The San Francisco Chapter of ISACA proudly presents...
SF ISACA 2007 Fall Conference
IT Audit
Information Security
IT Governance
Risk Management
Compliance

Security – A System Settings Perspective

By

Rodney Kocot,
Systems Control and Security, Incorporated

For

The San Francisco Chapter
of the
Information Systems Audit and Control Association

September 18, 2007

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Table of Contents

1. Introduction

1.1. Session Description:

This session provides an overview of system settings that must be reviewed in order to provide an opinion regarding the level of security implemented on a system. A method for determining the scope of a review and an approach for obtaining the necessary information will be discussed. A process for identifying system settings will be explained. System settings for several operating systems will be discussed. Examples of obtaining and reviewing information will be shown.

1.2. Instructor:

Rodney Kocot is a Technical IT Audit Consultant for Systems Control and Security Incorporated. Rodney provides technical audit training and consulting services for corporations world wide. He has been an IT Auditor for 23 years. Responsibilities have included technical audits of operating systems, network audits, application audits and audit software development.

Seminars presented by Rodney include automation techniques, software, and audit programs. Topics include programming, audit and security automation, auditing minicomputers, and securing minicomputers. He has performed AS/400, LAN, Tandem Guardian, Unisys, Unix and OpenVMS audits using Visual Basic and Microsoft Access to automate the reviews.

Rodney has been involved in the Information Systems Audit and Control Association and has held various positions in the Los Angeles and San Francisco chapters including President, Executive Vice President, Vice President, and Secretary.

2. Audit Approaches

In 23 years of IS Auditing I have observed many approaches to auditing the security of operating systems and applications. The level of confidence that all significant issues were identified differs significantly depending on the approach used. Yet many reports do not indicate how the review was performed or the level of confidence that all issues within the scope of the review were identified. Additionally, there are easily determined metrics that can be used to determine the level of operating system security. For example the percentage of unprotected files/objects on the system is a good indicator of the level of security but it is seldom reported.

Three of the more common approaches to security audits are described below:

2.1. *Audit by interview:*

This approach relies solely on interview and is common. Many auditors use this approach because it is doable with in the budget and time allocated. The auditor asks the client a series of questions and asks for documentation to support the answers. The report indicates a full scope audit was performed yet the depth was superficial. An example of a Q and A session is
Auditor: “Are your files protected?”
Client: “Yes.”
Auditor: “How do you know your files are protected?”
Client: “We periodically review the files to ensure they are protected.”
Auditor: “Please provide me with a sample listing that shows the files are protected.”
Client: “Done.” (The listing shows a directory with protected files. The listing might possibly show the only directory on the system that has protected files.)

2.2. *High level scan of selected listings:*

This approach relies on sampling. A sample of userids, files, system parameters, and other objects is printed and reviewed. A commonly used audit program from the internet requires 16 directories and files/objects be reviewed to complete the audit. To put things in perspective the type of system that this program pertains to usually has 20 to 100 thousand objects. The 16 objects reviewed are the most critical and are currently included in most audit programs. However, how confident can an organization be about the security of objects on the system when only 16 out of tens of thousands are reviewed?

2.3. *Detailed automated review of all relevant listings:*

This approach requires that detailed and complete listings be generated and reviewed for all the control and security related objects on the system. This approach uses the technology to audit the technology. Once the risk assessment, audit program, and queries are researched and developed, this type of review can be performed in a very short period of time by a knowledgeable auditor. The following listings are generated and copied into a database for analysis:

(a) all userids and their attributes,
(b) all objects on the system with their owner, security, and all other attributes,
(c) all privileged programs and their attributes,
(d) all system settings,
(e) all network settings,

When the above listings are loaded into a database, queries are executed which show exceptions to generally accepted security standards. Examples of possible exceptions are:

(a) number/percentage of application users not restricted to application menus,
(b) number/percentage of users with excessive privileges,
(c) number/percentage of unprotected objects,
(d) number/percentage of unprotected production programs and data files, (Reference the side bar regarding unprotected programs.)
(e) number/percentage of unprotected privileged programs,
(f) inappropriate system settings, and
(g) inappropriate network settings.

3. Background Information

Obtain organization charts and phone lists of all individuals involved in the LAN application. Include the following groups for each system used in the application:

- systems
- operations
- programming
- users

Obtain inventory listings for all equipment and software in the IT environment

4. Risk Assessment

- Using background information and documentation, identify and quantify risks
- Interview managers from all IT environment areas to identify and quantify risks
- Interview managers from areas supported by IT
- Identify resources available for the audit
- Rank risks and develop audit program

5. Areas to Be Included In a Comprehensive System Review

1. Physical Security
2. System Settings
3. System Startup and Shutdown Programs
4. Network Settings
5. Network Startup and Shutdown Programs
6. User Administration Settings
7. User Groups
8. User Login and Logoff Scripts
9. Device Security Settings
10. Object Security Settings
11. Privileged Program Settings
12. Dial-up Settings
13. Logging and Monitoring
14. Backup and Recovery
15. IT and User Security Awareness
16. Change Management
17. Application Security
18. Add-on Security Products

5.1. Physical Security

1. Physically inspect the buildings and areas which house any components of the IT environment
2. Determine whether physical security is adequate
3. Determine whether power conditioning and UPS equipment is adequate and appropriate for each component of the IT environment
4. Determine whether fire prevention and suppression programs and equipment are adequate
5. Inventory assets

Did I mention Inventory Assets?

- Hardware
- Software
- Staff
- Documentation - Obtain access to documentation for the following:
    - Application software
    - Data bases
    - Print servers
    - Communication servers
    - Hardware documentation for each system used
    - Software documentation for each operating system used
    - Hardware and software documentation for each network component
- Corporate knowledge base of risks, controls, issues, …

5.2. System Settings

- Identify configuration programs, files, and parameters
- Determine which programs, files, and parameters have audit or security significance and determine appropriate contents and values
- Verify system settings are set to appropriate values.
- Verify that configuration files and their directories and devices are adequately protected

For each system software and application software product identify system settings that could impact security and operations. Identifying system settings in Unix and Windows environments is a SIGNIFICANT EFFORT since the settings are scattered all over the system and numerous utilities and commands must be used to obtain the values of poorly documented system settings.

5.2.1. OS400

System Values

5.2.2. Windows

Baseline Security Analyzer

Windows 2000 Security Hardening Guide

While Windows can not be secured to prevent web sites from installing software, there are many areas containing system settings that should be reviewed.

5.2.2.1. SET Command

```
C:\Documents and Settings\Rodney>set
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\Rodney\Application Data
CLIENTNAME=Console
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=ONTLT01
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Documents and Settings\Rodney
LOGONSERVER=\\ONTDC1
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 13 Stepping 8, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=0d08
ProgramFiles=C:\Program Files
PROMPT=$P$G
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\DOCUME~1\Rodney\LOCALS~1\Temp
TMP=C:\DOCUME~1\Rodney\LOCALS~1\Temp
USERDNSDOMAIN=SYSSECURE.COM
USERDOMAIN=SYSSECURE
USERNAME=rodney
USERPROFILE=C:\Documents and Settings\Rodney
windir=C:\WINDOWS

C:\Documents and Settings\Rodney>
```

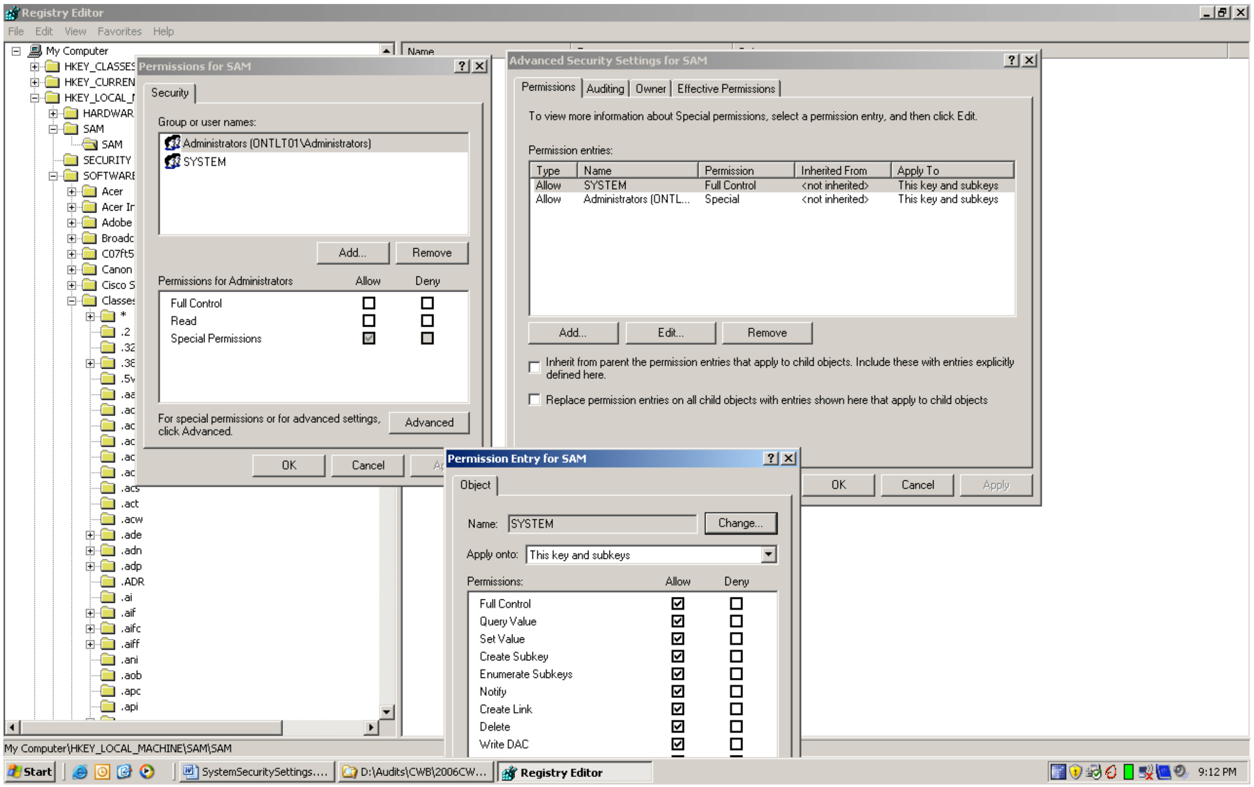
5.2.2.2. INI and Other Configuration Files

Ini and configuration files often contain userids and passwords in a large corporate environment.

```
[ApplicationName]
ServerName=PASAPP1
DatabaseName=APP1DB
LoginDatabaseName=Editor
UserName=Editor
Password=Editor
```

5.2.2.3. Registry

Cautiously use Regedit or regedt32 depending on your version of Windows to view, modify and dump the registry. As an auditor NEVER modify a production system.



Permissions for SAM

Security

Group or user names:

Administrators (ONTLT01\Administrators)
SYSTEM

Add... Remove

Permissions for Administrators	Allow	Deny
Full Control	□	□
Read	□	□
Special Permissions	☑	□

For special permissions or for advanced settings, click Advanced. Advanced

OK Cancel

Advanced Security Settings for SAM

Permissions | Auditing | Owner | Effective Permissions

To view more information about Special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	SYSTEM	Full Control	<not inherited>	This key and subkeys
Allow	Administrators (ONTL...	Special	<not inherited>	This key and subkeys

Add... Edit... Remove

□ Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here.

□ Replace permission entries on all child objects with entries shown here that apply to child objects

OK Cancel Apply

Permission Entry for SAM

Object

Name: SYSTEM Change...

Apply onto: This key and subkeys

Permissions:	Allow	Deny
Full Control	☑	□
Query Value	☑	□
Set Value	☑	□
Create Subkey	☑	□
Enumerate Subkeys	☑	□
Notify	☑	□
Create Link	☑	□
Delete	☑	□
Write DAC	☑	□

My Computer\HKEY_LOCAL_MACHINE\SAM\SAM

5.2.2.4. Group Policy Objects (GPO)

The Group Policy Object (GPO) Editor or the Group Policy Management Console are used to manage Group Policy Objects.
Group Policy Objects can be exported to an MS Excel file.
Group Policy Objects are assigned to users at logon and to workstations at boot.
The GPO hierarchy is Local > Site > Domain > OU > OU > OU > …
Inheritance of GPO settings goes down the list.
Lower levels can block non-enforced settings.
Higher levels can enforce settings down through the organization.

GPRESULT can be used to show what GPOs

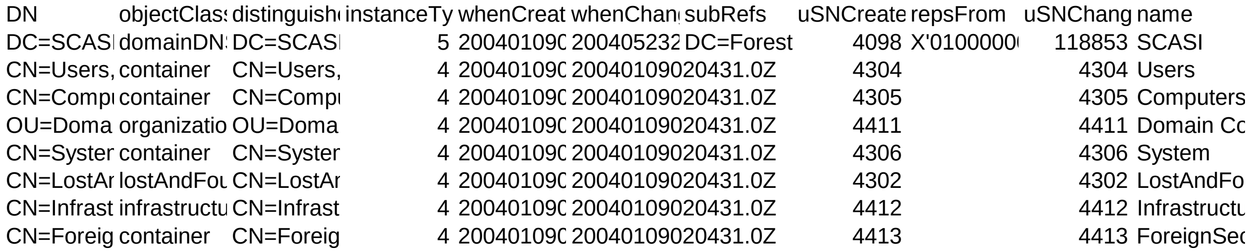
```
C:\Documents and Settings\rodney.kocot.adm>gpresult
Microsoft (R) Windows (R) 2000 Operating System Group Policy Result tool
Copyright (C) Microsoft Corp. 1981-1999

Created on Wednesday, January 19, 2005 at 11:42:40 PM

Operating System Information:

Operating System Type:          Professional
Operating System Version:       5.0.2195.Service Pack 4
Terminal Server Mode:           Not supported

###############################################################

  User Group Policy results for:

  SCASI\rodney.kocot.adm

  Domain Name:          SCASI
  Domain Type:          Windows NT v4

  Roaming profile:      (None)
  Local profile:        C:\Documents and Settings\rodney.kocot.adm

  The user is a member of the following security groups:

LookupAccountSid failed with 1789.
        \Everyone
        BUILTIN\Users
        BUILTIN\Administrators
        NT AUTHORITY\INTERACTIVE
        NT AUTHORITY\Authenticated Users
        \LOCAL
LookupAccountSid failed with 1789.

###############################################################

Last time Group Policy was applied: Wednesday, January 19, 2005 at 11:26:17
PM
```

```
Group Policy was applied from: systems-scasi.SCASI.com

===============================================================
The user received "Scripts" settings from these GPOs:

        New Group Policy Object

###############################################################

  Computer Group Policy results for:

  SCASI\WLSCASI0004$

  Domain Name:          SCASI
  Domain Type:          Windows NT v4

  The computer is a member of the following security groups:

        BUILTIN\Administrators
        \Everyone
        BUILTIN\Users
        NT AUTHORITY\NETWORK
        NT AUTHORITY\Authenticated Users
LookupAccountSid failed with 1789.
LookupAccountSid failed with 1789.

###############################################################

Last time Group Policy was applied: Wednesday, January 19, 2005 at 11:28:17
PM
Group Policy was applied from: systems-scasi.SCASI.com

===============================================================

The computer received "Registry" settings from these GPOs:

        Local Group Policy
        Default Domain Policy

===============================================================
The computer received "Security" settings from these GPOs:

        Local Group Policy
        Default Domain Policy

===============================================================
The computer received "EFS recovery" settings from these GPOs:

        Local Group Policy
        Default Domain Policy

===============================================================
The computer received "Application Management" settings from these GPOs:
        New Group Policy Object

C:\Documents and Settings\rodney.kocot.adm>
```

5.2.2.5. Active Directory Settings and Data

Active Directory permits domain administrators to set policies governing everything from whether or not users can customize their desktops to how often hard disks are defragmented to who can access what how and when.

Active Directory Dump Utilities - LDIFDE

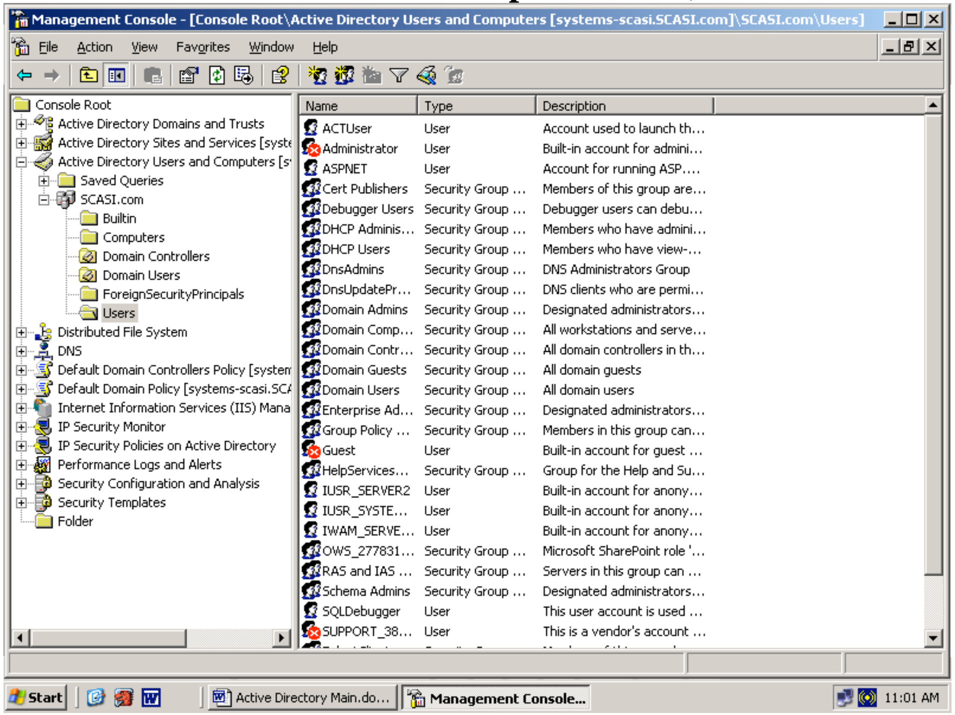


DN	objectClas	distinguish	instanceTy	whenCreat	whenChan	subRefs	uSNCreate	repsFrom	uSNChang	name
DC=SCAS	domainDN	DC=SCAS	5	200401090	200405232	DC=Forest	4098	X'010000	118853	SCASI
CN=Users,	container	CN=Users,	4	200401090	20040109020431.0Z		4304		4304	Users
CN=Comp	container	CN=Comp	4	200401090	20040109020431.0Z		4305		4305	Computers
OU=Doma	organizatio	OU=Doma	4	200401090	20040109020431.0Z		4411		4411	Domain C
CN=Syster	container	CN=Syster	4	200401090	20040109020431.0Z		4306		4306	System
CN=LostAr	lostAndFou	CN=LostAr	4	200401090	20040109020431.0Z		4302		4302	LostAndFo
CN=Infrast	infrastructu	CN=Infrast	4	200401090	20040109020431.0Z		4412		4412	Infrastructu
CN=Foreig	container	CN=Foreig	4	200401090	20040109020431.0Z		4413		4413	ForeignSe

Microsoft Management Console (MMC)

MMC is an easy to use console that can be extended by adding your own screens (snap-ins) for Active Directory management using the API(s) and by scripting.

Hundreds of snap-ins already exist for managing Active Directory. Some of the more commonly used will be discussed below.


Management Console - [Console Root\Active Directory Users and Computers [systems-scasi.SCASI.com]\SCASI.com\Users]
File
Action
View
Favorites
Window
Help
Console Root
Active Directory Domains and Trusts
Active Directory Sites and Services [syste
Active Directory Users and Computers [s
Saved Queries
SCASI.com
Builtin
Computers
Domain Controllers
Domain Users
ForeignSecurityPrincipals
Users
Distributed File System
DNS
Default Domain Controllers Policy [systen
Default Domain Policy [systems-scasi.SCA
Internet Information Services (IIS) Mana
IP Security Monitor
IP Security Policies on Active Directory
Performance Logs and Alerts
Security Configuration and Analysis
Security Templates
Folder
Start
Active Directory Main.do...
Management Console...
11:01 AM

Name	Type	Description
ACTUser	User	Account used to launch th...
Administrator	User	Built-in account for admini...
ASPNET	User	Account for running ASP....
Cert Publishers	Security Group ...	Members of this group are...
Debugger Users	Security Group ...	Debugger users can debu...
DHCP Adminis...	Security Group ...	Members who have admini...
DHCP Users	Security Group ...	Members who have view-...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Comp...	Security Group ...	All workstations and serve...
Domain Contr...	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Ad...	Security Group ...	Designated administrators...
Group Policy ...	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServices...	Security Group ...	Group for the Help and Su...
IUSR_SERVER2	User	Built-in account for anony...
IUSR_SYSTE...	User	Built-in account for anony...
IWAM_SERVE...	User	Built-in account for anony...
OWS_277831...	Security Group ...	Microsoft SharePoint role '...
RAS and IAS ...	Security Group ...	Servers in this group can ...
Schema Admins	Security Group ...	Designated administrators...
SQLDebugger	User	This user account is used ...
SUPPORT_38...	User	This is a vendor's account ...

Snap-ins

Snap-Ins are Microsoft Management Console applets that aid in the administration of Active Directory and local computer management. One of the most commonly-used snap-ins is the Active Directory Users and Computers snap-in. MMCs can be customized to include whichever snap-ins an administrator needs.

5.2.3. OpenVMS

For some systems such as OpenVMS reviewing system settings is an easy task since all system settings are in one spot (SYSGEN).

5.3. System Startup and Shutdown Programs

Review of startup, shutdown, logon, and logoff command files can be a significant manual effort. (The author once audited a system that had over 350 startup command files.) A table developed by Mike Kabel at Bank of America can organize the review of these files:

File #	Called By	File Name= Sys:: Disk: [Dir] File.ext	Owner	Protection	W/P	Comments
1	SYSGEN	SYS$SYSTEM: STARTUP.COM SYS$SYSTEM = DUA0: [SYS0.SYSEXE] 000000.DIR SYS0.DIR SYSEXE.DIR	 [SYSTEM] [SYSTEM] [SYSTEM] [SYSTEM] [SYSTEM]	 (RWED,RWED,RE,RE) (RWED,RWED,RWED,RWED) (RWE,RWE,RWE,RWE) (RWE,RWE,RWE,RE) (RWE,RWE,RWE,RE)	 6.4.3	 Unprotected root directory
2	1	SYS$MANAGER: SYSTARTUP_V5.COM SYS$MANAGER = DUA0:[SYS0.SYSMGR] SYSMGR.DIR	 [SYSTEM] [SYSTEM]	 (RWED,RWED,RWED,RE) (RWE,RWE,RWE,RE)		
3	1	SYS$MANAGER:SYLOGICALS.COM	[SYSTEM]	(RWE,RWE,RWE,RE)		
4	2	PROD_APPL1:START_FX.COM PROD_APPL1 = DUS0:[PROD]	[244,244]	(RWED,RWED,RWED,RWED)	6.5.2	Unprotected application startup file executed at startup by SYSTEM
		DUS0:	[133,133]		6.2.1	Production disk
		000000.DIR PROD.DIR	[244,244] [244,244]	(RWE,RWE,RWE,RE) (RWE,RWE,RWE,RE)		
		…				

5.4. Network Settings

- Obtain a copy of the network policies and standards.
- Obtain network diagrams and descriptions of components
- Determine what controls are in place to protect network devices from unauthorized access
- Determine whether the network is compartmentalized to prevent unauthorized access to resources
- Determine whether routing tables, domains, and/or filter tables are used to prevent address spoofing and protect traffic from unauthorized disclosure
- Verify that a firewall is used to protect the servers from external threats.
- Obtain a copy of dial-up policy and standards
- War dial
- Verify that the standards are appropriate and complied with.
- Determine whether remote access is allowed from the internet.
- If remote access is used determine how it is secured and whether security is adequate

IPCONFIG allows a workstation to request, change, or display information about it's IP address.

NETSTAT

NET VIEW

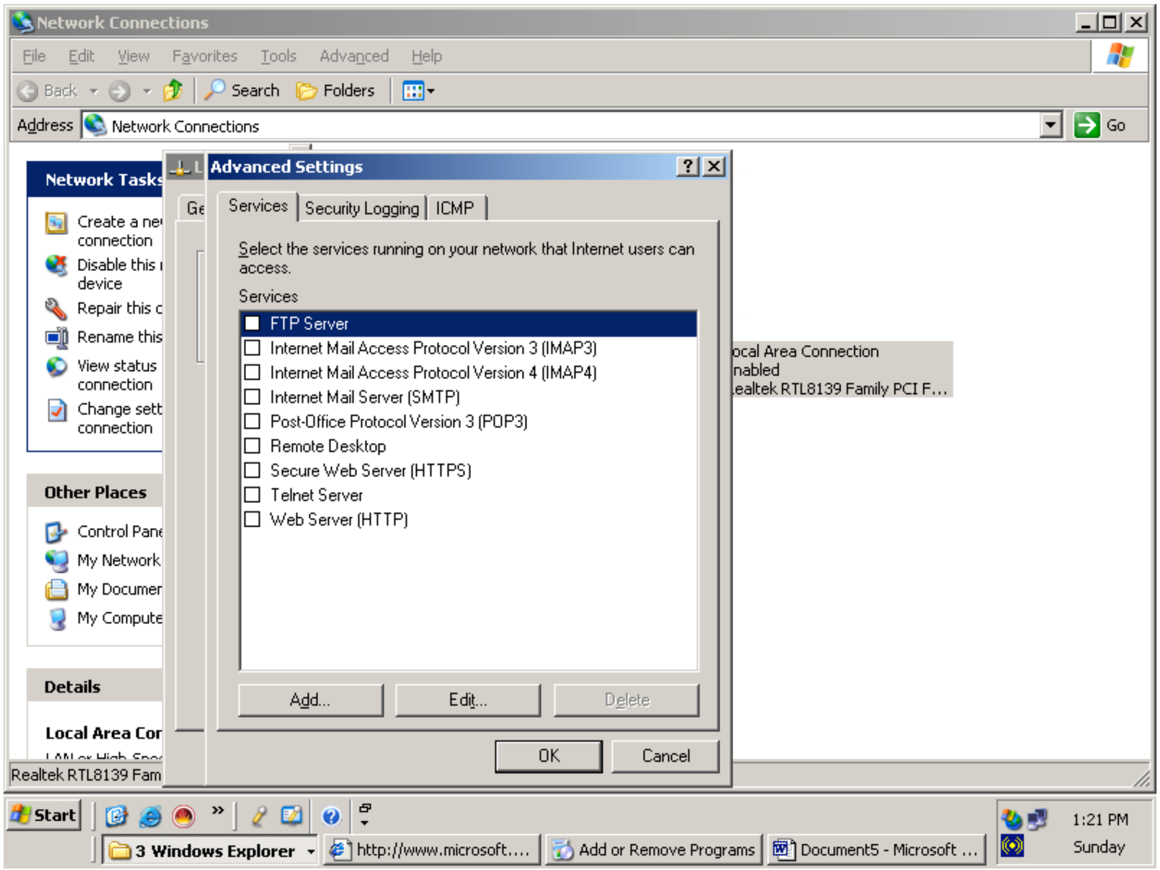
```
C:\Documents and Settings\rodney.kocot.adm>net view
Server Name            Remark

-----------------------------------------------------------------------------
--
\\SERVER2
\\SYSTEMS-SCASI
The command completed successfully.
```

NBTSTAT

NMAP

TRACERT

Windows Server 2003 Fire Wall Advanced Settings:



Advanced Settings

Services | Security Logging | ICMP

Select the services running on your network that Internet users can access.

Services

- □ FTP Server
- □ Internet Mail Access Protocol Version 3 (IMAP3)
- □ Internet Mail Access Protocol Version 4 (IMAP4)
- □ Internet Mail Server (SMTP)
- □ Post-Office Protocol Version 3 (POP3)
- □ Remote Desktop
- □ Secure Web Server (HTTPS)
- □ Telnet Server
- □ Web Server (HTTP)

5.5. Network Startup and Shutdown Programs

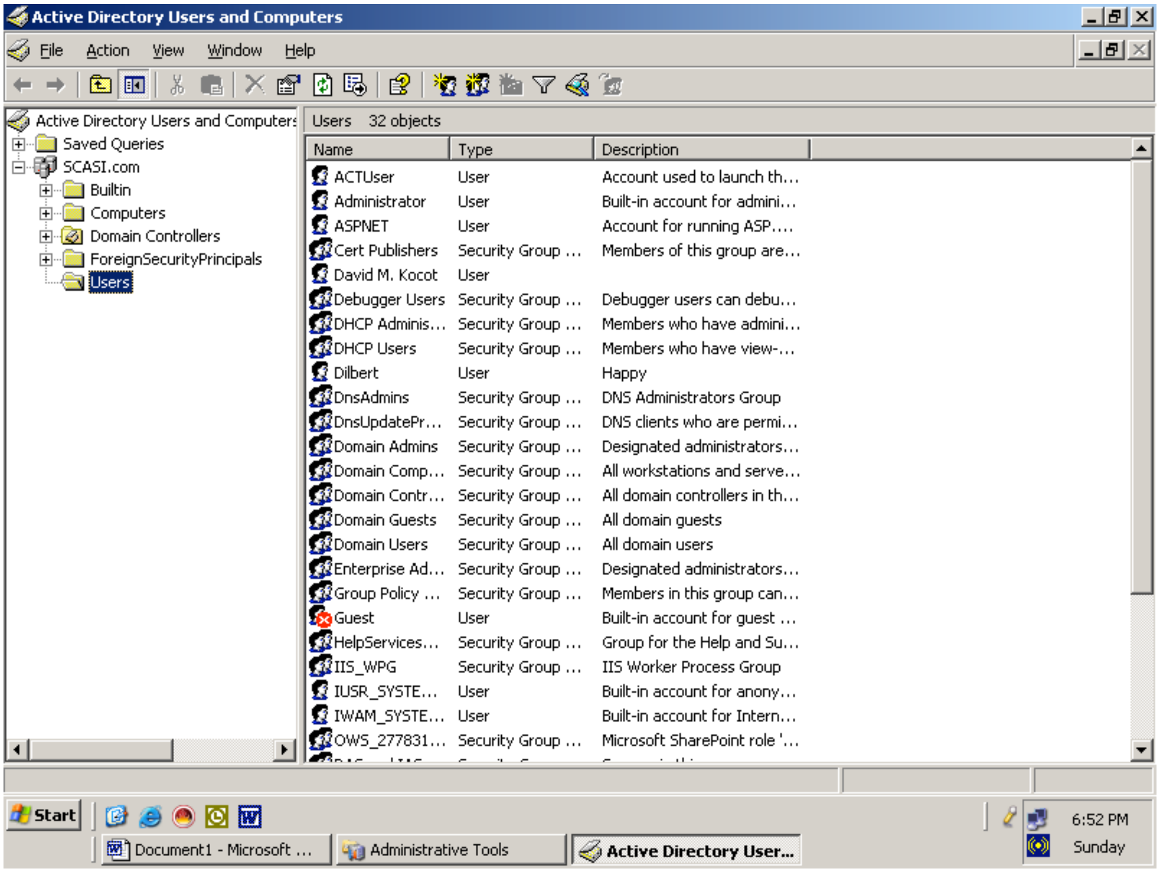
In most operating systems network startup and shutdown is performed with a single utility unless a third party network stack is used, for example:

- Open VMS - ncp
- HP NonStop – SCF

In Windows and Unix environments, however, there are many confusing programs, utilities and configuration files that can start and stop network sessions.

Windows Services
Windows SVCHOST

5.6. User Administration Settings



Users 32 objects

Name	Type	Description
ACTUser	User	Account used to launch th...
Administrator	User	Built-in account for admini...
ASPNET	User	Account for running ASP....
Cert Publishers	Security Group ...	Members of this group are...
David M. Kocot	User	
Debugger Users	Security Group ...	Debugger users can debu...
DHCP Adminis...	Security Group ...	Members who have admini...
DHCP Users	Security Group ...	Members who have view-...
Dilbert	User	Happy
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Comp...	Security Group ...	All workstations and serve...
Domain Contr...	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Ad...	Security Group ...	Designated administrators...
Group Policy ...	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServices...	Security Group ...	Group for the Help and Su...
IIS_WPG	Security Group ...	IIS Worker Process Group
IUSR_SYSTE...	User	Built-in account for anony...
IWAM_SYSTE...	User	Built-in account for Intern...
OWS_277831...	Security Group ...	Microsoft SharePoint role '...

5.6.1. User Authentication

Verify that each userid is owned by an authorized valid employee, contractor or vendor
Determine how users are authenticated.

Determine whether dynamic passwords used.
Verify that passwords are encrypted.
Verify that passwords are periodically changed.
Verify that passwords are at least seven characters and difficult to guess.
Verify that encrypted passwords are protected from unauthorized viewing.
Verify that password change and reset processes are secure

5.6.2. User Access Restrictions

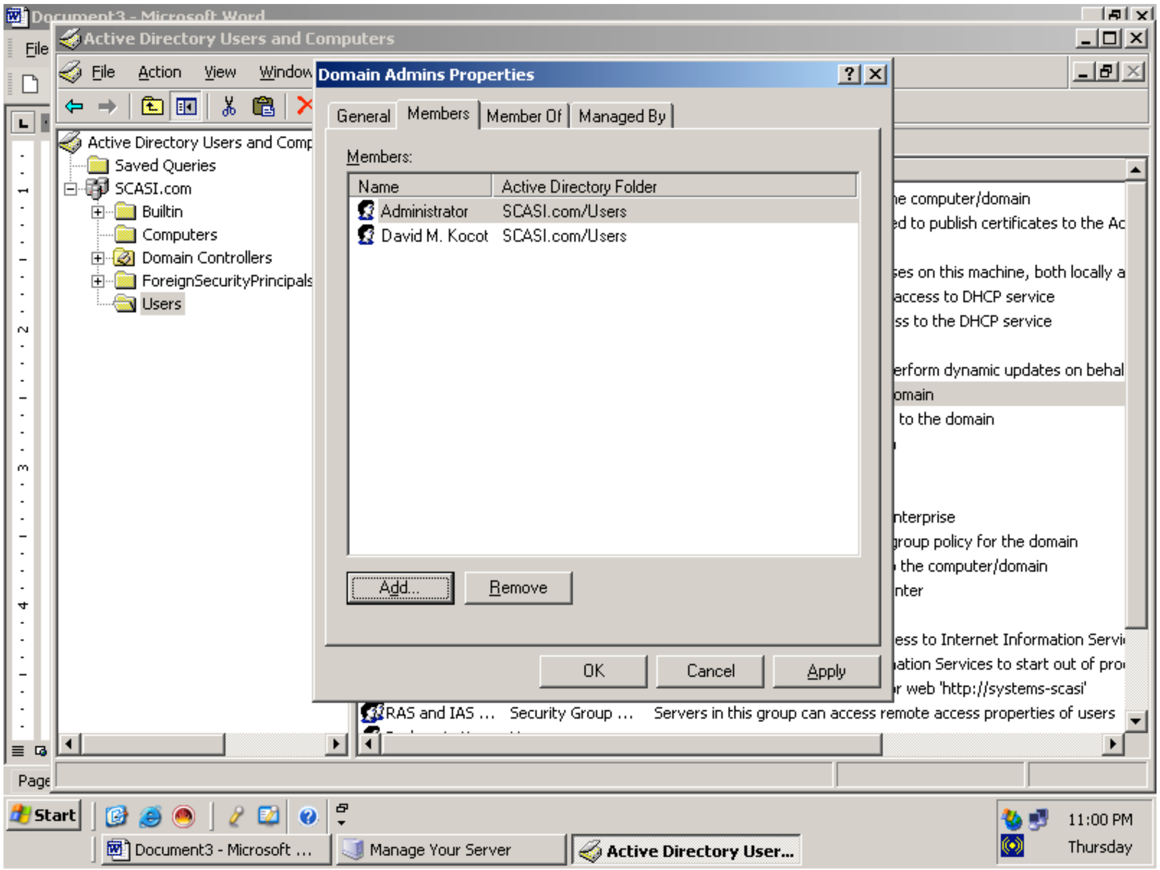
Verify that users are only allowed access from authorized sources.
Verify that application users are restricted to the applications they are authorized to use.
Verify that users are only allowed access to the programs, utilities, menus, and functions that they are authorized to access.

VMS Userid:

```
Username: CAPTIVEUSR                       Owner:
Account:                                   UIC:    [345,346] ([345,346])
CLI:      DCL                              Tables: DCLTABLES
Default:  [USER]
LGICMD:
Login Flags:  Captive Disnewmail Dismail Genpwd
Primary days:   Mon Tue Wed Thu Fri
Secondary days:                     Sat Sun
Primary   000000000011111111112222  Secondary 000000000011111111112222
Day Hours 012345678901234567890123  Day Hours 012345678901234567890123
Network:  -----  No access  ------            -----  No access  ------
Batch:    -----  No access  ------            -----  No access  ------
Local:    ##### Full access ######            -----  No access  ------
Dialup:   -----  No access  ------            -----  No access  ------
Remote:   ##### Full access ######            -----  No access  ------
Expiration:            (none)    Pwdminimum:  6   Login Fails:     0
Pwdlifetime:         85 00:00    Pwdchange:  17-JAN-1989 13:41
Last Login: 16-MAR-1989 14:33 (interactive),     (none) (non-interactive)

Maxjobs:         0  Fillm:        20  Bytlm:         4096
Maxacctjobs:     0  Shrfillm:      0  Pbytlm:           0
Maxdetach:       0  BIOlm:         6  JTquota:       1024
Prclm:           2  DIOlm:         6  WSdef:          150
Prio:            4  ASTlm:        10  WSquo:          200
Queprio:         4  TQElm:        10  WSextent:       500
CPU:        (none)  Enqlm:        10  Pgflquo:      10000
Authorized Privileges:
  TMPMBX NETMBX
Default Privileges:
  TMPMBX NETMBX
```

5.7. User Groups

In Windows to add someone to a group, go to the users folder, right-click on the group, and go to Properties. Click Add and select the user to add to the group.



Name	Active Directory Folder
Administrator	SCASI.com/Users
David M. Kocot	SCASI.com/Users

RAS and IAS ... Security Group ... Servers in this group can access remote access properties of users

Groups are containers which hold one or more users or computers. Large domains, with their size and complexity, would be impossible to manage without groups. Instead of having to apply permissions or policies to hundreds or thousands of users who work in the sales department (for instance), these permissions or policies can simply be applied to a group which contains all of the sales department employees. User and group administration is generally handled with the Users and Computers MMC snap-in

```
C:\Documents and Settings\rodney.kocot.adm>net group

Group Accounts for \\SYSTEMS-SCASI

-------------------------------------------------------------------------------
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Group Policy Creator Owners
*Schema Admins
The command completed successfully.
```

```
C:\Documents and Settings\rodney.kocot.adm>net localgroup

Aliases for \\SYSTEMS-SCASI

-------------------------------------------------------------------------------
*Account Operators
*Administrators
*Backup Operators
*Cert Publishers
*Debugger Users
*DHCP Administrators
*DHCP Users
*DnsAdmins
*Guests
*HelpServicesGroup
*IIS_WPG
*Incoming Forest Trust Builders
*Network Configuration Operators
*OWS_2778318560_admin
*Performance Log Users
*Performance Monitor Users
*Pre-Windows 2000 Compatible Access
*Print Operators
*RAS and IAS Servers
*Remote Desktop Users
*Replicator
*Server Operators
*TelnetClients
*Terminal Server License Servers
*Users
*VS Developers
*Windows Authorization Access Group
The command completed successfully.
```

5.8. User Login and Logoff Scripts

Users Sharing Same Default SubVolume

Default Volume	Default Sub Volume	Group	User	Last Log On Date	Default Security
$AUDIT	TODD	IS	USER21	26JUL06, 13:29	UUUU
$AUDIT	TODD	IS	USER32	14AUG06, 15:22	UUUU
$BATCH1	CGI	IMP	USER04	* NONE *	UUUU
$BATCH1	CGI	IMP	USER12	* NONE *	UUUU
$BATCH1	COMM	COMM	USER06	* NONE *	UUUU
$BATCH1	COMM	COMM	USER11	* NONE *	UUUU
$BATCH1	COMM	COMM	USER28	12MAR04, 15:12	UUUU
$BATCH1	COMM	COMM	USER29	27MAY06, 15:59	UUUU
$BATCH1	COMM	COMM	USER30	16AUG06, 13:01	NUNU

Security for Specified File

Volume	SubVolume	File	OwnerGID	OwnerUID	OwnerG	OwnerU	R	W	E	P
$AUDIT	TODD	TACLCSTM	255	175	SUPER	JOHN	A	A	A	A

Security for Specified File

Volume	SubVolume	File	OwnerGID	OwnerUID	OwnerG	OwnerU	R	W	E	P
$BATCH1	COMM	TACLCSTM	55	45	UNAVAIL	UNAVAIL	U	U	U	U

5.9. Device Security Settings

Every device has recommended and appropriate configuration options.

```
PAS-FW# sho run
: Saved
:
PIX Version 6.3(4)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password xcNbIe46RlNc/WAf encrypted
passwd zcJbke66ZlAc/XBd encrypted
hostname PAS-FW
domain-name sysconsec.com
clock timezone Pacific -8
fixup protocol dns maximum-length 512
fixup protocol ftp 21
no fixup protocol h323 h225 1720
no fixup protocol h323 ras 1718-1719
fixup protocol http 80
no fixup protocol rsh 514
```

5.10. Object Security Settings

- Determine how resources are protected
- Identify all sensitive and critical resources – an inventory of critical and sensitive files and directories should be maintained by IT
- Obtain an electronic copy of all objects on the system showing the protection of each object.
- Verify that sensitive resources are adequately protected
- Verify that no critical resources are unprotected
- Determine the total number of objects, the number of unprotected objects and the percentage of unprotected objects.

5.10.1. Windows

NTFS Security
NTFS is an acronym for “NT File System”, which has been available for the Windows NT series since NT4 and is more secure file system than FAT (File Allocation Table), which was the file system for the Windows 9X series. The NTFS file system allows users to establish security settings for files and folders on a computer. These are low-level properties and, while very similar to permissions (discussed later), file security specifies who has access to files and directories.

Encrypting File System

DFS – Distributed File System

5.10.1.1. Shares

BAT File to List Share Protections

```
net use z: \\SERVER01\DATABASE
net use z:
cacls z: >> C:\shareacls.txt
net use z: /delete
net use z: \\SERVER01\APPLICATION
net use z:
cacls z: >> C:\shareacls.txt
net use z: /delete
net use z: \\SERVER02\APPSETUP
net use z:
cacls z: >> C:\shareacls.txt
net use z: /delete
net use z: \\SERVER03\APPUSER
net use z:
```

Output From BAT File to List Share Protections

```
Local name        Z:
Remote name       \\SERVER01\APPLICATION
Resource type     Disk
Status            OK
# Opens           0
# Connections     1
The command completed successfully.

Z:\ Everyone:(OI)(CI)F

Local name        Z:
Remote name       \\SERVER01\DATABASE
Resource type     Disk
Status            OK
# Opens           0
# Connections     1
The command completed successfully.

Z:\ NT AUTHORITY\SYSTEM:(OI)(CI)F
    BUILTIN\Administrators:(OI)(CI)F
    <Account Domain not found>(OI)(CI)C
    SCASI\NETADM-G:(OI)(CI)F
    SCASI\DBADMIN-G:(OI)(CI)C
```

5.11. Privileged Program Settings

- Obtain a list of authorized services, privileged programs and drivers.
- Review the list of authorized services, privileged programs and drivers for appropriateness.
- Generate a list of running services, privileged programs and drivers from each system in the domain.
- Verify that only authorized and appropriate services, privileged programs and drivers are running on the systems.

Privileged programs can include and are not limited to the following:

5.11.1. HP Non Stop

- Licensed programs
- ProgID programs

5.11.2. Open VMS

- Installed images with privileges

5.11.3. OS400

- Programs that adopt authority

5.11.4. Unix

- SetUID and SetGID programs

5.11.5. Windows

- Windows components that magically run with unrestricted access to anything on the system
- Services that run as SYSTEM or other administrator userids
- SVCHost initiated programs
- Other programs using RunAs and a privileged userid

GenControl can be used to remote control workstations by any administrator.

The Microsoft Windows XP menu option <Start><Administrative Tools><Services> shows all running, paused, and stopped services. This utility can also be executed from the command line with the following command:

```
%SystemRoot%\system32\services.msc /s
```

Some versions of windows have a program named StartupList.exe which can show all programs started when the system was booted.

The SC command line program is used for communicating with the NT Service Controller and services and can:

- generate a list of all services,
- start and stop services, and
- change the properties of services.

Sample output from the “sc query state= all” command:

```
sc query state= all Listing


SERVICE_NAME: Alerter
DISPLAY_NAME: Alerter
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
                                (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 1077   (0x435)
        SERVICE_EXIT_CODE  : 0      (0x0)
        CHECKPOINT         : 0x0
```

TaskList can also be used to identify running tasks:

```
C:\Documents and Settings\Rodney>tasklist /SVC /FO CSV

"Image Name","PID","Services"
"System Idle Process","0","N/A"
"System","4","N/A"
"smss.exe","836","N/A"
"csrss.exe","884","N/A"
"winlogon.exe","908","N/A"
"services.exe","952","Eventlog,PlugPlay"
"lsass.exe","964","Netlogon,PolicyAgent,ProtectedStorage,SamSs"
"svchost.exe","1124","DcomLaunch"
"svchost.exe","1208","RpcSs"
"svchost.exe","1352","Dnscache"
"svchost.exe","1400","LmHosts,RemoteRegistry,SSDPSRV,WebClient"
"ccSetMgr.exe","1592","ccSetMgr"
"ccEvtMgr.exe","1620","ccEvtMgr"
```

5.12. Dial-up Settings

Dialup is using a modem to connect two PCs and or networks together. Dialup can open up your intranet to the internet if a user dials in to their ISP while connected to your intranet.

- Obtain policies and procedures for dial-up access
- Verify policies and procedures are appropriate
- Obtain an inventory of authorized modems
- Obtain a list of all phone numbers
- War Dial all phone numbers to identify all modems
- Compare the list of modems found with the list of authorized modems
- Verify all modems are configured according to policy and procedures
- Review the security of systems accessible through the modems, at a minimum:
  - Verify every userid has a password

- o Verify vendor supplied passwords have been changed
- o Verify logging is appropriate and monitored

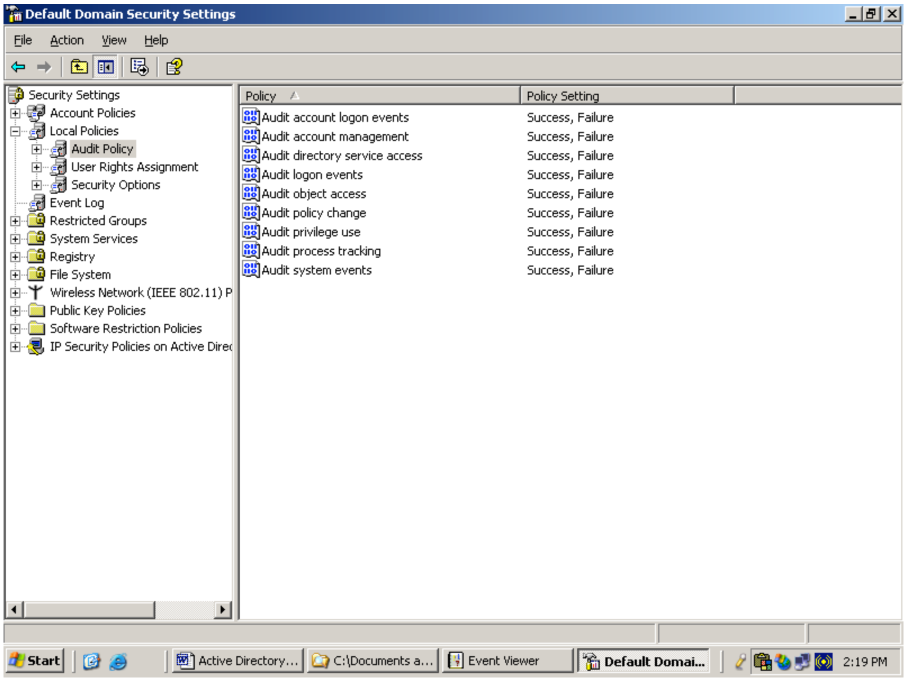
5.13. Logging and Monitoring

- Obtain procedures for monitoring and violation follow-up
- Determine whether monitoring and violation procedures are adequate
- Verify system logging settings are appropriate
- Determine whether monitoring and violation procedures are appropriately and adequately implemented

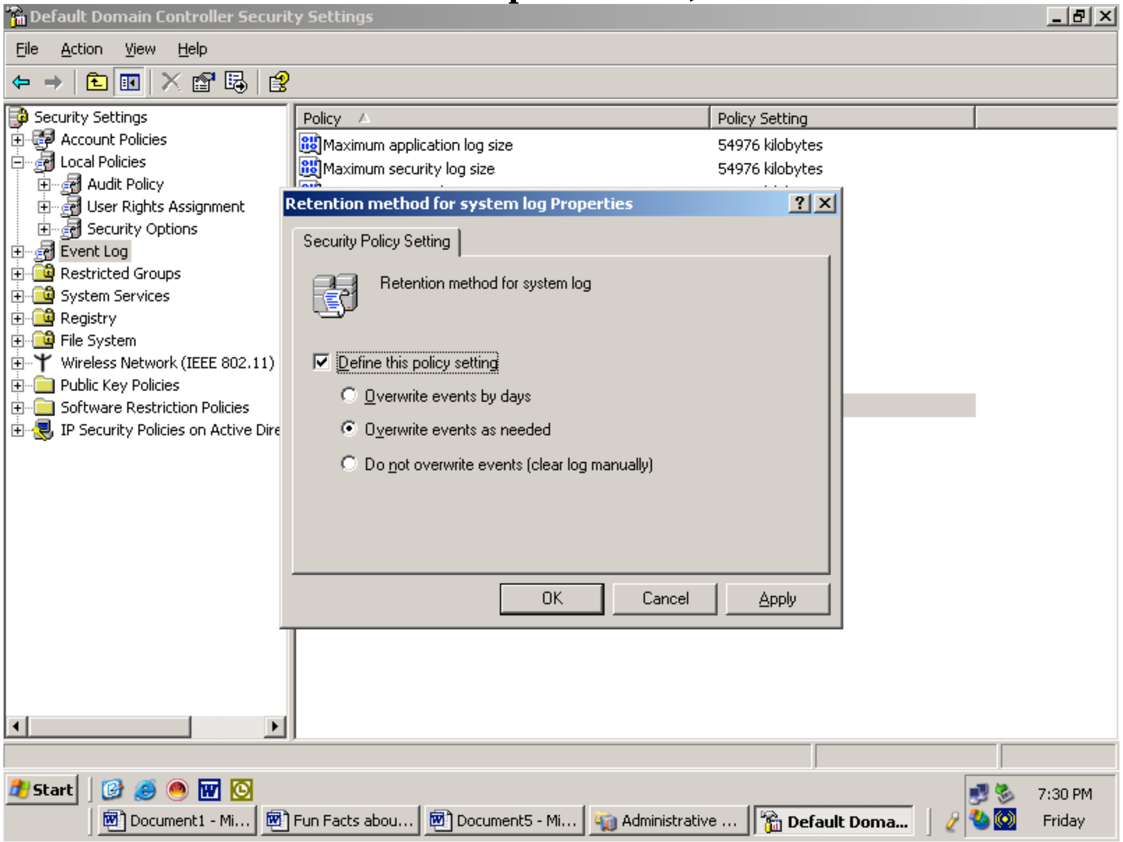
5.13.1. Windows

If logs from all systems are not consolidated and reviewed from a central location then attacks will not be identified. Even PC logs must be reviewed since unauthorized activities from a PC against resources on a network are often only logged on the PC being used to perpetrate the unauthorized activity.

Audit Policy



Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure



Policy	Policy Setting
Maximum application log size	54976 kilobytes
Maximum security log size	54976 kilobytes

Retention method for system log Properties

Security Policy Setting

Retention method for system log

☑ Define this policy setting

○ Overwrite events by days

● Overwrite events as needed

○ Do not overwrite events (clear log manually)

The eventquery script can be used to dump the event logs from local and remote systems:

```
C:\> cscript c:\windows\system32\eventquery.vbs
```

The event viewer can also be used to review logs.

5.13.2. Open VMS

- Show Accounting
- Show Audit
- Analyze /Audit
- Run Accounting

5.14. Backup and Recovery

- Obtain backup and COP plans and procedures for each component in the IT environment
- Determine whether backup and COP plans and procedures for each component in the client service environment are adequate and appropriate
- Determine whether backup and COP plans and procedures for each component in the IT environment are implemented
- Select a sample of programs and data from each component in the IT environment and determine whether the programs and data are backed up
- Obtain documentation describing backup procedures
- Verify that all critical and necessary data and software are included in backups
- Obtain a listing of all storage/backup media
- Inventory the media
- Review equipment and media disposal procedures

5.15. IT and User Security Awareness

- Obtain change management procedures for each component in the IT environment
- Determine whether change management procedures are adequate, appropriate, and apply to all components in the IT environment

5.16. Change Management

- Obtain change management procedures for each component in the IT environment
- Determine whether change management procedures are adequate, appropriate, and apply to all components in the IT environment

5.17. Application Security

- Identify all application activities, menus, and functions
- Determine whether access to application activities, menus, and functions is appropriate
- Determine whether automated edit checking of input is performed
- Determine whether all transactions can be tracked to the individual that initiated the transaction
- Determine whether sequencing and totals are used to identify lost or duplicate transactions
- Determine whether all applications are periodically reconciled
- Determine whether management reports are generated which identify fraud and any processing irregularities
- Determine whether management reports are periodically reviewed

The following areas should be reviewed in an application security review:

1. Physical Security
2. Application Settings
3. Application Startup and Shutdown Programs
4. Application Network Settings
5. Application Network Startup and Shutdown Programs
6. Application User Administration Settings
7. Application User Groups
8. Application User Login and Logoff Scripts

9. Application Device Security Settings
10. Application Object Security Settings
11. Application Privileged Program Settings
12. Application Dial-up Settings
13. Application Logging and Monitoring
14. Application Backup and Recovery
15. Application IT and User Security Awareness
16. Application Change Management
17. Application Security
18. Application Add-on Security Products

5.18. Add On Security Products

- Determine whether any add on security products are used to enhance security in the IT environment
- Identify the features of any add on security products
- Determine which features of the add on security products are used and whether the features are appropriate
- Determine whether the features of the add on security product are implemented properly
- Determine whether the features of the add on security product allow other security features to be circumvented

6. Summary

The following information and statistics should be reported in every operating system security evaluation: The information can be used to identify and compare similar systems. The statistics provide a baseline and common evaluation for most operating systems.

The following background Information is used to identify the system and describe the environment it operates in:

1. name of system,
2. location of system,
3. operating system name,
4. operating system version and patch level,
5. vendor of system,
6. name(s) of application(s)
7. vendor(s) of application(s)
8. type and model of hardware,
9. number of userids
10. number of objects/files
11. number of privileged programs
12. number of FTE performing system management functions
13. number of FTE performing security functions

Risk Statistics are used to measure system risk. Generally, the lower the number/percentage the more secure a system is. For example, if 100% of the passwords are the word password, all the objects are unprotected, privileged programs allow anyone on the system to do anything, and all the security related system and network settings are set to the most vulnerable settings then the system is probably not secure. Conversely, if all the passwords are difficult to guess, all the objects on the system are protected to only allow authorized users appropriate and authorized access levels, privileged programs are controlled with file security and internal checks to prevent unauthorized use, and all the system and network settings are set appropriately for the system and applications then the system is probably secure. The following risk statistics provide a basic indicator of the security of a system.

1. Number and percentage of easily guessable, blank and vendor supplied passwords. The percentage of easily guessable passwords can be generated by most password cracking utilities. Vendor supplied passwords should be easy to identify in any system just by trying the passwords in cooperation with the Security and System Administrators.
2. Number and percentage of unprotected files/objects. A percentage of unprotected files can be generated for any system. A simple program in every system can show the total number of files and the number of unprotected files. Listings can be analyzed with ACL or MS Access to generate this statistic.
3. Number and percentage of unprotected privileged programs. Once the list of unprotected objects is generated it can be compared to the list of privileged programs to identify unprotected privileged programs.
4. Number of unauthorized and/or inappropriate privileged programs. This count is more difficult than the rest of the counts and statistics because most vendors do not document their privileged programs. A lot of research is often needed to identify the purpose of undocumented privileged programs.
5. Number of unnecessary open ports.
6. Number of inappropriate system settings