	IUSR_Server7	Internet Guest Account	Never	11/25/02 6:34 PM	All	Never	No	
27	IWAM_Server7	Internet Guest Account	Never	11/25/02 6:34 PM	All	Never	No	
28	IUSR_Server6	Internet Guest Account	Never	1/20/03 11:30 AM	All	Never	No	
29	IWAM_Server6	Internet Guest Account	Never	1/20/03 11:30 AM	All	Never	No	
30	IUSR_Server9	Internet Guest Account	Never	1/20/03 12:00 PM	All	Never	No	
31	IWAM_Server9	Internet Guest Account	Never	1/20/03 12:00 PM	All	Never	No	
32	IUSR_DC1	Internet Guest Account	Never	1/21/03 2:26 PM	All	1/28/05 7:49 AM	No	
33	IWAM_DC1	Internet Guest Account	Never	1/21/03 2:26 PM	All	1/24/05 9:01 AM	No	
34	exch-nav-agent	Exch-NAV-Agent	Never	1/23/03 1:59 PM	All	10/1/03 11:00 AM	No	
35	Bank1	Bank1	Never	3/3/03 2:59 PM	All	Never	No	
36	aggrsp1	App Replication Account	Never	5/3/03 11:54 PM	All	Never	No	
37	dkinnear	Douglas Kinnear	Never	6/27/03 5:21 PM	All	1/15/05 8:51 AM	No	
38	Administrator	Administrator	Never	7/24/03 10:45 AM	All	1/28/05 9:17 AM	Yes	
39	emaildump	email dump	Never	8/7/03 11:47 AM	All	8/6/03 8:19 PM	No	
40	Enduser	Enduser	Never	9/3/03 9:09 AM	All	9/3/03 9:37 AM	No	
41	mkorth	March Keith	Never	3/7/04 12:57 PM	All	1/28/05 8:04 AM	No	
42	IUSR_Server2	Internet Guest Account	Never	4/2/04 9:09 AM	All	Never	No	

Page 1 of 2

Any Bank Password Age							
Information as of:		28-Jan-06					
Seq	User	FullName	Password Expires	Pwd Last Set	Logon Hours	Last Logon	Dial in ?
43	IWAM_Server2	Internet Guest Account	Never	4/2/04 9:09 AM	All	Never	No
44	stalemcmt	Statements	Never	7/2/04 9:14 AM	All	Never	No
45	exch-backup-agent	Exchange Backup Agent	Never	8/11/04 12:12 PM	All	8/11/04 12:26 PM	No
46	IUSR_Server5	Internet Guest Account	Never	8/16/04 4:25 PM	All	Never	No
47	IWAM_Server5	Launch ITS Process Account	Never	8/16/04 4:25 PM	All	Never	No
48	rtest	rtest	Never	9/13/04 3:40 PM	All	9/13/04 3:44 PM	No
49	emailad	emailad	Never	11/10/04 3:10 PM	All	Never	No
50	IUSR_Server8	Internet Guest Account	Never	11/11/04 9:36 AM	All	Never	No
51	IWAM_Server8	Internet Guest Account	Never	11/11/04 9:36 AM	All	Never	No
52	upgras	App RAS account	Never	12/3/04 1:24 PM	All	12/24/04 9:21 AM	Yes
53	krhgt		2/21/03 3:14 PM	11/23/02 3:14 PM	All	Never	No
54	auditor	Auditor	12/18/03 9:31 AM	9/19/03 10:31 AM	Mon(5-24/Tue)	10/7/03 3:31 PM	No
55	mkenncot	Martin Kennicot	2/3/05 9:05 AM	11/30/04 9:05 AM	All	12/10/05 8:31 AM	No
56	mhillam	Martin Hillam	3/10/05 10:32 AM	11/12/04 10:32 AM	All	12/10/05 11:29 AM	No
57	akendrick	Allan Kendrick	2/13/05 8:02 AM	11/15/04 8:02 AM	All	12/8/05 8:15 AM	No
58	ekercher	Eustace Kercher	2/13/05 8:42 AM	11/15/04 8:42 AM	All	12/7/05 9:36 AM	No
59	dkiersted	Dan Kiersted	2/15/05 8:35 AM	11/17/04 8:35 AM	All	12/7/05 10:33 AM	No
60	mkenncot	Martin Kennicot	2/16/05 8:15 AM	11/18/04 8:15 AM	All	12/1/05 8:41 AM	No
61	ekid	Emile Kid	2/17/05 7:51 AM	11/19/04 7:51 AM	All	12/8/05 7:32 AM	No
62	ecornelius	Ephraim Cornelius	2/18/05 8:50 AM	11/20/04 8:50 AM	All	12/8/05 9:25 AM	No
63	adiotrephe	Archibald Diotrephe	2/20/05 9:34 AM	11/22/04 9:34 AM	All	12/8/05 9:15 AM	No
64	olampor	Egbert Lampor	2/20/05 9:47 AM	11/22/04 9:47 AM	All	12/7/05 1:13 PM	No
65	mkimberley	March Kimberley	2/24/05 8:37 AM	11/26/04 8:37 AM	All	12/6/05 5:27 PM	No
66	abaptiste	Alfred Baptiste	2/24/05 5:07 PM	11/26/04 5:07 PM	All	12/8/05 9:33 AM	No
67	akelney	Andrew Kelney	2/27/05 8:02 AM	11/29/04 8:02 AM	All	12/7/05 6:49 PM	No
68	ekelso	Edward Kelso	2/27/05 9:12 AM	11/29/04 9:12 AM	All	12/8/05 5:19 PM	No
69	dkymyotus	Douglas Dymyotus	2/27/05 9:42 AM	11/29/04 9:42 AM	All	12/20/05 9:11 AM	No
70	akinsley	Angie Kinsley	2/28/05 6:35 AM	11/30/04 6:35 AM	All	12/6/05 4:44 PM	No
71	alampor	Alan Lampor	2/28/05 9:02 AM	11/30/04 9:02 AM	All	12/5/05 8:41 AM	No

Observations on Password Age:

The top of this list should be reviewed for users who no longer require system access. We should also look for users who have not changed password for an extended period of time.

- Many of the accounts on the list are generic accounts (not best practice), and should be reviewed for purpose and validity.
- Too many accounts' (including recep) passwords have not been changed since 1999. This is either poor policy or mis-configuration of system policy applied to this user.
- In general, quite a bit of attention should be placed on reviewing the accounts on this list.

© SANS Institute

Auditing Firm

AnyBank User Statistics								
Information as of: 20-Jun-05								
Seq	User	Full Name	Disabled ?	Password Expires	Pwd Last Set	Logon Hours	Last Logon	Dial In ?
1	10R38CUC-2901-1969-A	System Mailbox (10R38CUC-2901-1969-A)1C4E3DH7CF1D74B6	Yes	Never	Never	All	Never	No
2	Administrator	Administrator	No	Never	7/24/03 10:45 AM	All	1/28/05 9:17 AM	Yes
3	AdminSch	Microsoft Schedule+ Free/Busy Connector	Yes	Never	Never	All	Never	No
4	mrlacy	Malcolm Lacy	No	4/18/05 9:12 AM	1/18/05 8:12 AM	All	1/27/05 10:58 AM	Yes
5	ArcheServe	ArcheServe Account	No	Never	12/30/98 11:32 AM	All	Never	No
6	skiel	Annalee Kiel	No	3/1/05 2:00 PM	12/1/04 2:00 PM	All	1/26/05 11:24 AM	No
7	auditor	Auditors	Yes	12/18/03 9:31 AM	9/19/03 10:31 AM	Mon(5-24)Tue	10/7/03 3:31 PM	No
8	backup	Backup for servers	No	Never	1/12/98 12:29 PM	All	Never	No
9	backup_svc	backup_svc	No	Never	1/19/01 2:28 PM	All	Never	No
10	clay	Breast Clay	No	3/14/05 9:36 AM	12/14/04 9:36 AM	All	12/14/04 9:36 AM	No
11	ceramus	Edgar Ceramus	No	3/14/05 8:33 AM	12/14/04 8:33 AM	All	1/19/05 1:22 PM	No
12	clipp	Dagene Klipp	No	4/12/05 9:19 AM	1/12/05 8:19 AM	All	1/28/05 7:30 AM	No
13	clingham	Elisba Kington	No	3/13/05 7:52 AM	12/13/04 7:52 AM	All	1/27/05 7:46 AM	No
14	ukington	Malcolm Kingston	No	3/13/05 7:57 AM	12/13/04 7:57 AM	All	1/18/05 7:36 AM	No
15	ukimberley	March Kimberley	No	2/4/05 8:37 AM	1/16/04 8:37 AM	All	1/26/05 3:27 PM	No
16	udiana	Adrian Diana	No	3/22/05 3:06 PM	12/22/04 3:06 PM	All	1/23/05 9:30 AM	No
17	ckerchar	Bustace Kercher	No	2/13/05 8:42 AM	1/13/04 8:42 AM	All	1/27/05 9:36 AM	No
18	ekenard	Ezekiel Kemard	No	3/24/05 1:43 PM	12/24/04 1:43 PM	All	1/27/05 10:43 AM	No
19	CSR	CSR's Branch 1	No	Never	3/11/99 3:39 PM	All	1/28/05 7:44 AM	No
20	CSR2	CSR's Branch 2	No	Never	1/15/98 3:46 PM	All	12/9/04 8:49 AM	No
21	CSR3	CSR's Branch 3	No	Never	1/16/98 5:00 PM	All	1/28/05 7:48 AM	No
22	CSR4	CSR's Branch 4	No	Never	1/19/98 1:53 PM	All	12/13/04 8:38 AM	No
23	CSR5	CSR's Branch 5	No	Never	5/18/01 8:53 AM	All	1/26/05 7:46 AM	No
24	mdiodorus	Malcolm Diodorus	No	4/3/05 12:01 PM	1/3/05 11:01 AM	All	1/28/05 10:02 AM	No
25	dkeese	Donald Keese	No	4/5/05 9:22 AM	1/5/05 8:22 AM	All	1/28/05 9:20 AM	No
26	eken	Hustace Ken	No	3/26/05 8:13 AM	12/26/04 8:13 AM	All	1/28/05 7:59 AM	No
27	ukiemman	Michael Kieman	No	4/21/05 9:11 AM	1/21/05 8:11 AM	All	1/28/05 8:05 AM	No
28	aker	Adam Ken	No	3/10/05 8:03 AM	12/10/04 8:03 AM	All	1/27/05 3:38 PM	No
29	alcant	Alick Kent	No	3/13/05 6:36 AM	12/13/04 6:36 AM	All	1/27/05 12:32 PM	No
30	ukennicot	Martin Kennicot	No	2/3/05 9:05 AM	1/3/04 9:05 AM	All	1/24/05 8:31 AM	No
31	ukinsley	Mark Kinsley	No	4/3/05 10:37 AM	1/3/05 1:17 PM	All	1/3/05 1:17 PM	No
32	dyovynius	Douglas Dyovynius	No	2/27/05 9:42 AM	1/29/04 9:42 AM	All	1/26/05 9:11 AM	No
33	akinghom	Alfred Kington	No	4/11/05 10:31 AM	1/11/05 9:31 AM	All	1/23/05 2:38 PM	No
34	mkelly	Maximilian Kelly	No	4/14/05 9:23 AM	1/13/05 8:23 AM	All	12/3/04 8:05 AM	No
35	emailed	emailed	No	Never	1/10/04 3:10 PM	All	Never	No
36	emaildump	email dump	No	Never	8/1/03 1:47 AM	All	8/6/03 5:19 PM	No
37	udiotreplies	Archibald Diutrepiles	No	2/20/05 9:34 AM	1/12/04 9:34 AM	All	1/28/05 9:13 AM	No
38	exch-backup-agent	Exchange Backup Agent	No	Never	8/11/04 12:12 PM	All	8/11/04 12:26 PM	No
39	exch-nas-agent	Exch-NAV-Agent	No	Never	1/23/03 1:39 PM	All	10/1/03 11:00 AM	No
40	EXCH-SERVICE-ACCOUNT	NAY for Microsoft Exchange	No	Never	12/14/00 3:38 PM	All	1/28/05 10:05 AM	No
41	Fedline	Fedline Machine	Yes	Never	2/15/99 1:23 PM	All	Never	No
42	akung	Alfred King	No	3/6/05 2:09 PM	12/6/04 2:09 PM	All	12/6/04 2:10 PM	No
43	Gnest		Yes	Never	3/7/99 9:50 AM	All	Never	No
44	Bank	Bank	No	Never	3/16/00 9:36 AM	All	1/23/05 10:33 AM	No

Page 1 of 3

Auditing Firm

AnyBank User Statistics								
Information as of: 29-Jun-05								
Seq	User	Full Name	Disabled ?	Password Expires	Pwd Last Set	Logon Hours	Last Logon	Dial In ?
45	Bank1	Bank1	No	Never	3/3/03 2:30 PM	All	Never	No
46	finlout	finlout	No	Never	9/3/03 9:09 AM	All	9/3/03 9:31 AM	No
47	Internal		No	Never	9/9/02 11:02 AM	All	Never	Yes
48	IUSR_DCL	Internet Guest Account	No	Never	1/21/03 2:26 PM	All	1/28/05 7:49 AM	No
49	IUSR_Server2	Internet Guest Account	No	Never	4/2/04 9:09 AM	All	Never	No
50	IUSR_Server3	Internet Guest Account	No	Never	10/13/99 4:07 PM	All	Never	No
51	IUSR_Server4	Internet Guest Account	No	Never	3/23/00 3:53 PM	All	Never	No
52	IUSR_Server5	Internet Guest Account	No	Never	8/16/04 4:25 PM	All	Never	No
53	IUSR_Server6	Internet Guest Account	No	Never	1/20/03 11:30 AM	All	Never	No
54	IUSR_Server7	Internet Guest Account	No	Never	11/25/02 6:34 PM	All	Never	No
55	IUSR_Server8	Internet Guest Account	No	Never	11/11/04 9:36 AM	All	Never	No
56	IUSR_Server9	Internet Guest Account	No	Never	1/20/03 12:00 PM	All	Never	No
57	IWAM_DCL	Internet Guest Account	No	Never	1/21/03 2:26 PM	All	1/24/05 9:01 AM	No
58	IWAM_Server2	Internet Guest Account	No	Never	4/2/04 9:09 AM	All	Never	No
59	IWAM_Server3	Web Application Manager account	No	Never	10/13/99 4:08 PM	All	Never	No
60	IWAM_Server4	Web Application Manager account	No	Never	3/23/00 3:54 PM	All	Never	No
61	IWAM_Server5	Launch IS Process Account	No	Never	9/16/04 4:25 PM	All	Never	No
62	IWAM_Server6	Internet Guest Account	No	Never	1/20/03 11:30 AM	All	Never	No
63	IWAM_Server7	Internet Guest Account	No	Never	11/25/02 6:34 PM	All	Never	No
64	IWAM_Server8	Internet Guest Account	No	Never	11/11/04 9:36 AM	All	Never	No
65	IWAM_Server9	Internet Guest Account	No	Never	1/20/03 12:00 PM	All	Never	No
66	ahambourne	Allan Lambourne	No	4/4/05 7:59 AM	1/4/05 6:59 AM	All	1/27/05 7:02 AM	No
67	mkirkaldy	March Kirkaldy	No	3/16/05 8:48 AM	12/16/04 8:48 AM	All	12/16/04 8:43 AM	No
68	mkinsley	Miles Kinsley	No	3/6/05 8:37 AM	12/6/04 8:37 AM	All	1/28/05 8:31 AM	No
69	mkent	Mark Kent	No	4/10/05 9:33 AM	1/10/05 8:33 AM	All	1/12/05 8:26 AM	No
70	dkinner	Douglas Kinner	No	Never	6/27/03 3:21 PM	All	1/13/05 8:31 AM	No
71	ukimberley	Martin Kimberley	No	3/21/05 8:53 AM	12/21/04 8:53 AM	All	1/28/05 8:32 AM	No
72	krltjg		Yes	2/21/03 3:14 PM	1/23/02 3:14 PM	All	Never	No
73	abapliste	Alfred Hapliste	No	2/24/05 5:07 PM	1/26/04 5:07 PM	All	1/28/05 9:43 AM	No
74	mkennicot	Martin Kennicot	No	2/16/05 8:15 AM	1/18/04 8:15 AM	All	1/21/05 8:41 AM	No
75	akelsey	Alan Kelsey	No	3/8/05 4:13 PM	12/8/04 4:13 PM	All	12/22/04 8:44 AM	No
76	ekelso	Edward Kelso	No	2/27/05 9:12 AM	1/29/04 9:12 AM	All	1/23/05 5:19 PM	No
77	akimberley	Alban Kimberley	No	4/10/05 9:37 AM	1/10/05 8:37 AM	All	1/27/05 8:42 AM	No
78	elampot	Egbert Lampot	No	2/26/05 9:47 AM	1/22/04 9:47 AM	All	1/27/05 1:13 PM	No
79	mlampot	Manuel Lampot	No	4/24/05 8:46 AM	1/24/05 7:46 AM	All	1/18/05 8:34 AM	No
80	ekid	Emile Kid	No	2/7/05 7:51 AM	1/19/04 7:51 AM	All	1/28/05 7:42 AM	No
81	dkimble	Diamond Kimble	No	3/16/05 10:19 AM	12/16/04 10:19 AM	All	1/27/05 9:29 AM	No
82	dkinner	Dudley Kinner	No	3/22/05 9:00 AM	12/22/04 9:00 AM	All	1/28/05 10:07 AM	No
83	mkcys	Monis Keys	No	3/13/05 8:20 AM	12/13/04 8:20 AM	All	1/28/05 8:17 AM	No
84	appras	App RAS account	No	Never	12/3/04 1:24 PM	All	12/24/03 9:21 AM	Yes
85	apprpl	App Replication Account	No	Never	5/31/03 11:54 PM	All	Never	No
86	svdr	App Vendor	Yes	Never	11/6/98 10:21 AM	All	Never	Yes
87	vendor	Application Vendor	Yes	Never	11/23/02 12:54 PM	All	Never	Yes
88	ukirkaldy	Anthony Kirkaldy	No	3/16/05 8:48 AM	12/16/04 8:48 AM	All	1/28/05 7:41 AM	No

Page 2 of 3

AnyBank User Statistics								
Information as of:		20-Jan-08						
Seq	User	FullName	Disabled ?	Password Expires	Pwd Last Set	Logon Hours	Last Logon	Dial in ?
89	mk-illum	Martin Killum	No	3/21/03 3:40 PM	12/21/04 3:40 PM	All	1/28/03 9:32 AM	No
90	Recep	Receptionist	No	Never	6/16/99 8:18 AM	All	1/28/03 7:58 AM	No
91	akinsley	Angus Kinsley	No	2/28/03 6:33 AM	11/30/04 6:33 AM	All	1/26/03 4:44 PM	No
92	dicigwin	Dudley Keigwin	No	4/24/03 16:57 AM	1/24/05 9:57 AM	All	1/28/03 7:40 AM	No
93	alahcy	Abalom Lahcy	No	3/24/03 9:05 AM	12/24/04 9:05 AM	All	1/21/03 4:46 PM	No
94	rttest	rttest	No	Never	9/13/04 3:40 PM	All	9/13/04 3:44 PM	No
95	mkempster	Morris Kempster	No	4/26/03 9:08 AM	1/26/05 8:08 AM	All	1/27/03 8:03 AM	No
96	akendrick	Allan Kendrick	No	2/13/03 8:03 AM	11/13/04 8:03 AM	All	1/28/03 8:18 AM	No
97	mkillum	Martin Killum	No	2/16/03 16:32 AM	1/12/04 16:32 AM	All	1/24/03 11:29 AM	No
98	ccornelius	Ephraim Cornelius	No	2/18/03 8:30 AM	11/20/04 8:30 AM	All	12/8/04 9:25 AM	No
99	akelcey	Andrew Kelcey	No	2/27/03 8:02 AM	1/29/04 8:02 AM	All	1/27/03 6:49 PM	No
100	statements	Statements	No	Never	7/2/04 9:14 AM	All	Never	No
101	Supervisor	Supervisor	Yes	Never	11/5/98 3:17 PM	All	Never	No
102	dkiersted	Dan Kiersted	No	2/15/03 8:35 AM	11/17/04 8:35 AM	All	1/27/03 10:33 AM	No
103	alamport	Alan Lamport	No	2/28/03 9:02 AM	11/30/04 9:02 AM	All	1/28/03 8:41 AM	No
104	ekinney	Eric Kinney	No	4/3/03 8:33 AM	1/3/03 7:35 AM	All	1/28/03 7:33 AM	No
105	Sync Agent Account	Sync Agent Account	No	Never	1/5/99 10:12 AM	All	Never	No
106	ekay	Edgar Kay	No	4/3/03 9:02 AM	1/3/03 8:02 AM	All	1/28/03 9:10 AM	No
107	ekendrick	Evelyn Kendrick	No	3/21/03 7:37 AM	1/21/04 7:37 AM	All	1/28/03 8:31 AM	No
108	TLR	Teller branch 1	No	Never	2/11/99 6:04 PM	Sun(5:24)Mon(1/28/03 7:32 AM	No
109	TLR2	Teller branch 2	No	Never	11/5/98 3:47 PM	Mon(5:24)Tue(2/21/04 9:19 AM	No
110	TLR3	Teller branch 3	No	Never	11/16/98 3:40 PM	Mon(5:24)Tue(1/28/03 8:12 AM	No
111	TLR4	Teller branch 4	No	Never	11/9/98 3:53 PM	Mon(5:24)Tue(11/30/04 9:21 AM	No
112	TLR5	Teller branch 5	No	Never	5/16/01 8:31 AM	Mon(5:24)Tue(12/8/04 8:52 AM	No
113	acornelius	Angus Cornelius	No	4/24/03 8:39 AM	1/24/05 7:39 AM	All	1/25/03 1:20 PM	No
114	mkcoith	March Koith	No	Never	3/15/04 12:57 PM	All	1/28/03 8:04 AM	No
115	TstInternetUser	TstInternetUser	No	Never	11/23/02 2:57 PM	All	Never	No
116	elamb	Edwin Lamb	No	4/27/03 7:48 AM	1/27/04 7:48 AM	All	1/27/03 4:58 PM	No
117	VHE ADMIN		No	Never	4/3/00 11:26 AM	All	8/18/01 4:43 PM	No
118	Vinca	Vinca Login	No	Never	12/30/98 11:53 PM	All	Never	No
119								
120								

Observations on User Statistics:

This gives a picture of key information about each user. Reviewing it allows us to get a “feel” for the user population. As mentioned before, a key issue with this audit is the practice of using a significant number of generic user IDs.

- A significant number of generic user accounts
- A significant number of accounts where the password never expires
- A significant number of accounts that are allowed to logon All hours (24x7x365 should be an UNUSUAL requirement.
- It appears that no review process of user accounts exists. This should be checked against policies and processes of the organization.

© SANS Institute

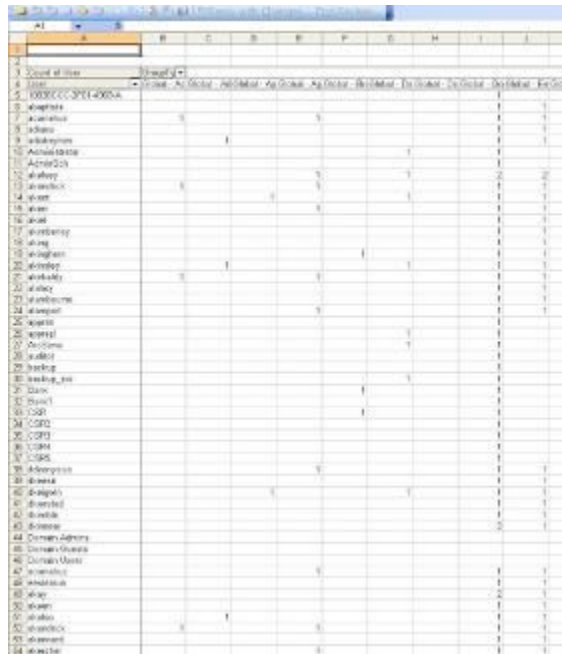
-

[illegible]

- Cut and Edit Paste Special Values into a raw data area. Sort the users and delete blank lines.

File Edit View Window Help		Go to: page number
Go to: page number		
1	File	Global: Open/Save
2	File	Global: Open/Save
3	File	Global: Open/Save
4	File	Global: Open/Save
5	File	Global: Open/Save
6	File	Global: Open/Save
7	File	Global: Open/Save
8	File	Global: Open/Save
9	File	Global: Open/Save
10	File	Global: Open/Save
11	File	Global: Open/Save
12	File	Global: Open/Save
13	File	Global: Open/Save
14	File	Global: Open/Save
15	File	Global: Open/Save
16	File	Global: Open/Save
17	File	Global: Open/Save
18	File	Global: Open/Save
19	File	Global: Open/Save
20	File	Global: Open/Save
21	File	Global: Open/Save
22	File	Global: Open/Save
23	File	Global: Open/Save
24	File	Global: Open/Save
25	File	Global: Open/Save
26	File	Global: Open/Save
27	File	Global: Open/Save
28	File	Global: Open/Save
29	File	Global: Open/Save
30	File	Global: Open/Save
31	File	Global: Open/Save
32	File	Global: Open/Save
33	File	Global: Open/Save
34	File	Global: Open/Save
35	File	Global: Open/Save
36	File	Global: Open/Save
37	File	Global: Open/Save
38	File	Global: Open/Save
39	File	Global: Open/Save
40	File	Global: Open/Save
41	File	Global: Open/Save
42	File	Global: Open/Save
43	File	Global: Open/Save
44	File	Global: Open/Save
45	File	Global: Open/Save
46	File	Global: Open/Save
47	File	Global: Open/Save
48	File	Global: Open/Save
49	File	Global: Open/Save
50	File	Global: Open/Save
51	File	Global: Open/Save
52	File	Global: Open/Save
53	File	Global: Open/Save
54	File	Global: Open/Save

- Perform a Data PivotTable on the data area with user as the row, GroupType as the Column, and count of users as the data element.



user	GroupType	Count of users
1	1	1
2	2	1
3	3	1
4	4	1
5	5	1
6	6	1
7	7	1
8	8	1
9	9	1
10	10	1
11	11	1
12	12	1
13	13	1
14	14	1
15	15	1
16	16	1
17	17	1
18	18	1
19	19	1
20	20	1
21	21	1
22	22	1
23	23	1
24	24	1
25	25	1
26	26	1
27	27	1
28	28	1
29	29	1
30	30	1
31	31	1
32	32	1
33	33	1
34	34	1
35	35	1
36	36	1
37	37	1
38	38	1
39	39	1
40	40	1
41	41	1
42	42	1
43	43	1
44	44	1
45	45	1
46	46	1
47	47	1
48	48	1
49	49	1
50	50	1
51	51	1
52	52	1
53	53	1
54	54	1
55	55	1
56	56	1
57	57	1
58	58	1
59	59	1
60	60	1
61	61	1
62	62	1
63	63	1
64	64	1
65	65	1
66	66	1
67	67	1
68	68	1
69	69	1
70	70	1
71	71	1
72	72	1
73	73	1
74	74	1
75	75	1
76	76	1
77	77	1
78	78	1
79	79	1
80	80	1
81	81	1
82	82	1
83	83	1
84	84	1
85	85	1
86	86	1
87	87	1
88	88	1
89	89	1
90	90	1
91	91	1
92	92	1
93	93	1
94	94	1
95	95	1
96	96	1
97	97	1
98	98	1
99	99	1
100	100	1

- Format the presentation sheets to point to the underlying table. Copy and Edit Paste Special Values and Transpose the results of the totals into the second presentation sheet.

Auditing Firm

AnyBank																																
Users and Groups																																
	Global - Accounting	Global - Administration	Global - App Ops	Global - App Users	Global - Branch 1 Users	Global - Domain Admins	Global - Domain Guests	Global - Domain Users	Global - Email Users	Global - Enterprise Admins	Global - Exchange Domain Servers	Global - Exchange Services	Global - Group Policy Creator Owners	Global - IdentAdmin	Global - Information Systems	Global - Internet Access	Global - Licensing	Global - Manual Exports	Global - NetScape Users	Global - Schema Admins	Global - SWSMSE Admins	Local - Administrators	Local - Backup Operators	Local - DiskAdmins	Local - Exchange Enterprise Servers	Local - Guests	Local - Print Operators	Local - Replicator	Local - Server Operators	Local - Users	Grand Total	
1033000-20-01-4999-A																																
abaptiste								1	1									1													3	
acomelius	1				1				1	1																					4	
adina									1	1																					3	
adictrephes			1						1	1																					3	
Administrator						1					1			1							1	1	1	1							6	
AdminSch								1																							1	
akeley					1			1	2	2							1		1												8	
akerchick	1				1				1	1																					4	
akerd				1				1	1	1																					4	
akern					1				1	1					1	1			1												5	
akial									1	1																					2	
akimberley									1	1								1													3	
aking									1	1																					2	
akinghom						1			1	1																					3	
akisley								1	1	1																					3	
akikakdv	1				1				1	1																					4	
alahey									1	1																					2	
alambourne									1	1																					2	
alamport					1				1	1																					3	
arcas									1	1												1									2	
arcprel									1	1												1									2	
ArcServe								1	1													1	1						1		4	
auditor								1	1																						2	
backup								1	1																						2	
backup_svc						1			1	1												1	1								3	
Bank						1			1	1																					2	
Bank1									1	1																					2	
CSR						1			1	1																					3	
CSR2									1	1																					2	
CSR3									1	1																					2	
CSR4									1	1																					2	
CSR5									1	1																					2	
doyonyklus					1				1	1																					3	
doesea									1	1								1													3	
diagwin						1			1	1					1	1	1			1		1									9	
diarstad									1	1																					2	
diimbio									1	1																					2	
dinnear									2	1																					3	
Domain Admins																			1												1	
Domain Admins																															1	
Domain Guests																															1	
Domain Users																															1	
domelius					1				1	1																					3	
doerachus									1	1									1												3	
dkay									2	1									1												4	
akeen									1	1																					2	
dkolto			1						1	1									1												4	
dkerchick									1	1																					2	
dkomard									1	1																					2	
dkerchor					1				1	1									1												4	
dkid									1	1																					2	
dkinghom									1	1																					2	
dkimny									1	1																					2	
dkup									1	1																					2	
dkamp									1	1									1												3	
dkamp									1	1																					2	
dkampont									1	1																					2	
emolad									1	1																					2	
emoladump									1	1																					2	
Enterprise Admins																						1									1	
Exchange Domain Servers																															1	
exch-backup-agent								1	1				1												1						5	
exch-new-agent								1	1																						2	
EXCH-SERVICEACCOUNT								1	1			1	1									1	1								6	
Fedline									1	1																					2	
Intlogn									1	1																					2	
Guest									1	1																					2	
Internal									1	1												1	1								2	

Users and Groups	AnyBank																															
	Global - Accounting	Global - Administration	Global - App/Ops	Global - App/Users	Global - Branch 1 Users	Global - Domain Admins	Global - Domain Guests	Global - Domain Users	Global - Email Users	Global - Enterprise Admins	Global - Exchange Domain Servers	Global - Exchange Services	Global - Group Policy Creator Owners	Global - IdentAdmin	Global - Information Systems	Global - Internet Access	Global - Lending	Global - Manual Errors	Global - NetScape Users	Global - Schema Admins	Global - SMS/MSE Admins	Local - Administrators	Local - Backup Operators	Local - DisAdmins	Local - Exchange Enterprise Servers	Local - Guests	Local - Print Operators	Local - Replicator	Local - Server Operators	Local - Users	Grand Total	
IUSR_DC1								1																	1							1
IUSR_Server2								1																								1
IUSR_Server3								1																								1
IUSR_Server4								1																								1
IUSR_Server5								1																								1
IUSR_Server6								1																								1
IUSR_Server7								1																								1
IUSR_Server8								1																								1
IUSR_Server9								1																								1
IWAM_DC1								1																								1
IWAM_Server2								1																								1
IWAM_Server3								1																								1
IWAM_Server4								1																								1
IWAM_Server5								1																								1
IWAM_Server6								1																								1
IWAM_Server7								1																								1
IWAM_Server8								1																								1
IWAM_Server9								1																								1
lrbtbt								1																								1
mlodochus	1		1					1	1																							1
mlkath	1							1																								1
mlkelly								1	1																							1
mlkempster								1	1									1														2
mlkennicot					2			2	2									1														7
mlkent					1			1	1									1														4
mlkeys								1										1														2
mlkooman					1			1	1																							4
mlksham								2	1																							3
mlkimberley								2	2									2														6
mlkingston	1	1						1	1																							4
mlkmsley				1				2	2									1														4
mlkukady				1				1	1									1														3
mlmacy			1			1		1	1					1	1	1						1										8
mlmimport				1				1	1																							3
mlmcp								1	1																							2
mlrst								1																								1
mlsternb								1																								1
mlsupervisor								1														1										2
mlsync Agent Account								1														1										2
mlTLR					1			1															1									2
mlTLR2								1																								1
mlTLR3								1																								1
mlTLR4								1																								1
mlTLR5								1																								1
mlInternetUser								1																								1
mlVEE_ADMIN								1														1	1				1					3
mlvendor						1		1														1	1									3
mlvince						1		1														1										2
mlvndr						1		1								1						1										3
Grand Total	9	6	5	18	5	16	1	117	55	1	1	2	1	3	3	5	18	3	2	1	1	18	10	1	1	16	1	1	2	1	324	

AnyBank			
Groups			
Global - Accounting	9	Global - Domain Users	117
Global - Administration	6	Global - Email Users	55
Global - App1Ops	5	Global - App1Users	18
Global - App1Users	18	Global - Lending	18
Global - Branch1 Users	5	Local - Administrators	18
Global - Domain Admins	16	Global - Domain Admins	16
Global - Domain Guests	1	Local - Guests	16
Global - Domain Users	117	Local - Backup Operators	10
Global - Email Users	55	Global - Accounting	9
Global - Enterprise Admins	1	Global - Administration	6
Global - Exchange Domain Servers	1	Global - App1Ops	5
Global - Exchange Services	2	Global - Branch1 Users	5
Global - Group Policy Creator Owners	1	Global - Internet Access	5
Global - identiadmin	3	Global - identiadmin	3
Global - Information Systems	3	Global - Information Systems	3
Global - Internet Access	5	Global - Manual Editors	3
Global - Lending	18	Global - Exchange Services	2
Global - Manual Editors	3	Global - NetScape Users	2
Global - NetScape Users	2	Local - Server Operators	2
Global - Schema Admins	1	Global - Domain Guests	1
Global - SMSMSE Admins	1	Global - Enterprise Admins	1
Local - Administrators	18	Global - Exchange Domain Servers	1
Local - Backup Operators	10	Global - Group Policy Creator Owners	1
Local - DnsAdmins	1	Global - Schema Admins	1
Local - Exchange Enterprise Servers	1	Global - SMSMSE Admins	1
Local - Guests	16	Local - DnsAdmins	1
Local - Print Operators	1	Local - Exchange Enterprise Servers	1
Local - Replicator	1	Local - Print Operators	1
Local - Server Operators	2	Local - Replicator	1
Local - Users	1	Local - Users	1
Grand Total	324	Grand Total	324

Observations on User / Group Statistics:

This gives a picture of the groups of authenticated users. Reviewing it allows us to see the number and specific users assigned to key groups. It should be reviewed with a member of operational management.

- There is only one (1) Schema and Enterprise Admin. This does not allow for a backup if that user should become locked out.
- There are sixteen (16) Domain Admins (16% of the accounts). This is not best practice. Domain Admins have the “keys to the kingdom” and can change other Domain Admin’s rights. Many sources recommend (renaming “Administrator”) creating Administrative accounts for individual’s to use when Domain Administration tasks (or Enterprise or Schema extensions) are being performed. This allows better tracking of those tasks and prevents inadvertent changes while logged in with a regular (lower-level authority) account.

4.2 Review Group Policy Objects and Assignment

Running the GPO Management Console against the domain on a laptop with administrative access yielded the following GPO resultant report:

The screenshot displays the 'Group Policy Results' window for a user named 'Administrator' on a computer named 'DCVAIO'. The window is divided into several sections:

- Computer Configuration Summary:** Shows the computer name 'DCVAIO', domain 'dcvaio.local', and the GPO 'Default Domain Policy' applied.
- Group Policy Objects:** Lists applied and denied GPOs. The 'Default Domain Policy' is applied, while 'Local Group Policy' is denied.
- Security Group Membership:** Shows the user is a member of the 'Administrators' group.
- WMF Filters:** Shows the 'None' filter is applied.
- Component Status:** Lists the status of various components like 'Security Policy', 'Network Policy', and 'System Policy'.
- User Configuration Summary:** Shows the user name 'Administrator', domain 'dcvaio.local', and the GPO 'Default Domain Policy' applied.
- Group Policy Objects:** Lists applied and denied GPOs. The 'Default Domain Policy' is applied, while 'Local Group Policy' is denied.
- WMF Filters:** Shows the 'None' filter is applied.
- Component Status:** Lists the status of various components like 'Security Policy', 'Network Policy', and 'System Policy'.
- Computer Configuration:** Shows the status of various settings like 'Security Settings', 'Network Settings', and 'System Settings'.
- Security Settings:** Lists the status of various security settings like 'Account Policies', 'Local Policies', and 'Network Security'.
- Account Policies:** Shows the status of various account policies like 'Password Policy', 'Account Lockout Policy', and 'Local Policies'.
- Local Policies:** Shows the status of various local policies like 'Network Security', 'Public Key Policies', and 'Public Key Policies'.
- Network Security:** Shows the status of various network security settings like 'Network Security', 'Public Key Policies', and 'Public Key Policies'.
- Public Key Policies:** Shows the status of various public key policies like 'Public Key Policies', 'Public Key Policies', and 'Public Key Policies'.

This gives a picture of the policies that are delivered to a particular user (Administrator) when logging onto a particular computer (Sony Vaio). Here you can see the Security Group membership, the applied and denied Group Policies, and the Group Policy responsible for each setting applied.

Observations on Group Policy Objects:

- Notice that the Default Domain Policy is the “winning GPO” for several of the security related policies.
- Overall, it appears that Group Policy Objects are only being used for a minimum number of the settings that are available. A review of the Security settings section reveals that the “Default Domain Policy” was the only policy applied here. It indicates that:
 - 3 passwords are remembered
 - Maximum password age is 90 days
 - Minimum password age is 0 days
 - Minimum password length is 4 characters
 - Password complexity requirement is Disabled
 - Account lockout duration is 1440 minutes (24 hours)
 - Account lockout threshold is 5 attempts
 - Reset account lockout counter after 1440 minutes
- The minimum password length of 4 is weak. Enabling password complexity requires the password to contain at least three of the four categories of upper case letters, lower case letters, numbers, and special characters (which is disabled). Because the minimum password age is 0 and 3 passwords are remembered, a user can change his/her password four times in succession back to the original password on the fourth change.
- Lockout will occur after the fifth incorrect attempt at a password in any given 24 hour period. The counter will reset 24 hours after the last invalid attempt. This should be sufficient for most accounts, but consideration should be given to an infinite reset time (requires manual reset by a Domain Administrator) for accounts with higher levels of authority. This can be accomplished by keeping Domain Administrators and other groups with elevated authority in a separate Organizational Unit with its own Group Policy Object.

Group Policy Modeling was run against several users, two examples are shown here for illustration:

Group Policy Modeling			
domainname\ekimsey			
Data collected on: 1/26/2005 11:56:04 AM			
Summary			hide all
Computer Configuration Summary			hide
No data available.			
User Configuration Summary			hide
General			hide
User name	domainname\ekimsey		
User container	ad.domainname.com/Vest Branch		
Domain	ad.domainname.com		
Shutlkr processing	No		
Localhost processing	No		
Group Policy Objects			hide
Applied GPOs			hide
Name	Link Location	Revision	
Default Domain Policy	ad.domainname.com	4D (3) Syntex (2)	
Default Toler	ad.domainname.com/Vest Branch	4D (3) Syntex (2)	
Denied GPOs			hide
Name	Link Location	Reason Denied	
None			
Simulated security group membership			hide
domainname\ekimsey BUILTIN\Users domainname\Ekimsey Users Everyone BUILTIN\The Windows 2000 Compatible Access NT AUTHORITY\Authenticated Users NT AUTHORITY\This Organization domainname\Local Toler			
WMI Filters			hide
Name	Value	Reference GPO(s)	
None			
Component Status			hide
Component Name	Status		
Group Policy Infrastructure	Success		
Internet Explorer Branding	Success		
Registry	Success		
Computer Configuration			hide
No data available.			
User Configuration			hide
Windows Settings			hide
Internet Explorer Maintenance			hide
Connection/Proxy Settings			hide
Winning GPO			Default Domain Policy
Enable proxy settings			
Protocol	Server	Port	
HTTP	192.168.1.1	80	
Secure	192.168.1.1	80	
FTP	192.168.1.1	80	
Gopher	192.168.1.1	80	
Socket	192.168.1.1	80	
Exceptions			
Do not use proxy server for addresses beginning with			
Do not use proxy server for local (internal) addresses			Enabled
Administrative Templates			hide
Control Panel			hide
Policy	Setting	Winning GPO	
Prohibit access to the Control Panel	Enabled	Default Toler	
Start Menu and Taskbar			hide
Policy	Setting	Winning GPO	
Remove Fast menu from Start Menu	Enabled	Default Toler	

© SANS Institute 2005

Group Policy Modeling			
domainname\akinghorn			hide all
Data collected on: 1/26/2005 11:55:19 AM			hide
Summary			hide
Computer Configuration Summary			hide
No data available.			
User Configuration Summary			hide
General			hide
User name	domainname\akinghorn		
User container	ad.domainname.com/East Branch		
Domain	ad.domainname.com		
Slowlink processing	No		
Logon processing	No		
Group Policy Objects			hide
Applied GPOs			hide
Name	Link Location	Revision	
Default Domain Policy	ad.domainname.com	40 (2), 50 (2)	
Denied GPOs			hide
Name	Link Location	Reason Denied	
Default Teller	ad.domainname.com/East Branch	Disabled Link	
Simulated security group membership			hide
domainname\akinghorn BUILTIN\Users domainname\Domain Users Everyone BUILTIN\The Windows 2000 Compatible Access NT AUTHORITY\Authenticated Users NT AUTHORITY\This Organization domainname\East Teller			
WMI Filters			hide
Name	Value	Reference GPO(s)	
None			
Component Status			hide
Component Name	Status		
Group Policy Infrastructure	Success		
Internet Explorer Branding	Success		
Computer Configuration			hide
No data available.			
User Configuration			hide
Windows Settings			hide
Internet Explorer Maintenance			hide
Connections/Proxy Settings			hide
Winning GPO			Default Domain Policy
Enable proxy settings			
Protocol	Server	Port	
HTTP	192.168.1.1	80	
Secure	192.168.1.1	80	
FTP	192.168.1.1	80	
Gopher	192.168.1.1	80	
Socks	192.168.1.1	80	
Exceptions			
Do not use proxy server for addresses beginning with		Enabled	
Do not use proxy server for local (intranet) addresses			

Observations on Group Policy Object Modeling:

ekinney

- Specifically, notice that the “Default Teller” would be the winning GPO for Administrative Templates that “Prohibit access to the Control Panel” and “Remove Run menu from the Start Menu”. Also, no “Denied GPO’s” exist, meaning that there would be nothing to prevent a GPO from being inherited by this account during log on.

akinghorn

- Here, notice that the same Default Teller GPO that would block access to the Control Panel and Run commands is being denied. This user would have those rights after logon. The “Denied GPO’s” section shows the Default Teller GPO is a “Disabled Link”. In this case, there should is not a legitimate reason for the denial. The account should be investigated to determine if the GPO is mis-configured or if this user (or another user with the rights to modify) has the explicitly denied the inheritance. In general, no GPO’s should be denied, so a GPO denial should be a red flag to the auditor.

Password, account lockout, auditing, user access to services that allow the Run command and Control Panel, access to removable devices, Proxy settings, and more should all be delivered with Group Policy Objects.

4.3 Review Password Strength

[illegible]

Microsoft Excel - GSNA-User Review-2005-PasswordAudit.xls						
File Edit View Insert Format Tools Data Window Help Adobe PDF						
A B C D E F G						
1	Count of Rows	Crack Method				
2	Crack Method	Brute Force	Dictionary	Hybrid	NA	User Info
3	NA					
4	a- Under 1 minute	26		2	11	11
5	b- Under 1 hour		5			29
6	c- Under 4 hours	6				6
7	d- Under 24 hours	6				6
8	e- 1-2 days	2				2
9	f- 2-3 days	2				4
10	Grand Total	34	26	9	11	11
11						
12						
13						
14						
15						
16						
17	Count of Rows	Crack Method				
18	Crack Method	Brute Force	Dictionary	Hybrid	NA	User Info
19	NA					
20	a- Under 1 minute	13	21	2	13	13
21	b- Under 1 hour			6		24
22	c- Under 4 hours	5				5
23	d- Under 24 hours	5				5
24	e- 1-2 days	2				2
25	f- 2-3 days	4				4
26	Grand Total	27	27	8	13	13
27						

Microsoft Excel - GSNA-User Review-2005-PasswordAudit.xls						
File Edit View Insert Format Tools Data Window Help Adobe PDF						
A B C D E F G						
1	Auditing Firm					(11/28/06)
2						
3	AnyBank					
4	Password Cracking Statistics					
5	All Active User Accounts					
6						
7	Crack Method					
8	TimeFrame	Brute Force	Dictionary	Hybrid	NA	User Info
9	NA		26	2	11	11
10	a- Under 1 minute	15		6		11
11	b- Under 1 hour		5			21
12	c- Under 4 hours	6				6
13	d- Under 24 hours	6				6
14	e- 1-2 days	2				2
15	f- 2-3 days	4				4
16	Grand Total	34	26	8	11	11
17						
18						
19						
20						
21	All User Accounts					
22						
23	Crack Method					
24	TimeFrame	Brute Force	Dictionary	Hybrid	NA	User Info
25	NA		27	2	13	13
26	a- Under 1 minute	18		6		12
27	b- Under 1 hour		5			24
28	c- Under 4 hours	5				5
29	d- Under 24 hours	5				5
30	e- 1-2 days	2				2
31	f- 2-3 days	4				4
32	Grand Total	37	27	8	13	12
33						
34						

Microsoft Excel - GSNA-User Review-2005-PasswordAudit.xls						
File Edit View Insert Format Tools Data Window Help Adobe PDF						
A1 Auditing Firm						
Financial Institution						
Password List						
Seq	Username	Pwd Length	Crack Method	Crack Time Hours	Crack Time Minutes	TimeFrame
1	Administrator	0	Hybrid		23	b- Under 1 hour
2	macy	0	Brute Force	10	6	e- Under 24 hours
3	AnsSene	8	User Info		<1	a- Under 1 minute
4	ajist	6	Brute Force	69	46	g- 2-3 days
5	backup	6	User Info		<1	a- Under 1 minute
6	backup_exe	6	Brute Force		26	b- Under 1 hour
7	aray	5	Dictionary		<1	a- Under 1 minute
8	aynasrus	6	Dictionary		<1	a- Under 1 minute
9	shipp	7	Brute Force	53	14	g- 2-3 days
10	avingham	5	Dictionary		<1	a- Under 1 minute
11	mkingston	6	Dictionary		<1	a- Under 1 minute
12	mkimberley	6	Brute Force		26	b- Under 1 hour
13	adana	6	Dictionary		<1	a- Under 1 minute
14	awercher	8	Dictionary		<1	a- Under 1 minute
15	avonard	6	Dictionary		<1	a- Under 1 minute
16	CSR	None	N/A			N/A
17	CSR2	None	N/A			N/A
18	CSR3	None	N/A			N/A
19	CSR4	None	N/A			N/A
20	CSR5	None	N/A			N/A
21	mabodera	0	Hybrid		16	b- Under 1 hour
22	skreen	6	Brute Force		41	b- Under 1 hour
23	skreen	5	Dictionary		<1	a- Under 1 minute
24	mksman	6	Dictionary		<1	a- Under 1 minute
25	avert	7	Brute Force	45	16	f- 1-2 days
26	avert	7	Brute Force	54	45	g- 2-3 days
27	mkenicott	6	Brute Force		43	b- Under 1 hour
28	mkenicott	6	Dictionary		<1	a- Under 1 minute
29	dforyopus	10	Dictionary		<1	a- Under 1 minute
30	avingham	5	Brute Force		26	b- Under 1 hour
31	mkeby	5	Brute Force		26	b- Under 1 hour
32	emailed	6	Dictionary		<1	a- Under 1 minute
33	emailedump	9	User Info		<1	a- Under 1 minute
34	aditrophes	4	Dictionary		<1	a- Under 1 minute
35	exch-backup-agent	6	Hybrid		29	b- Under 1 hour
36	exch-backup-agent	5	Brute Force		26	b- Under 1 hour
37	EXCH-SERVICE-ACCOUNT	5	Brute Force		26	b- Under 1 hour
38	king	9	Hybrid		21	b- Under 1 hour
39	Dank	3	User Info		<1	a- Under 1 minute
40	Bunk1	4	User Info		<1	a- Under 1 minute
41	frisan	7	User Info		<1	a- Under 1 minute
42	Internal	None	N/A			N/A
43	slamboune	5	Brute Force		26	b- Under 1 hour
44	makiakaly	0	Dictionary		<1	a- Under 1 minute
45	mkenley	0	Dictionary		<1	a- Under 1 minute
46	mkenid	6	Brute Force		27	b- Under 1 hour
47	disinner	5	User Info		<1	a- Under 1 minute
48	mkenberley	5	Brute Force		26	b- Under 1 hour
49	avastista	5	Brute Force	1	41	c- Under 4 hours
50	mkenicott	6	Brute Force		40	b- Under 1 hour
51	avilbey	8	Brute Force	20	66	e- Under 24 hours
52	avilbey	5	Dictionary		<1	a- Under 1 minute
53	avimberley	6	Dictionary		<1	a- Under 1 minute
54	slamport	6	Brute Force	1	36	c- Under 4 hours
55	slamport	5	Dictionary		<1	a- Under 1 minute
56	ind	6	Brute Force		69	b- Under 1 hour
57	disimble	6	Brute Force	1	4	c- Under 4 hours
58	disinner	5	Dictionary		<1	a- Under 1 minute
59	mkeys	6	Dictionary		<1	a- Under 1 minute
60	apores	9	Brute Force	9	46	e- Under 24 hours
61	apropri	7	Brute Force	9	66	e- Under 24 hours
62	avikakaly	5	Brute Force		26	b- Under 1 hour
63	mkuham	7	Brute Force	15	12	e- Under 24 hours
64	Recep	5	User Info		<1	a- Under 1 minute
65	avinsley	0	Dictionary		<1	a- Under 1 minute
66	dringens	6	Hybrid		21	b- Under 1 hour
67	alisher	7	Brute Force	2	17	c- Under 4 hours
68	dest	5	User Info		<1	a- Under 1 minute
69	mkenmaster	8	Brute Force	20	52	e- Under 24 hours
70	avendrick	6	Brute Force	1	26	c- Under 4 hours
71	mkuham	10	Hybrid		<1	a- Under 1 minute
72	avornelles	13	Brute Force	15	28	e- Under 24 hours
73	avilbey	5	Dictionary		<1	a- Under 1 minute
74	statements	10	User Info		<1	a- Under 1 minute
75	diarsted	8	Dictionary		<1	a- Under 1 minute
76	slamport	0	Dictionary		<1	a- Under 1 minute
77	avinner	5	Dictionary		<1	a- Under 1 minute
78	Sync Agent Account	5	Brute Force		26	b- Under 1 hour
79	aray	10	Brute Force	33	54	f- 1-2 days
80	avendrick	6	Brute Force	60	7	g- 2-3 days
81	TLR	None	N/A			N/A
82	TLR2	None	N/A			N/A
83	TLR3	None	N/A			N/A
84	TLR4	None	N/A			N/A
85	TLR5	None	N/A			N/A
86	avornelles	0	Hybrid		16	b- Under 1 hour
87	mkeith	0	Dictionary		<1	a- Under 1 minute
88	slamb	10	Hybrid		<1	a- Under 1 minute
89	VBE ADMIN	7	Brute Force	15	24	e- Under 24 hours
90	Vacca	5	User Info		<1	a- Under 1 minute
91	AdminSch	None	N/A			N/A
92	auditor	0	Dictionary		<1	a- Under 1 minute
93	Fedline	7	User Info		<1	a- Under 1 minute
94	Guest	None	N/A			N/A
95	indr	5	Brute Force		26	b- Under 1 hour
96	vender	5	Brute Force		26	b- Under 1 hour
97	Supervisor	5	Brute Force		26	b- Under 1 hour

Observations on User Passwords:

This allows us to determine the time window of risk should passwords be compromised.

- All passwords were cracked within 4 days
- Four (4) Domain Administrator level passwords were cracked in under a minute, eight (8) in under an hour, and three (3) more in under a day. This means that the password strength is poor for accounts with a very high level of authority.
- Twenty seven (27) of the 97 accounts (38%) were cracked using a Dictionary.
- Twelve (12) (12%) were cracked using some form of the user account ID
- Thirty seven (37) (38%) were cracked using Brute Force
- Forty seven (47) (48%) were cracked using some combination of user account information and Dictionary (did not have to resort to Brute Force)

© SANS Institute 2005, Author retains full rights.

4.4 Institution Policies related to passwords and users

PURGE POLICY

The Human Resource Department will notify the Information Systems Manager on the same day, of any and all terminated employees. Upon notification, the Information Systems Manager will remove immediately, from the Windows NT system, the User ID and associated passwords of all terminated employees.

PROCEDURES

1. The Human Resource Department will immediately notify the Information Systems Manager or his subordinate the same day an employee terminates from the bank.
2. System security procedures will call for the Information Systems Manager or his subordinate to remove the User ID and Passwords from the network as well as the e-mail system of the terminated employee immediately upon their separation from the bank.
3. The Security Officer will remove the terminated employee from accessing the Application System.
4. The Human Resources department will immediately notify the Information Systems Manager of any change in employee job function that would require the removal of Administrator privileges from that employee's user profile.

PASSWORD POLICY

Passwords are the primary means of correlating the user's identity to the system approval control process. Combined with the User's ID, the password will provide approved users with initial system access. The password will be selected by the system user and is to be known only by that person. The format of the password is free form, as long as it conforms to the following formatting rules.

PROCEDURES

1. Passwords will be comprised of a combination of alpha and numeric characters.
2. Repetitive character strings, such as 1111, 1234, ABCD and AAAA are not to be used.
3. The size of the password may range from a minimum of six (6) to a maximum of fifteen (15) characters in length.
4. Passwords are not to reference the names of any spouse, children, pet, first name or any other such name that may easily be associated with a specific user.
5. Passwords for all system users shall be changed every 90 days.
6. Whenever a password is being changed, the user must select a password different from that, which was just used.
7. Passwords may not be duplicated among system users, but must be unique.
8. Passwords may not be the same as the User ID, except for initial access.

Observations on Related Policies:

Policy review allows us to put the review of users, groups, Active Directory GPOs, and Password assessments into perspective of the stated objectives of the institution.

- The removal of users promptly of their termination should be reviewed against the password age report. It appears there may be several accounts in question.
- Over fifty (50) of the passwords violate the requirement to have a combination of letters and numbers.
- Over fifty (50) of the accounts have passwords that have not been changed in the required 90 day window.
- Several of the accounts have passwords that appear to violate the prohibition of names.

© SANS Institute 2005, Author retains full rights.

4.4 Conclusions

This Windows 2000/2003 Active Directory Domain is not secure from an account configuration and password perspective. If the physical access to the network has any vulnerability, the entire network and all of its information is vulnerable. Specific comments that would make the Executive Summary (written in a politically correct way) with specific recommendations for remediation are:

- Too many accounts have Domain Admin authority
- Password Policy is being violated
- Passwords, in general, are insecure
- Group Policy Objects are not implemented effectively
- Active Directory Password configurations are weak and do not match institution policy

© SANS Institute 2005, Author retains full rights.

References

University of Washington's School of Medicine Windows Server 2000 Security
<https://security.uwmedicine.org/Docs/Procs/MSWebsiteWin2000ServerSecurity.htm>

Kathy Ivens Getting Started with Windows Administration - InstantDoc #40721
Windows IT Pro
<http://www.windowsitpro.com/Windows/Article/ArticleID/40721/40721.html>

FFIEC Information Security - IT Examination Handbook December 2002
http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#infosec

Microsoft Technet 10 Immutable Laws of Security
<http://www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.aspx>

SANS Institute Top Vulnerabilities to Windows Systems
<http://www.sans.org/top20/#w5>

Peter Tippet, Chief Technology Officer of Reston, Virginia-based TruSecure™ Corp.
Calculating Your Security Risk
http://www.theciostore.com/watchit_product.asp?id=196

Microsoft Corporation Security Risk Management Guide Chapter 4: Assessing Risk
<http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/srsgch04.msp#EAAA>

Microsoft Corporation Group Policy Management Console Help Text

© SANS Institute 2005 Author retains full rights.