Active Directory & Windows Audit and Security

Presented by:

Rodney Kocot
Systems Control and Security Incorporated
Rodneykocot@gmail.com
818-370-0442

Presented to the:

Information Systems Security Association
Inland Empire Chapter

Windows Active Directory & Vista

This updated full day session will cover audit and security of Windows and Active Directory. The related network and systems components will also be covered. For example, integration with DHCP, name resolution with DNS, and the Active Directory network are included. The Active Directory structure and schema will be described. Users and groups, the group policy, active directory management, security, replication and backup are discussed. Active directory and Windows add-ins will be demonstrated and audit and security automation tools and scripting will be demonstrated. A partial outline for the session follows:

Introduction to Windows
Physical Security
Windows Security Overview
Patch Management
Virus Protection
Introduction to Active Directory
Active Directory Configuration
Active Directory Administration
Active Directory Policies
Active Directory Security
Group Policies
User and Group Administration
NTFS Permissions
Shared Folder Administration
Logging and Monitoring
Network Security
Ports and Services
Remote Access
Disaster Recovery
Audit Program
Tools Summary

PREREQUISITE
None. Familiarity with Windows and/or network operating systems is helpful.

SPEAKER: Rodney Kocot, Systems Control and Security Incorporated

Rodney Kocot is a technical IS Audit Consultant for Systems Control and Security Incorporated. Rodney provides technical audit training and consulting services for corporations worldwide. He has been an IT Auditor since 1981 with responsibilities that included technical audits of operating systems, networks, and audit software development. Positions at fortune 50 companies have included EDP Auditor, Senior EDP Auditor, AVP and EDP Auditor, VP and IT Auditor, VP and IT Audit Manager, SVP and Senior Audit Manager.

Rodney has often presented at the ISACA CACS and International conferences. He has presented numerous seminars and dinner meetings all over the world for the last 23 years. 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 working with and programming PCs since 1982 beginning with CPM and BASIC. He currently programs mostly with Visual Basic, but also knows C++ and other languages. He has been working with Windows since its inception.

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.

SYSTEMS CONTROL AND SECURITY, INCORPORATED (SCASI) was established in 2003 and provides system security consulting. The Sys Secure ™ service provides a low cost very effective review of system security for many operating systems. For example, we perform over 170 tests of the security on OS400 systems for $1500.00. The output of our Sys Secure ™ service is a report between 60 and 190 pages describing the security on the system. The report contains the following sections:

- Cover Page - shows the organization, system name and data date.
- Copyright, Disclaimer, Read Me, and Reading Notes - explains why people should not be fired.
- Table of Contents
- Executive Summary - describes the report and its contents in non-technical terms.
- Executive Level Issues - explains the issues and their risk in non-technical terms.
- Comparisons with Other Systems – shows how the system compares with other organizations.
- System Information and Issues Summary – System statistics and configuration values.
- Detailed Issues in the areas of system configuration, user administration, resource protections, privileged programs, network configuration and other areas depending on the operating system. Each issue includes the following sections:
    - Issue/Information Title
    - Description
    - Finding
    - Detail Information
    - Risk
    - Recommendation

Caution: If you do NOT want to know what the issues are, then do NOT use the Sys Secure ™ service.

Windows Active Directory & Vista

Table of Contents

1 Introduction to Windows 10
1.1 Why is Security Important? 10
1.2 Windows History 10
1.3 Which Windows are you Looking Through? 11
1.4 Active Directory 11
1.5 Security Standards 11
1.6 Introduction to Windows Audit Steps 12
1.6.1 Background 12
1.6.2 Documentation 12
1.6.3 Listings 12
1.6.4 Risk Analysis 13
1.6.5 High Level Audit Program 14
2 Physical Security 15
2.1 Key Katcher 15
2.2 Unix Boot Software 15
2.3 Password Cracking Software 15
2.4 Physical Security Audit Steps 16
3 Active Directory and the Global Catalog 17
3.1 Active Directory Details 17
3.2 The Schema 18
3.2.1 Registering the Schema Manager MMC DLL: 18
3.2.2 Active Directory Schema Snap-in: 18
3.3 Active Directory Structure 19
3.4 Active Directory Dump Utilities - LDIFDE 19
3.5 The Global Catalog (GC) 19
3.6 Light Weight Directory Access Protocol (LDAP) 19
3.7 Enumeration of Active Directory Information 19
3.7.1 Script to Dump Active Directory Information 20
3.7.2 Script to Dump Active Directory Information Output 20
3.8 Active Directory and the Global Catalog Audit Procedures 21
4 Domains, Forests, and Trees 22
4.1 Trust Relationships 22
4.2 Active Directory Domains and Trusts 23
4.3 Domains Forrests and Trees Audit Program 23
5 Security Settings and Group Policy Objects 24
5.1 Microsoft Management Console (MMC) 24
5.2 Snap-ins 25
5.3 Manage Your Server Wizard: 25
5.4 Default Domain Controller Security Settings 26
5.5 Password Security Settings 27
5.6 Default Domain Controller Security Settings: 28
5.7 Event Log Configuration 29
5.8 More Default Security Settings 30
5.9 Group Policy Objects (GPOs) 30
5.9.1 GPResult 31

5.9.2 GPInventory 33
5.9.3 GPLogView 33
5.10 Security Settings and GPOs Audit Program 34
6 User Profiles, Groups, and Organizational Units 35
6.1 User Profiles 35
6.1.1 RunAS.exe 35
6.1.2 Active Directory Users and Computers: 36
6.1.3 New Object – User - Identifying Information: 37
6.1.4 New Object - User - Password 38
6.1.5 Adding Users to Groups 39
6.1.6 Administrators 40
6.1.7 Security Accounts Manager (SAM) 40
6.2 Groups 41
6.3 Global Groups 41
6.3.1 NET GROUP 41
6.4 Local Groups 42
6.4.1 NET LOCALGROUP 42
6.5 User Administration Audit Procedures 43
7 Resource Protections 44
7.1 NTFS Security 44
7.2 Encrypting File System 44
7.3 DFS – Distributed File System 44
7.4 File Security Properties 45
7.5 Permission options 46
7.6 File Server Management 47
7.7 Share Protections 47
7.7.1 Shared Folder Properties: 49
7.8 Directory and File Protections 49
7.9 BAT File to List Share Protections 51
7.10 Output From BAT File to List Share Protections 51
7.11 SubInACL.exe 52
7.12 Openfiles 52
7.13 Resource Protections Audit Program 54
8 Services and Privileged Programs 55
8.1 Services and Privileged Programs Overview 55
8.2 Services and Privileged Programs Commands 55
8.2.1 Services.msc 55
8.2.2 SC 55
8.3 Tasklist 56
8.3.1 Schtasks /Query 57
8.4 Services and Privileged Programs Audit Program 58
9 Network Access 59
9.1 Network Configuration 59
9.1.1 Network Address Translation 59
9.1.2 Routers and Firewalls 59
9.1.3 Dynamic Host Configuration Protocol (DHCP) 61
9.1.4 GetMAC.exe 61

9.1.5 Hostname.exe 61
9.1.6 NSLookUp.exe 62
9.2 PathPing.exe 62
9.3 Network Commands 62
9.3.1 NET /? 62
9.3.2 NET SHARE 63
9.3.3 NET USE /H 63
9.3.4 NET USER 63
9.3.5 NET VIEW 64
9.3.6 Ipconfig 64
9.3.7 Netstat 64
9.3.8 Nbtstat 66
9.3.9 Ping 66
9.3.10 Tracert 67
9.3.11 Netsh 67
9.4 NMAP 67
9.5 Network Load Balancing Manager 69
9.6 Routing and Remote Access 70
9.7 Sniffers 71
9.7.1 Sniffer Data Display 71
9.7.2 Sniffer Packet Dump: 72
9.8 FTP 73
9.9 Dialup 73
9.10 Wireless 73
9.11 Internet Information Services Manager 74
9.12 Network Security Audit Program 74
10 Logging and Monitoring 75
10.1 Reviewing Logs 75
10.1.1 EventQuery.vbs 75
10.1.2 Log Parser 75
10.1.3 Event Viewer – Security Log 76
10.1.4 Security Log Settings 77
10.2 Baseline Security Analyzer 78
10.2.1 Baseline Security Analyzer Help 78
10.2.2 Baseline Security Analyzer Output 79
10.3 File Integrity Monitoring 83
10.4 Open Source Host Based Intrusion Detection System (OSSEC) 83
10.5 Free PC Audits 83
10.6 Logging and Monitoring Audit Procedures 84
11 Backup and Contingency Planning 85
11.1 Backup and Contingency Planning Audit Program 85
12 Patch Management 86
12.1 Patch Management Systems 86
12.2 Don’t Forget Application Patches! 87
12.3 Patcher Beware 87
12.4 Patch Management Audit Program 87
13 Miscellaneous Tools 88

13.1 Active Directory Scripting....88
13.2 VBScript to List Users and Groups....89
13.2.1 Scriptomatic....90
13.2.2 WMI Code Creator....91
13.3 Active Directory API....91
14 Add On Security Products....92
14.1 DumpSec....92
14.2 Sys-Secure....92
14.3 Encryption....92
14.3.1 GnuPG....92
14.3.2 FileZilla....92
14.3.3 TrueCrypt....92
14.4 Add On Security Products Audit Program....93
15 System Management....94
15.1 Chkdsk....94
15.2 Defrag....96
15.3 Virtual Machines....96
16 Application Security....98
16.1 Web Application Security....98
16.2 Application Database Security....98
16.3 Application Configuration Files....98
17 Other Sources of Information/Bibliography....99
18 Windows Information Request List....101
18.1 RunAllNetCommands.bat....104

Table of Illustrations

Introduction to Windows 10
Physical Security..15
Key Katcher 15
Active Directory and the Global Catalog..17
Registering the Schema Manager MMC DLL..18
Active Directory Schema Snap-in 18
LDIFDE Sample Output 19
Script to Dump Active Directory Information..20
Script to Dump Active Directory Information Output..20
Domains, Forests, and Trees..22
Active Directory Domains and Trusts 23
Security Settings and Group Policy Objects..24
Microsoft Management Console (MMC) 24
Manage Your Server Wizard 25
Password Security Settings..27
Default Domain Controller Security Settings..28
Event Log Configuration 29
Default Domain Controller Security Settings..30
User Profiles, Groups, and Organizational Units..35
Active Directory Users and Computers 36
New Object – User - Identifying Information..37
New Object - User - Password..38
Net Group..41
Net Localgroup..42
Resource Protections..44
Distributed File System..44
File Security Properties..45
File Server Management..47
Shared Folder Properties..49
Directory ACL 50
Share ACL 50
BAT File to List Share Protections..51
Output From BAT File to List Share Protections 51
Openfiles..52
Services and Privileged Programs 55
sc query state= all 55
Tasklist..56
Network Access 59
Router Logs..60
Windows Server 2003 Fire Wall Advanced Settings 61
Net Help 62
Net Share..63
Net User 63
Net View 64

`Netstat -help` 64
`Netstat Active Connections` 65
`Nbtstat protocol statistics and TCP/IP connections` 66
`Ping` 66
Tracert 67
Nmap 67
Network Load Balancing Manager 69
Routig and Remote Access 70
Sniffer Data Display 71
Sniffer Packet Dump 72
Internet Information Services (IIS) Manager 74
Logging and Monitoring 75
Event Viewer - Security Log 76
Audit Policy 77
Security Options 77
Baseline Security Analyzer Help 78
Baseline Security Analyzer Output 79
Backup and Contingency Planning 85
Patch Management 86
Miscellaneous Tools 88
ListAllUsersAndGroups.vbs Source 89
ListAllUsersAndGroups.vbs Execution 90
Add On Security Products 92
System Management 94
Application Security 98
Other Sources of Information 99

1 Introduction to Windows

Windows is the most widely used operating system in the world. Because of its popularity Windows is the most popular target for hackers, viruses, and other malicious acts.

With Windows, Microsoft has traditionally traded security for user friendliness. However, there have been initiatives by Microsoft in recent years to improve the security of Windows.

Obviously, Microsoft is the final authority for Microsoft products: www.Microsoft.com The Microsoft on-line knowledge base is extensive and has examples for almost anything you want to do with Windows (good or bad.)

1.1 Why is Security Important?

Computers and technology in general have become an integral part of our lives. Every day, computers manage the movement of hundreds of billions of dollars through bank wire systems. Our cities' electrical supplies are managed by computers. Manufacturing plants make production and purchasing schedules by computer. And every day, hundreds of millions of dollars' worth of purchases are made on Amazon, EBay, or any of literally hundreds of thousands of other e-commerce internet sites.

Computers have made the world smaller, faster, more efficient, and less expensive. Unfortunately, the world has been made smaller, faster, and more efficient for criminals, too. The last ten years have seen an astounding rise in computer crime. Hackers, Viruses, Worms, identity thieves, and disgruntled employees now have the power to ruin the day for literally hundreds of millions of people with a click of the mouse.

These threats have led to the rise of Information Security as one of the most important fields in IT today.

1.2 Windows History

For a very complete history of windows go to:
http://www.computerhope.com/history/windows.htm

1.3 Which Windows are you Looking Through?

Windows actually refers to two different series of operating systems. The first is the Windows 9X series (Windows 95, Windows 98, and Windows Millennium Edition (ME)), which was built on a perceived need to maintain backwards-compatibility with 16 bit processors and hardware. The second series is known as "NT" (New Technology), and had its debut with NT4.0 in 1996. Designed for business use and utilizing all the potential of the new (at the time) 32-bit processors, NT is far more stable than the Windows 9X series. Windows 200X (Also known as "Windows NT5.0"…) and Windows XP are the son and grandson, respectively, of NT4. The NT series which is predominantly Windows 2000, is far and away the most prevalent operating system in use in medium and large business and governments organizations.   Windows Vista is making a forced debut.

1.4 Active Directory

The NT series of Windows operating systems have both client and server versions (except for Windows XP - Windows Server 2003 was released a year or so after Windows XP). Windows 2000 Server introduced a full-featured Active Directory network management system into the Windows world. Active Directory is a system for managing the user account and computer objects in a given network, referred to as a Domain. Windows 2008 continues to use active directory.

Active Directory manages an organization called a Domain. Each domain is used to control a group of Windows computers and users, and can range in size from one host to hundreds of thousands of hosts. Every domain is managed by one or more Domain Controllers – servers whose primary responsibility is keeping track of domain objects (primarily user and computer accounts). Domains can be broken down and objects categorized for more efficient organization through the use of Organizational Units (OUs). Also, multiple domains can be grouped together in domain trees and domain forests.

1.5 Security Standards

- ✓ **http://www.cerias.purdue.edu The Center for Education and Research in Information Assurance and Security**
- ✓ **http://www.cert.org Part of the Software Engineering Institute (SEI) at Carnegie Mellon University funded by DARPA.**
- ✓ **http://www.cisecurity.org/ The Center for Internet Security**
- ✓ **http://csrc.ncsl.nist.gov National Institute of Standards and Technology, Computer Security Division, Computer Security Resource Center**
- ✓ **http://www.first.org Forum of Incident Response and Security Teams**
- ✓ **http://www.fraud.org National Consumers League Fraud Center**
- ✓ **http://itgi.org IT Governance Institute**
- ✓ **http://www.nist.gov/ National Institute of Standards and Technology**
- ✓ **http://www.pcisecuritystandards.com/ Payment Card Industry Security Standards Council**

- ✓ **http://www.SANS.org** **SysAdmin, Audit, Network Security Institute**
- ✓ **http://www.us-cert.gov/** **United States Computer Emergency Readiness Team**

Many web sites provide great information and services. A few are not trustworthy.

1.6 Introduction to Windows Audit Steps

1.6.1 Background

- Obtain organization charts and phone lists of all individuals involved in the LAN, servers, and applications. Include the following groups for each component of the environment:
    - ➢ systems
    - ➢ operations
    - ➢ programming
    - ➢ users
- Verify that system administrators, security administrators, and other appropriate individuals are involved in the appropriate user and professional associations and groups
- Obtain inventory listings for all equipment used in the LAN environment
- Obtain vendor documentation for all equipment used in the LAN environment
- Obtain copies of, or access to, all policies, standards and procedures
- Obtain risk assessments for the LAN and related environments
- Obtain audit reports for the LAN and related environments.

1.6.2 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

1.6.3 Listings

Obtain all the listings described in this handout. Obtain ALL the listings before reporting any issues.

1.6.4 Risk Analysis

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

1.6.5 High Level Audit Program

- Review Physical Security
- Obtain a complete inventory of all system, network, database and application components
- Active Directory and the Global Catalog
  - ✓ Identify all programs, tools, utilities and add-ins used to generate listings and reports from Active Directory and the Global Catalog.
  - ✓ Identify all parameters and settings related to security.
- Identify Domains, Forests, and Trees
  - ✓ Determine trust relationships between all domains.
  - ✓ Determine appropriate scope.
- Identify Operating System Security Settings and Group Policy Objects (GPOs)
  - ✓ Identify all programs, tools, utilities and add-ins used to generate listings and reports from the operating system and GPOs.
  - ✓ Determine appropriate values for operating system security settings and GPOs.
- User Profiles, Groups, and Organizational Units
  - ✓ Identify all types of users and groups (local, remote, domain, application, database, …)
  - ✓ Identify all programs, tools, utilities and add-ins used to generate listings and reports from user profiles, groups, organizational units, etc.
- Resource Protections
  - ✓ Device protections
  - ✓ Share protections
  - ✓ Directory and file protections
  - ✓ Utility protections
  - ✓ Registry protections
- Services/Privileged Programs
- Network Access
- Logging and Monitoring
- Backup and Contingency Planning
- Patch Management

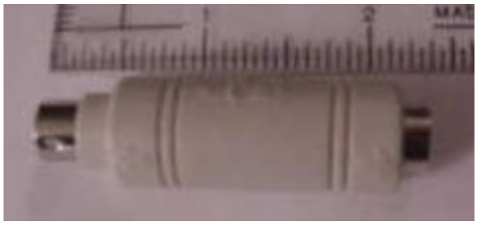
Note that for any audit step, hack, exploit, etc. described in this handout, a Google, Yahoo, or whatever search can provide numerous ways to hack, exploit, use, … the information provided.

Check out Auditnet.org and other sites for sample audit programs.

2 Physical Security

Any server or PC with critical information or confidential data must be physically secured. There are numerous ways to compromise a PC or server if you have physical access. No matter how many services and ports you disable, firewalls and intrusion detection systems you install, or permissions you deny, if your critical servers are not physically secure, your network is not secure. If an attacker has physical access to a server (or any other electronic device, for that matter) and knows what he or she is doing, he or she can take total control of that server in a matter of minutes. Even if he or she doesn't know what he or she is doing, he or she can still engage in numerous other destructive and dastardly dirty deeds, like installing a keystroke logger that will capture every single keystroke entered on the keyboard. Also, a variety of "live" CDs exist which can be used to boot a machine to a Linux distribution that includes a number of cracker tools (examples include Knoppix, Phlak, and Whoppix).

2.1 Key Katcher



2.2 Unix Boot Software

2.3 Password Cracking Software

John the Ripper password cracker - http://www.openwall.com/john/

Advanced Windows Password Recovery by ElcomSoft -
http://www.openwall.com/passwords/nt.shtml
Win32, shareware, 30 day free trial, $60 personal / $120 business license (purchase)
Advanced Windows Password Recovery (AWPR) is a program to recover most types of Windows passwords:
Windows 95/98/ME/NT/2000 logon password
Windows 95/98/ME/NT/2000/XP auto logon password
Windows XP stored user passwords
screensaver, RAS and dial-up passwords
passwords to VPN connections

passwords and access rights to shared resources
AWPR is also able to recover LSA Secrets, and decrypt product ID and CD key for Windows and Microsoft Office installations, and perform brute-force and dictionary attacks on Windows 9x PWL files.

2.4 Physical Security Audit Steps

- Review physical security policies, standards and procedures and determine whether they are appropriate. .
- Physically inspect the buildings and areas which house any components of the LAN environment
- Test all data center and server room doors and locks
- Inspect network closets and server rooms for unauthorized equipment.
- Determine whether power conditioning and UPS equipment is adequate and appropriate for each component of the LAN environment
- Determine whether fire prevention and suppression programs and equipment are adequate
- Inspect fire escapes and areas in and around the server room for safety issues.
- Inventory assets… Inventory Assets, …Did I say inventory assets? Things walk away. If you don't know something exists then you cannot secure it.
- Determine whether physical security is adequate

3 Active Directory and the Global Catalog

The NT series of Windows operating systems have both client and server versions (except for Windows XP - Windows Server 2003 was released a year or so after Windows XP). Windows 2000 Server introduced a full-featured Active Directory network management system into the Windows world. Active Directory is a system for managing the user account and computer objects in a given network, referred to as a Domain. Windows 2003 through 2008 continue to use Active Directory.

Active Directory manages an organization called a Domain. Each domain is used to control a group of Windows computers and users, and can range in size from one host to hundreds of thousands of hosts. Every domain is managed by one or more Domain Controllers – servers whose primary responsibility is keeping track of domain objects (primarily user and computer accounts). Domains can be broken down and objects categorized for more efficient organization through the use of Organizational Units (OUs). Also, multiple domains can be grouped together in domain tress and domain forests.

3.1 Active Directory Details

Active directory is a database that allows you to store and locate things based on their attributes and/or name. The database consists of objects with attributes. You can modify the schema and query the database

A copy of the Active Directory database is stored on a domain's Domain Controllers. By default, the Active Directory database file is

C:\WINNT\NTDS\NTDS.dit

On Windows 2003 Server, it is C:\WINDOWS\NTDS\NTDS.dir

In addition, the C:\WINNT(or WINDOWS)\NTDS and C:\WINNT(or WINDOWS)\Sysvol directories contain a great deal of information needed by Active Directory, such as log files, Logon/Logoff and Startup/Shutdown scripts, group policies, etc. These directories can be renamed from these defaults, however, when Active Directory is installed on the Domain Controller.

The database can be configured to replicate with other servers for performance and reliability. The database is hierarchical and usually distributed.

3.2 The Schema

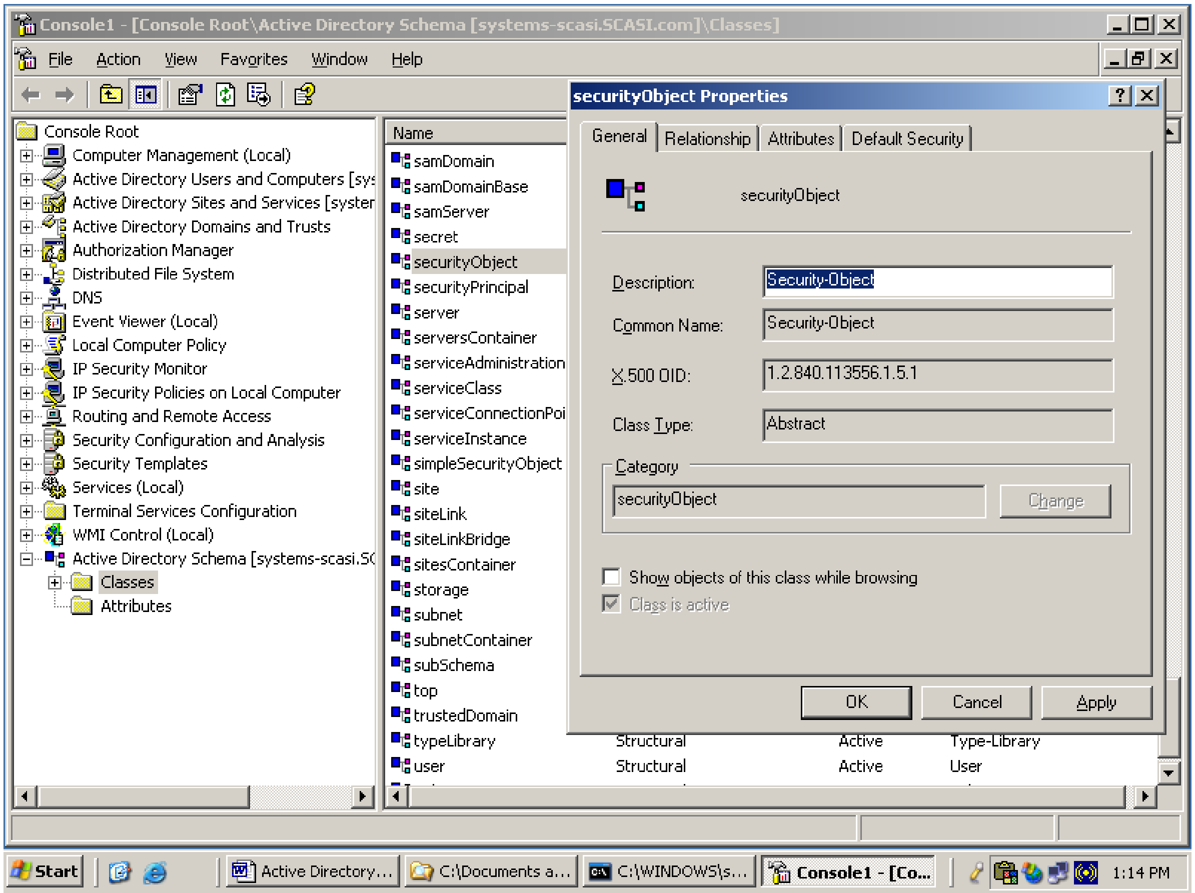
The schema is a database that contains templates that define the structure of all objects and their attributes. There are three ways to manage the schema:

1. The Schema Manager MMC
2. LDIF files, or
3. programmatically using ADSI

3.2.1 Registering the Schema Manager MMC DLL:

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\rodney.kocot.adm>regsvr32.exe schmmgmt.dll

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

3.2.2 Active Directory Schema Snap-in:



Console1 - [Console Root\Active Directory Schema [systems-scasi.SCASI.com]\Classes]

securityObject Properties

General | Relationship | Attributes | Default Security

securityObject

Description: Security-Object

Common Name: Security-Object

X.500 OID: 1.2.840.113556.1.5.1

Class Type: Abstract

Category: securityObject

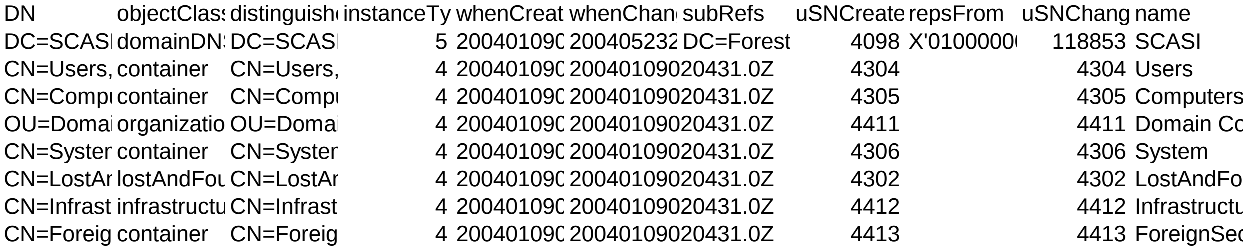
☐ Show objects of this class while browsing

☑ Class is active

3.3 Active Directory Structure

Forest – A group of trees.
Tree – A group of Domains
Domain – A network managed by Active Directory
Organizational Unit (OU) – A container used to organize Active Directory objects.

3.4 Active Directory Dump Utilities - LDIFDE



DN	objectClass	distinguish	instanceTy	whenCreat	whenChang	subRefs	uSNCreate	repsFrom	uSNChang	name
DC=SCASI	domainDN	DC=SCASI	5	200401090	200405232	DC=Forest	4098	X'0100000	118853	SCASI
CN=Users,	container	CN=Users,	4	200401090	20040109020431.0Z		4304		4304	Users
CN=Compu	container	CN=Compu	4	200401090	20040109020431.0Z		4305		4305	Computers
OU=Domai	organizatio	OU=Domai	4	200401090	20040109020431.0Z		4411		4411	Domain Cc
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	ForeignSec

3.5 The Global Catalog (GC)

The Global Catalog (GC) is used to perform forest wide searches. The GC contains a list of all objects in the forest with a subset of attributes.

3.6 Light Weight Directory Access Protocol (LDAP)

A very common directory system protocol that requires the operating system to enforce access control.

3.7 Enumeration of Active Directory Information

Can a non privileged user access Active Directory and enumerate information?

The answer is yes, depending on the configuration of the environment, the Windows version and the information retrieved. The following was done with a non-Administrator userid on a PC connected to the network with a Windows 2003 domain controller.

3.7.1 Script to Dump Active Directory Information

```
On Error Resume Next
'strComputer = "."
strComputer = "Systems-SCASI"
Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")
Set colItems = objWMIService.ExecQuery("Select * from Win32_NTDomain")
For Each objItem in colItems
    Wscript.Echo "Client Site Name: " & objItem.ClientSiteName
    Wscript.Echo "DC Site Name: " & objItem.DcSiteName
    Wscript.Echo "Description: " & objItem.Description
    Wscript.Echo "Dns Forest Name: " & objItem.DnsForestName
    Wscript.Echo "Domain Controller Address: " & objItem.DomainControllerAddress
    Wscript.Echo "Domain Controller Address Type: " & objItem.DomainControllerAddressType
    Wscript.Echo "Domain Controller Name: " & objItem.DomainControllerName
    Wscript.Echo "Domain Guid: " & objItem.DomainGuid
    Wscript.Echo "Domain Name: " & objItem.DomainName
    Wscript.Echo "DS Directory Service Flag: " & objItem.DSDirectoryServiceFlag
    Wscript.Echo "DS DNS Controller Flag: " & objItem.DSDnsControllerFlag
    Wscript.Echo "DS DNS Domain Flag: " & objItem.DSDnsDomainFlag
    Wscript.Echo "DS DNS Forest Flag: " & objItem.DSDnsForestFlag
    Wscript.Echo "DS Global Catalog Flag: " & objItem.DSGlobalCatalogFlag
    Wscript.Echo "DS Kerberos Distribution Center Flag: " &
objItem.DSKerberosDistributionCenterFlag
    Wscript.Echo "DS Primary Domain Controller Flag: " &
objItem.DSPrimaryDomainControllerFlag
    Wscript.Echo "DS Time Service Flag: " & objItem.DSTimeServiceFlag
    Wscript.Echo "DS Writable Flag: " & objItem.DSWritableFlag
    Wscript.Echo "Name: " & objItem.Name
    Wscript.Echo "Primary Owner Contact: " & objItem.PrimaryOwnerContact
    Wscript.Echo
Next
```

3.7.2 Script to Dump Active Directory Information Output

```
C:\Classes\Active Directory>cscript getdomaininfo.vbs
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

Client Site Name: Default-First-Site-Name
DC Site Name: Default-First-Site-Name
Description: SCASI
Dns Forest Name: SCASI.com
Domain Controller Address: \\10.0.0.10
Domain Controller Address Type: 1
Domain Controller Name: \\SYSTEMS-SCASI
Domain Guid: {09E6DBF7-95CC-4250-B1A4-AFFFF220A3E0}
Domain Name: SCASI
DS Directory Service Flag: True
DS DNS Controller Flag: False
DS DNS Domain Flag: False
DS DNS Forest Flag: True
DS Global Catalog Flag: True
DS Kerberos Distribution Center Flag: True
DS Primary Domain Controller Flag: True
DS Time Service Flag: True
DS Writable Flag: True
Name: Domain: SCASI
Primary Owner Contact: Rodney Kocot
```

3.8 Active Directory and the Global Catalog Audit Procedures

Determine whether policies and procedures for use and management of active directory and the global catalog are formalized and implemented.

Determine how Active Directory and the Global Catalog are protected from unauthorized modification.

Determine whether responsibility for management of Active Directory and the Global Catalog have been assigned.

Determine how Active Directory and the Global Catalog are backed up.

Determine whether the Active Directory has been modified and whether the modifications are appropriate.

Determine whether the Active Directory files are properly protected.

4 Domains, Forests, and Trees

4.1 Trust Relationships

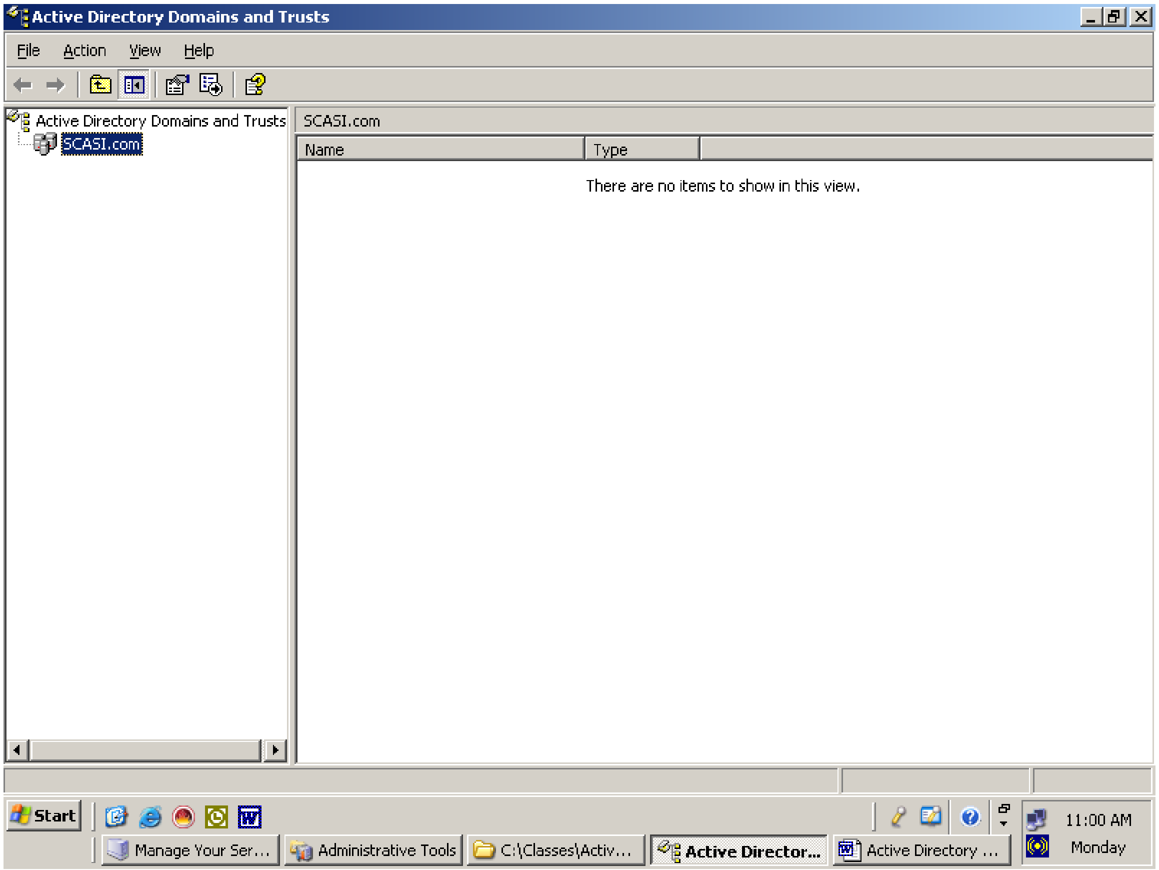
Active Directory domain trusts work differently depending on the version of windows in use. The following sites provide information about domains, forests and trees:

- ✓ http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx
- ✓ http://En.Wikipedia.com/Active_Directory#Trust

The following types of trusts can be defined between domains:

- ✓ Cross-link Trust
- ✓ Explicit Trust
- ✓ Intransitive Trust
- ✓ One Way Trust
- ✓ Shortcut Trust
- ✓ Transitive Trust
- ✓ Two way Trust

4.2 Active Directory Domains and Trusts



There are no items to show in this view.

4.3 Domains Forrests and Trees Audit Program

- Determine whether policies and procedures are formalized and appropriate for trust relationships.
- Obtain listings showing trust relationships
- Obtain a description of each trust relationship.
- Determine whether each trust relationship complies with policies and procedures and is authorized and appropriate.

5 Security Settings and Group Policy Objects

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.

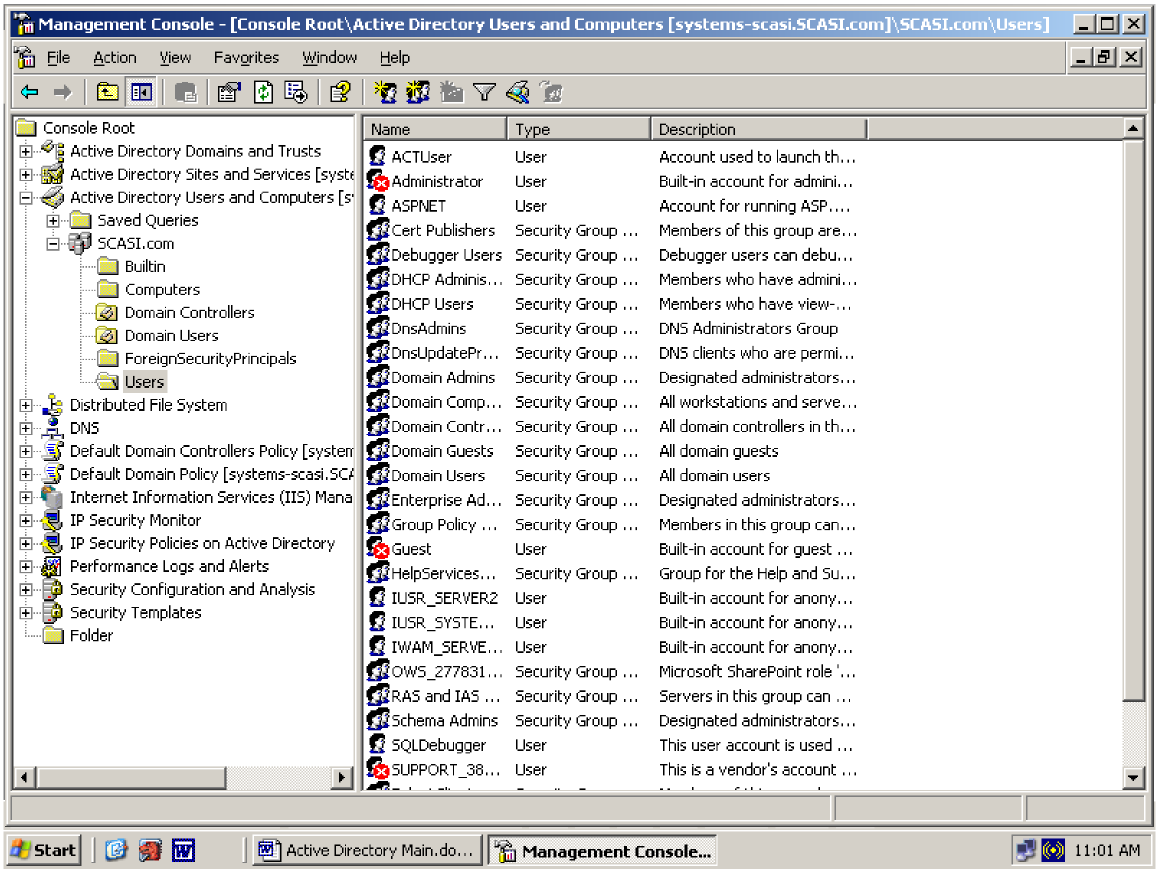
There is even a group policy that allows a user to circumvent all security. (Period.)

5.1 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.

Microsoft Management Console (MMC)


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 [system
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 ...

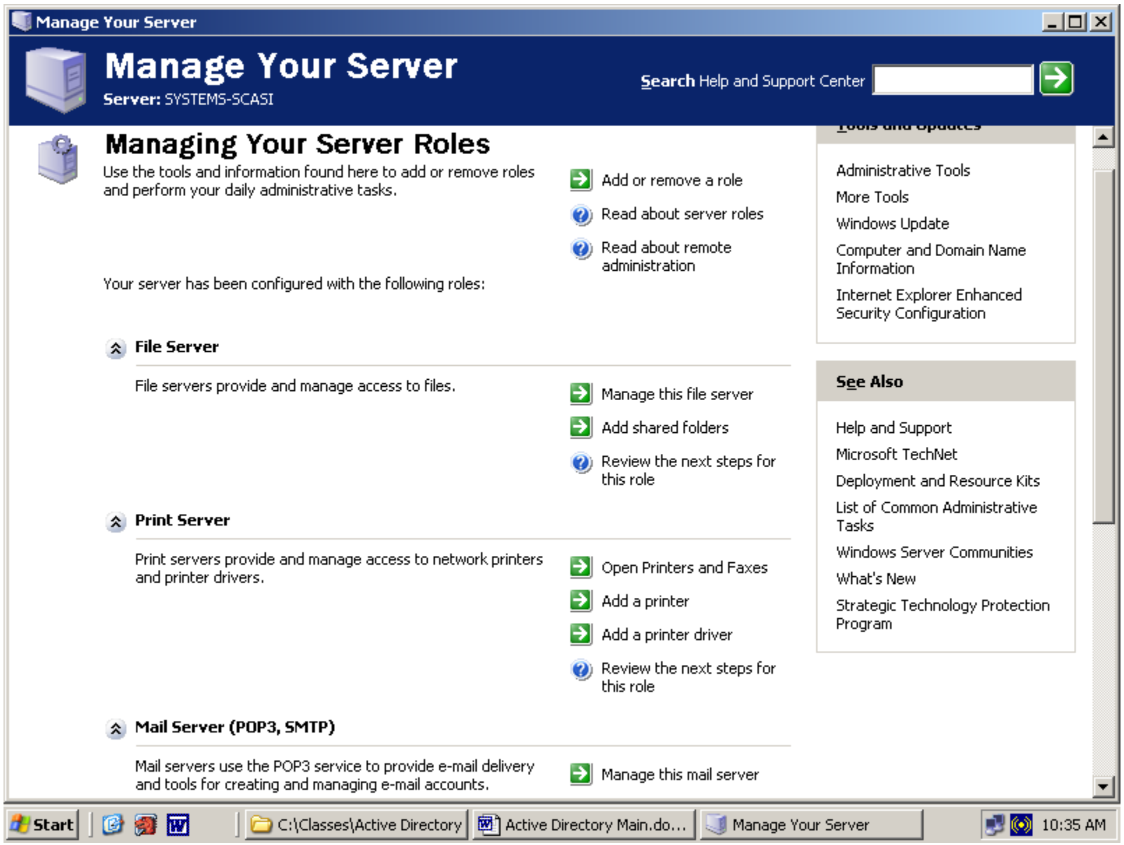
5.2 Snap-ins

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.

5.3 Manage Your Server Wizard:

While not a snap-in the Manage Your Server Wizard new in Windows 2003 is a convenient place to start when managing Windows2003.

Manage Your Server Wizard:



Manage Your Server

Server: SYSTEMS-SCASI

Search Help and Support Center

Managing Your Server Roles

Use the tools and information found here to add or remove roles and perform your daily administrative tasks.

Your server has been configured with the following roles:

File Server

File servers provide and manage access to files.

Print Server

Print servers provide and manage access to network printers and printer drivers.

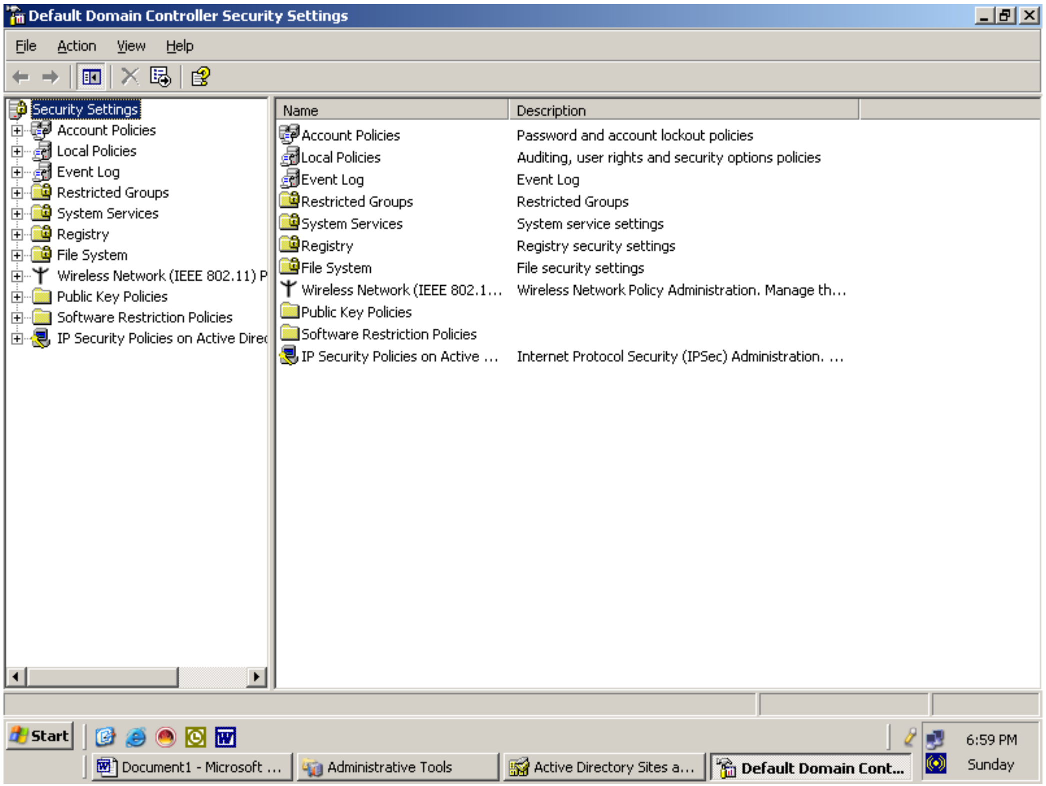
Mail Server (POP3, SMTP)

Mail servers use the POP3 service to provide e-mail delivery and tools for creating and managing e-mail accounts.

Add or remove a role
Read about server roles
Read about remote administration
Manage this file server
Add shared folders
Review the next steps for this role
Open Printers and Faxes
Add a printer
Add a printer driver
Review the next steps for this role
Manage this mail server
Tools and Updates
Administrative Tools
More Tools
Windows Update
Computer and Domain Name Information
Internet Explorer Enhanced Security Configuration
See Also
Help and Support
Microsoft TechNet
Deployment and Resource Kits
List of Common Administrative Tasks
Windows Server Communities
What's New
Strategic Technology Protection Program
Start
C:\Classes\Active Directory
Active Directory Main.do...
Manage Your Server
10:35 AM

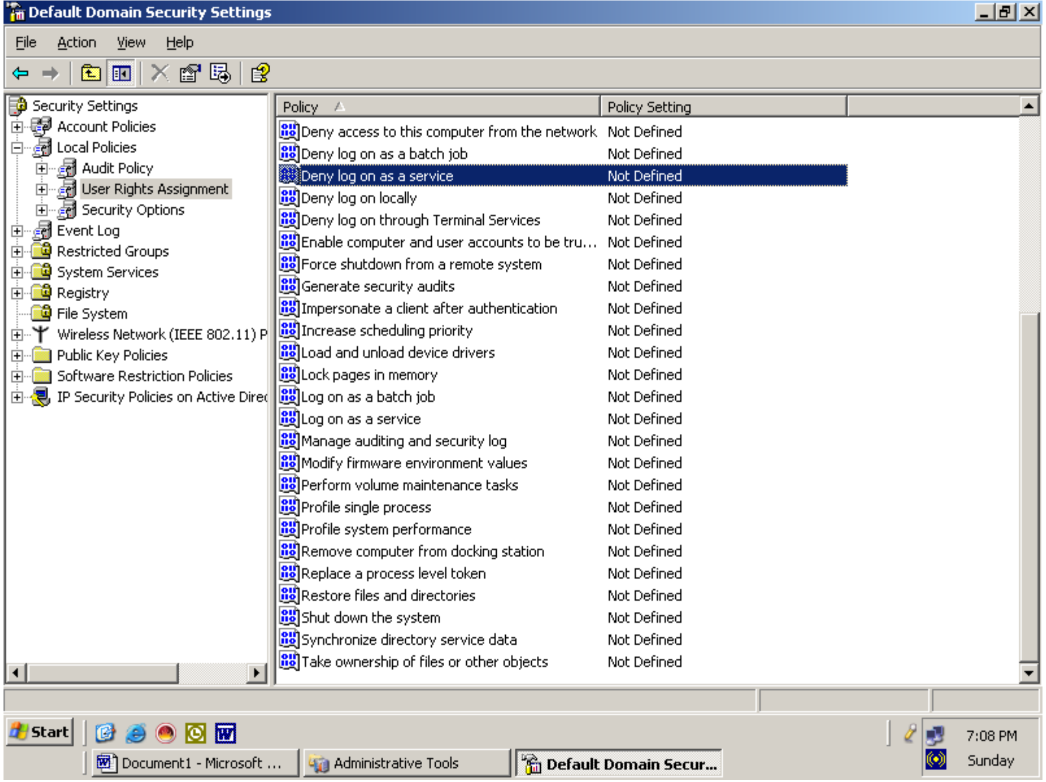
You can find the wizard at <Start><All Programs><Administrative Tools><Manage Your Server>

5.4 Default Domain Controller Security Settings



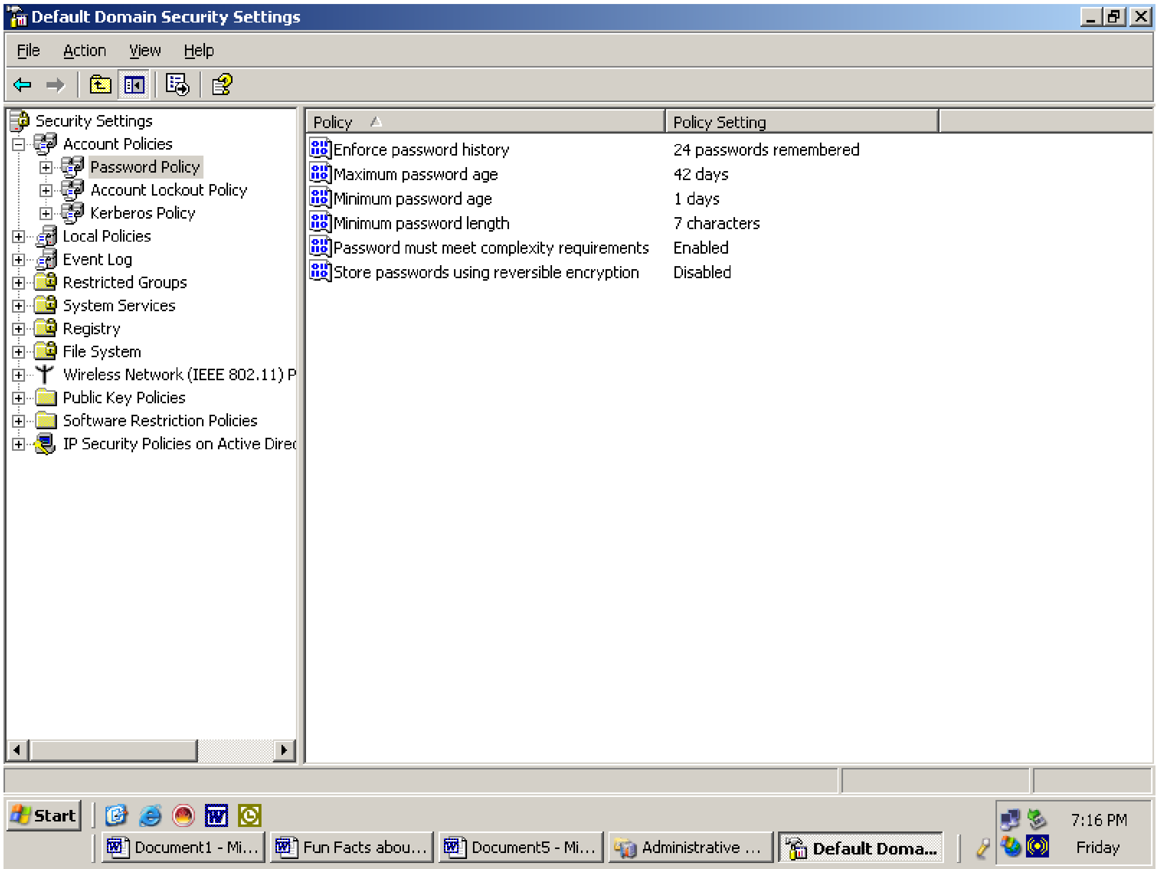
Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options policies
Event Log	Event Log
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File security settings
Wireless Network (IEEE 802.1...	Wireless Network Policy Administration. Manage th...
Public Key Policies	
Software Restriction Policies	
IP Security Policies on Active ...	Internet Protocol Security (IPSec) Administration. ...

Uncle Bill's Default Security Settings:



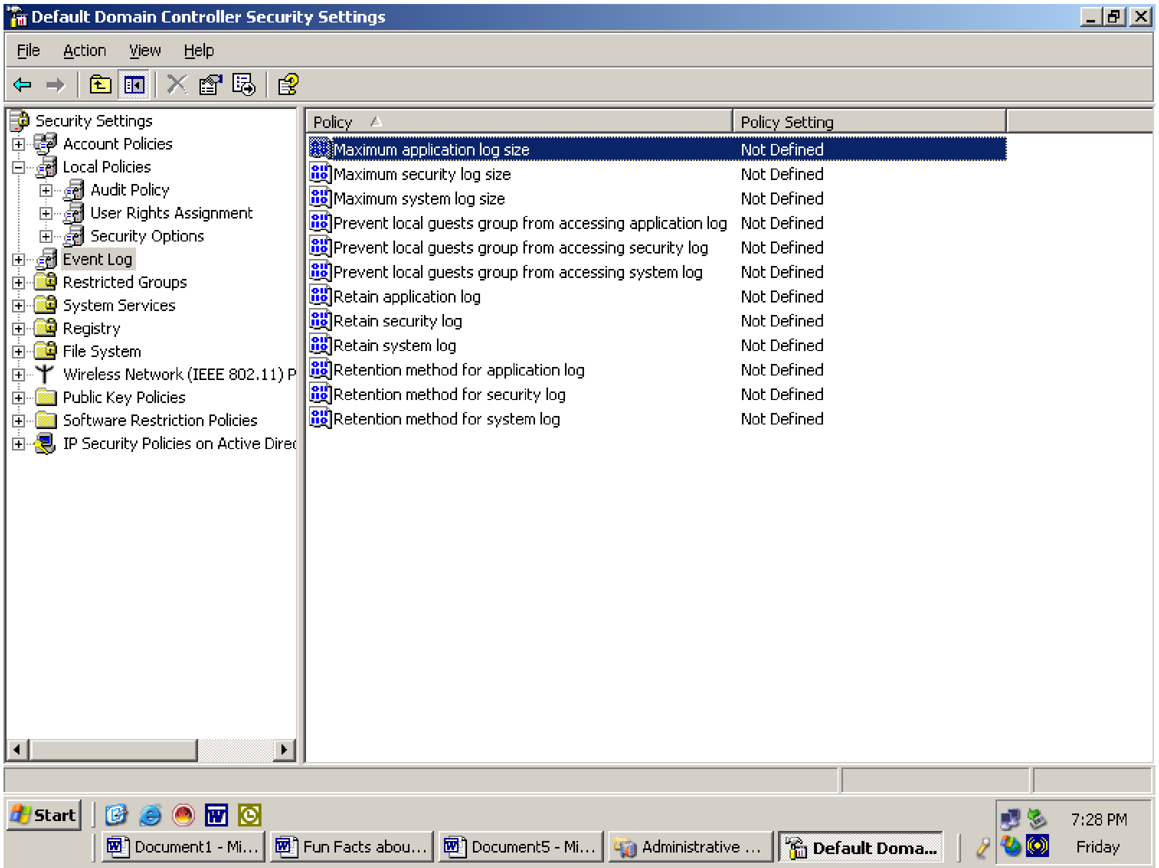
Policy	Policy Setting
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Terminal Services	Not Defined
Enable computer and user accounts to be tru...	Not Defined
Force shutdown from a remote system	Not Defined
Generate security audits	Not Defined
Impersonate a client after authentication	Not Defined
Increase scheduling priority	Not Defined
Load and unload device drivers	Not Defined
Lock pages in memory	Not Defined
Log on as a batch job	Not Defined
Log on as a service	Not Defined
Manage auditing and security log	Not Defined
Modify firmware environment values	Not Defined
Perform volume maintenance tasks	Not Defined
Profile single process	Not Defined
Profile system performance	Not Defined
Remove computer from docking station	Not Defined
Replace a process level token	Not Defined
Restore files and directories	Not Defined
Shut down the system	Not Defined
Synchronize directory service data	Not Defined
Take ownership of files or other objects	Not Defined

5.5 Password Security Settings



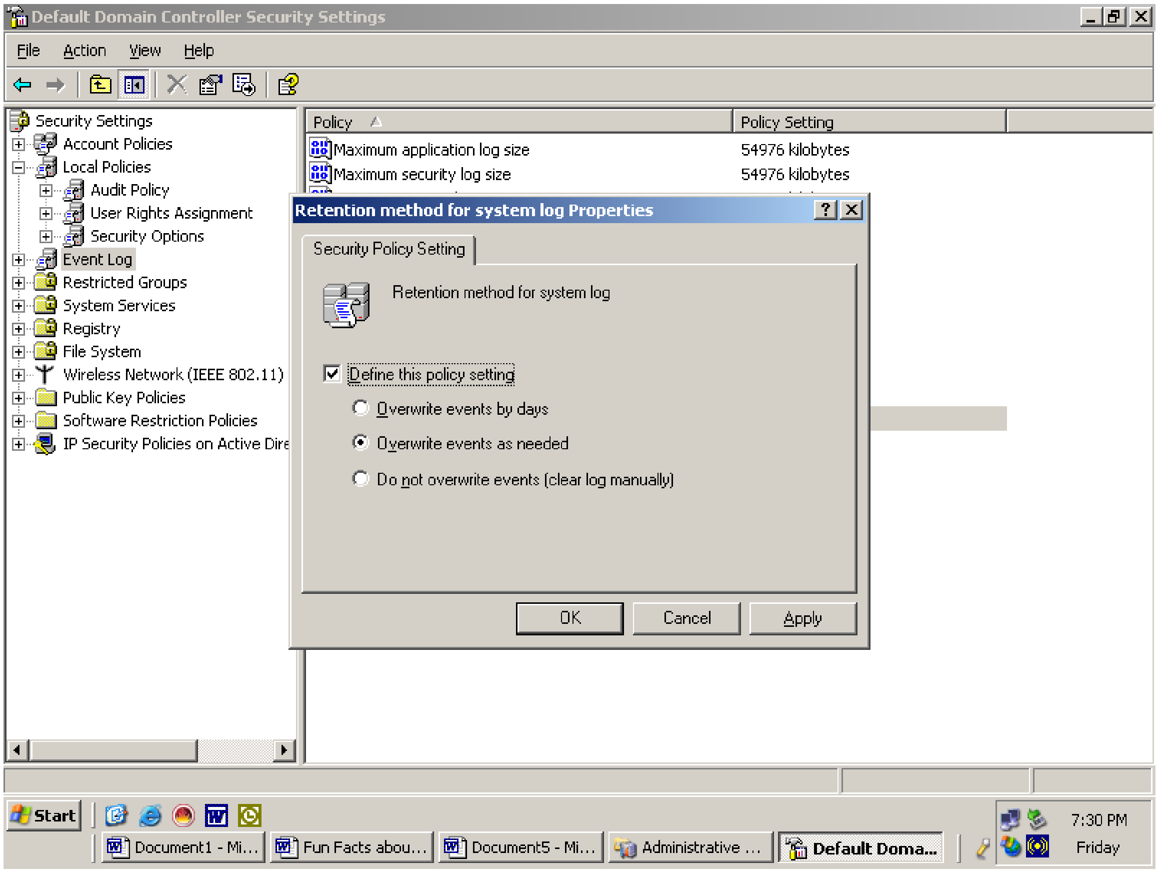
Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

5.6 Default Domain Controller Security Settings:



Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	Not Defined
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	Not Defined
Retention method for system log	Not Defined

5.7 Event Log Configuration



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

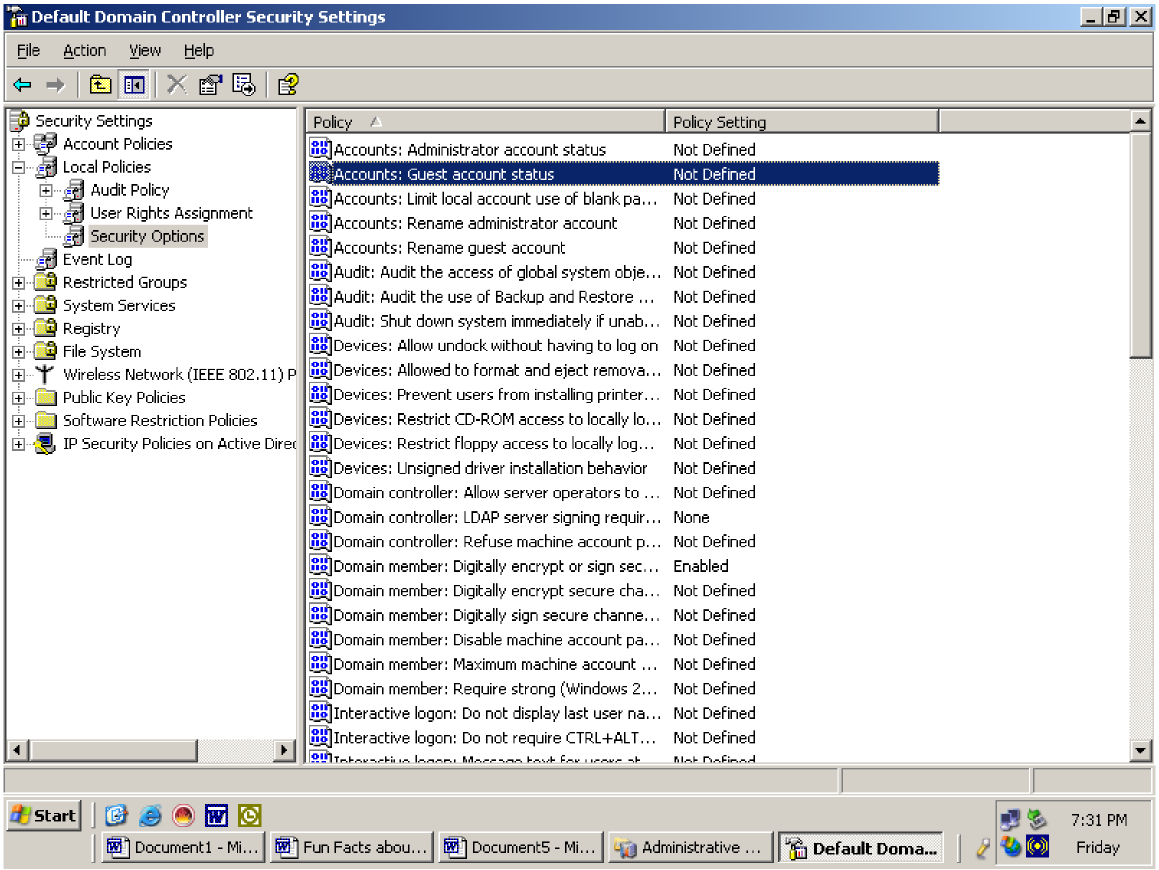
○ Overwrite events by days

● Overwrite events as needed

○ Do not overwrite events (clear log manually)

OK Cancel Apply

5.8 More Default Security Settings



- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Event Log
  - Restricted Groups
  - System Services
  - Registry
  - File System
  - Wireless Network (IEEE 802.11) P
  - Public Key Policies
  - Software Restriction Policies
  - IP Security Policies on Active Direc

Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank pa…	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system obje…	Not Defined
Audit: Audit the use of Backup and Restore …	Not Defined
Audit: Shut down system immediately if unab…	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject remova…	Not Defined
Devices: Prevent users from installing printer…	Not Defined
Devices: Restrict CD-ROM access to locally lo…	Not Defined
Devices: Restrict floppy access to locally log…	Not Defined
Devices: Unsigned driver installation behavior	Not Defined
Domain controller: Allow server operators to …	Not Defined
Domain controller: LDAP server signing requir…	None
Domain controller: Refuse machine account p…	Not Defined
Domain member: Digitally encrypt or sign sec…	Enabled
Domain member: Digitally encrypt secure cha…	Not Defined
Domain member: Digitally sign secure channe…	Not Defined
Domain member: Disable machine account pa…	Not Defined
Domain member: Maximum machine account …	Not Defined
Domain member: Require strong (Windows 2…	Not Defined
Interactive logon: Do not display last user na…	Not Defined
Interactive logon: Do not require CTRL+ALT…	Not Defined
Interactive logon: Message text for users at…	Not Defined

5.9 Group Policy Objects (GPOs)

The Group Policy Object (GPO) Editor (gpedit.msc) or the Group Policy Management Console are used to manage Group Policy Objects. (SecPol.msc is also available and is a subset of gpedit.msc.)
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.

Ensure that GPOs are periodically backed-up using Backupallgpos.wsf or another utility. A batch job that runs monthly and keeps the last year of GPOs could be used so it does not add any overhead for Administrators.

To export the GPOs to an HTML document use GPMC.MSC, Select each GPO and use the menu option <Action><Save Report>, specify the directory, file name and Save As Type.

Default Domain
Policy.mht

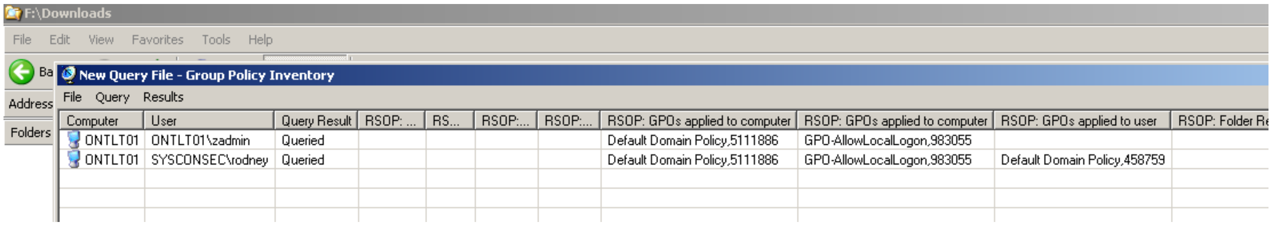
5.9.1 GPResult

GPRESULT can be used to show what GPOs are in effect on a specific system.

```
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>
```

5.9.2 GPInventory

The program GPInventory.exe from Microsoft can also report on Group Policies installed on specified systems:


F:\Downloads
File Edit View Favorites Tools Help
Ba
Address
Folders
New Query File - Group Policy Inventory
File Query Results

Computer	User	Query Result	RSOP: ...	RS...	RSOP:...	RSOP:...	RSOP: GPOs applied to computer	RSOP: GPOs applied to computer	RSOP: GPOs applied to user	RSOP: Folder Re
ONTLT01	ONTLT01\zadmin	Queried					Default Domain Policy,5111886	GPO-AllowLocalLogon,983055		
ONTLT01	SYSCONSEC\rodney	Queried					Default Domain Policy,5111886	GPO-AllowLocalLogon,983055	Default Domain Policy,458759	

Results from GPInventory.exe can be saved as an XML or text file and loaded into Excel or Access for analysis.

5.9.3 GPLogView

GPLogView from Microsoft only runs on Vista. GPLogView dumps Group Policy related events from the System Event Log channel and the Group Policy Operational Event Log channel.

5.10 Security Settings and GPOs Audit Program

- Determine whether policy, standards and procedures regarding security settings and Group Policy Objects have been formalized and implemented.
- Determine whether policy, standards and procedures regarding security settings and Group Policy Objects is appropriate.
- Identify sensitive security settings by reviewing vendor documentation, security web sites, publications, policies, standards, procedures and interviews with system managers.
- Determine appropriate values for security settings and GPOs
- Obtain listings that show the security settings and GPOs that are implemented. (Reference the request list at the end of the presentation.)
- Verify that security settings and GPOs are appropriate.

6 User Profiles, Groups, and Organizational Units

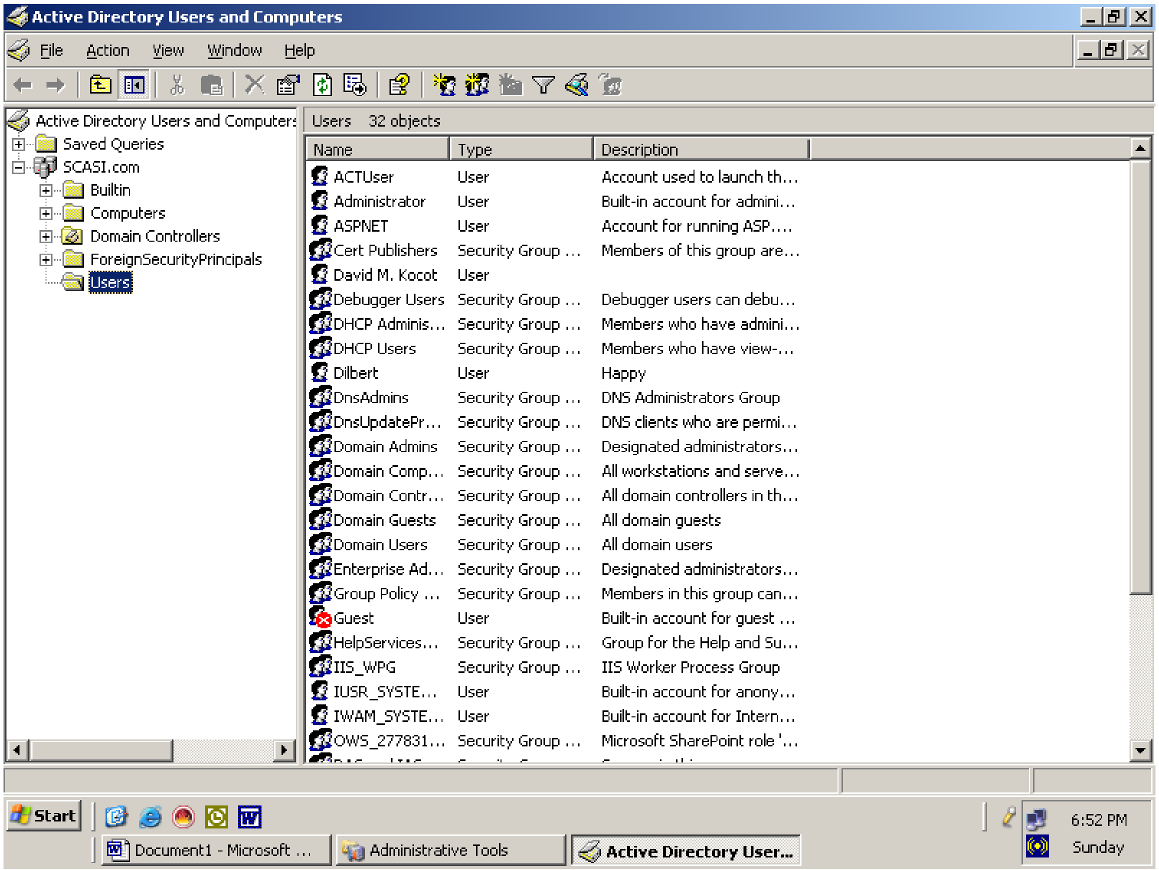
6.1 User Profiles

User profiles identify people and process owners to the domain and systems. User profiles are assigned to groups which define access to resources and functions.

6.1.1 RunAS.exe

```
C:\Program Files\Windows Resource Kits\Tools>runas /user:sysconsec\rodney.adm "subinacl
/outputlog=c:\Audits\subinaclTujLT12.txt /keyreg /display"
Enter the password for sysconsec\rodney.adm:
Attempting to start subinacl /outputlog=c:\Audits\subinaclTujLT12.txt /keyreg /display as user
"sysconsec\rodney.adm" ...

C:\Program Files\Windows Resource Kits\Tools>
```

6.1.2 Active Directory Users and Computers:



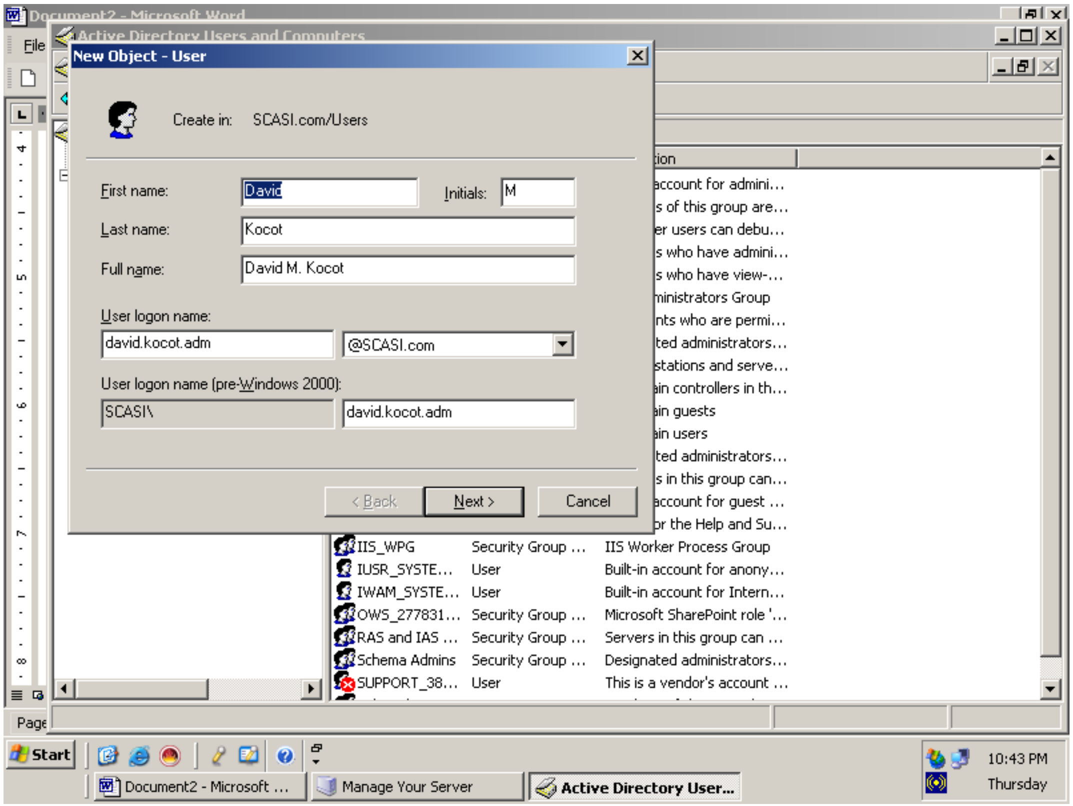
- Active Directory Users and Computers
  - Saved Queries
  - SCASI.com
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Users

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 '...

To add a user, go to the “Active Directory Users and Computers” snap-in, right-click the “Users” folder, then left click “New” and “User.”

6.1.3 New Object – User - Identifying Information:



New Object - User

Create in: SCASI.com/Users

First name: David

Initials: M

Last name: Kocot

Full name: David M. Kocot

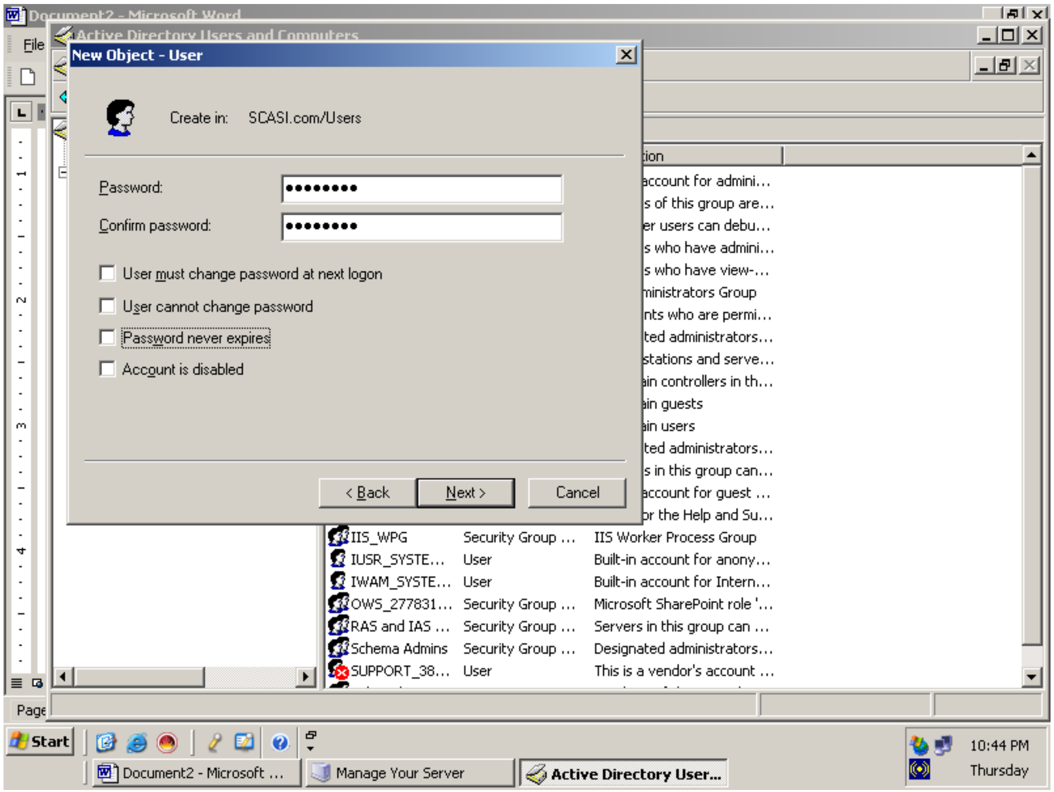
User logon name: david.kocot.adm @SCASI.com

User logon name (pre-Windows 2000): SCASI\ david.kocot.adm

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 '...
RAS and IAS ...	Security Group ...	Servers in this group can ...
Schema Admins	Security Group ...	Designated administrators...
SUPPORT_38...	User	This is a vendor's account ...

Document2 - Microsoft Word
Active Directory Users and Computers
< Back
Next >
Cancel
Start
Document2 - Microsoft ...
Manage Your Server
Active Directory User...
10:43 PM
Thursday

6.1.4 New Object - User - Password



Create in: SCASI.com/Users

Password: ••••••••

Confirm password: ••••••••

□ User must change password at next logon

□ User cannot change password

□ Password never expires

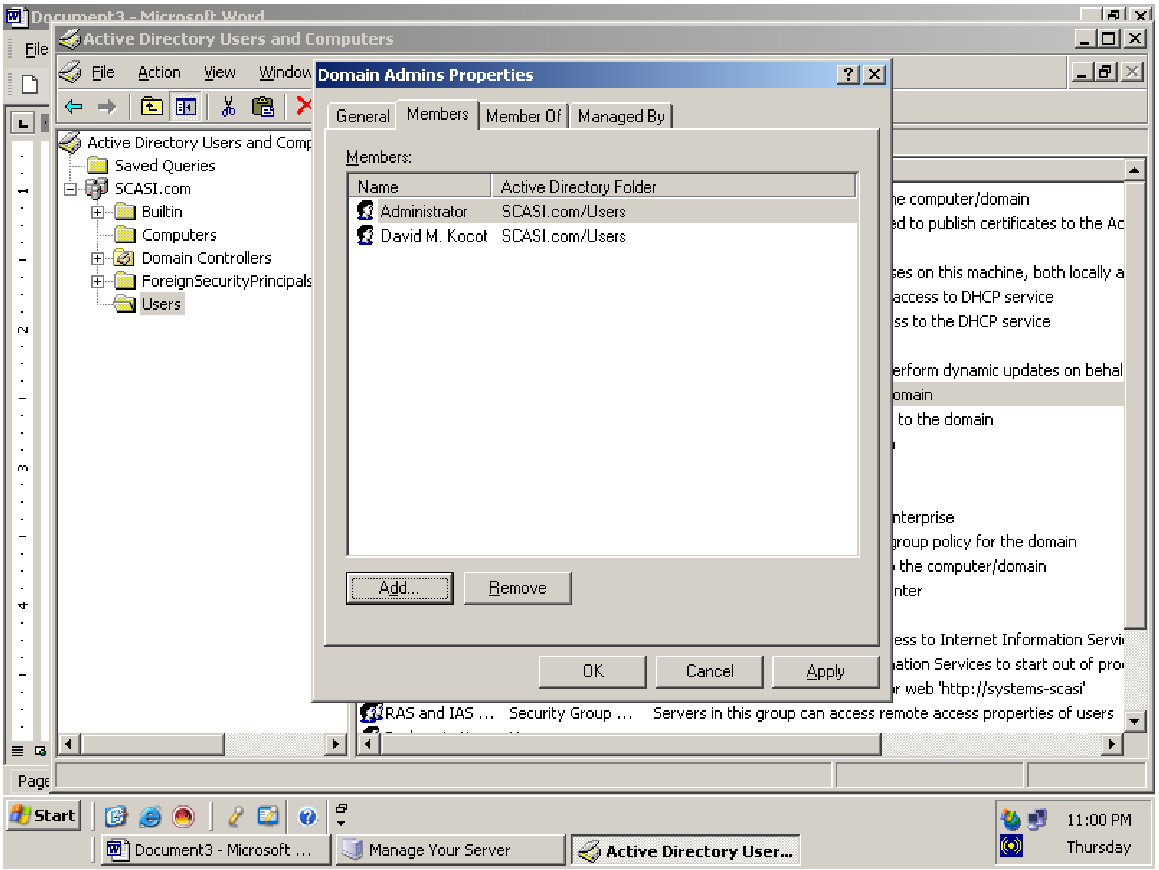
□ Account is disabled

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 '...
RAS and IAS ...	Security Group ...	Servers in this group can ...
Schema Admins	Security Group ...	Designated administrators...
SUPPORT_38...	User	This is a vendor's account ...

When creating a new user the “User must change password at next logon” should be checked so only the user knows their password. The users properties should be reviewed and updated with the users address, phone number and other identifying information so that the user can be confirmed if their password needs to be reset.

6.1.5 Adding Users to Groups

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

6.1.6 Administrators

Domains are created and maintained by people with special magic powers called Administrators. Their user accounts belong to various Administrator groups, from which their magic powers derive. There are several different types of administrators in Windows. The three main types of administrators in a Windows Active Directory environment are Local Administrators, who have full and complete power over a given machine; Domain Admins, who have full and complete power over the domain; and Enterprise Admins, who have full and complete power over domain trees and domain forests. There are other types of administrator accounts, but their powers are more limited; for instance, DHCP Admins. You can have administrative rights over one thing and not have it over another, or vice versa; for instance, in a large environment, the end user support group probably has local administrator rights on all workstations they are responsible for, but will not be members of the Domain Administrators group.

It is very easy – and also very dangerous - to underestimate an administrator's power. Basically, an administrator either has or (if they're halfway competent) can get full control over any file, directory, program, service, or device on a machine and/or domain to which they have administrator rights. There is a GPO that can be set which allows a user to circumvent all resource protections.

In addition, most distributed applications, such as Microsoft Exchange or network managed anti-virus systems, are also managed by special administrators. These administrators also have untold powers over the applications they administer.

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

6.1.7 Security Accounts Manager (SAM)

The Security Accounts Manager (SAM) database is stored as a registry hive file. The SAM file is usually in c:\Windows\System32\Config and contains user and group information. The following site describes the location and contents of the SAM in detail:

http://www.beginningtoseethelight.org/ntsecurity/index.php

A Google search reveals many tools that allow passwords local and domain passwords to be compromised:

Ophcrack
Cain&Able.
…

6.2 Groups

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

6.3 Global Groups

Global groups are used to grant access to resources globally.

6.3.1 NET GROUP

```
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.
```

6.4 Local Groups

Local groups are used to grant access to local resources.

6.4.1 NET LOCALGROUP

```
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.
```

6.5 User Administration Audit Procedures

- Determine whether user administration policies and procedures are formalized and implemented.
- Determine whether user administration policies and procedures are adequate and appropriate.
- Obtain a description of all user groups. (This will also be used when reviewing resource protections.)
- Determine whether all user attributes meet requirements defined in policy and procedures.
- Verify that every userid is assigned to an individual.
- Verify that there are no shared userids.
- Verify that unused user profiles are removed from the system when no longer used.
- Verify that users in sensitive groups such as Administrators, Domain Administrators, Enterprise Administrators, etc. are appropriate.
- Verify that vendor user profiles are adequately controlled.

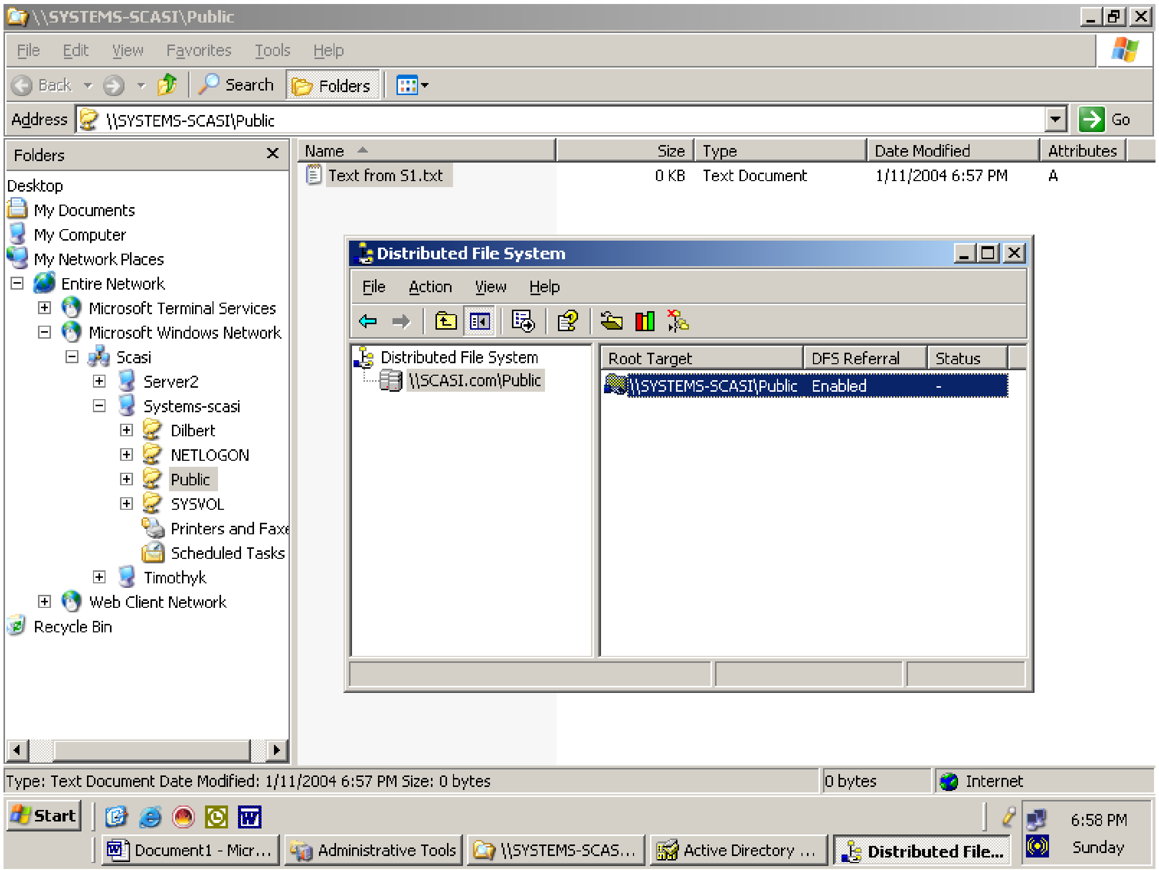
7 Resource Protections

7.1 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.

7.2 Encrypting File System

7.3 DFS – Distributed File System



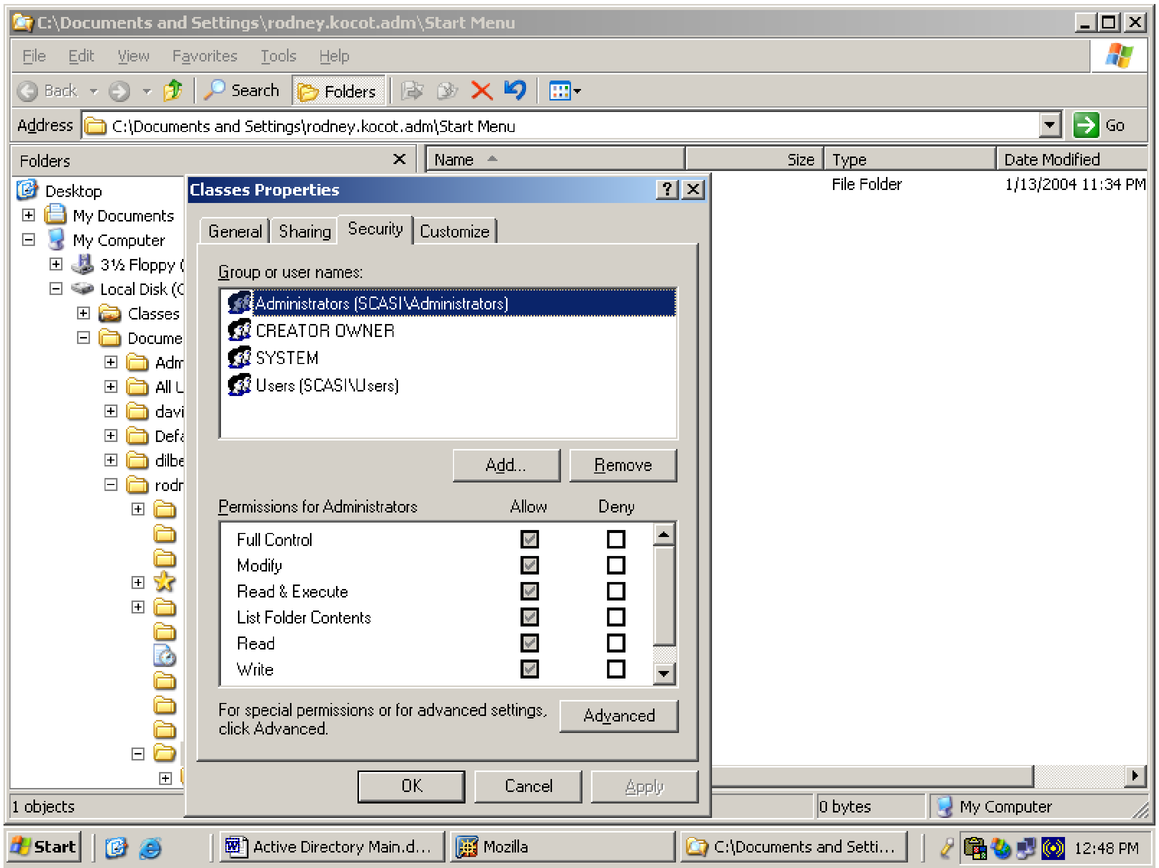
Address: \\SYSTEMS-SCASI\Public

Name	Size	Type	Date Modified	Attributes
Text from S1.txt	0 KB	Text Document	1/11/2004 6:57 PM	A

Root Target	DFS Referral	Status
\\SYSTEMS-SCASI\Public	Enabled	-

Type: Text Document Date Modified: 1/11/2004 6:57 PM Size: 0 bytes

7.4 File Security Properties



Classes Properties

General | Sharing | Security | Customize

Group or user names:

- Administrators (SCASI\Administrators)
- CREATOR OWNER
- SYSTEM
- Users (SCASI\Users)

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

For special permissions or for advanced settings, click Advanced.

7.5 Permission options

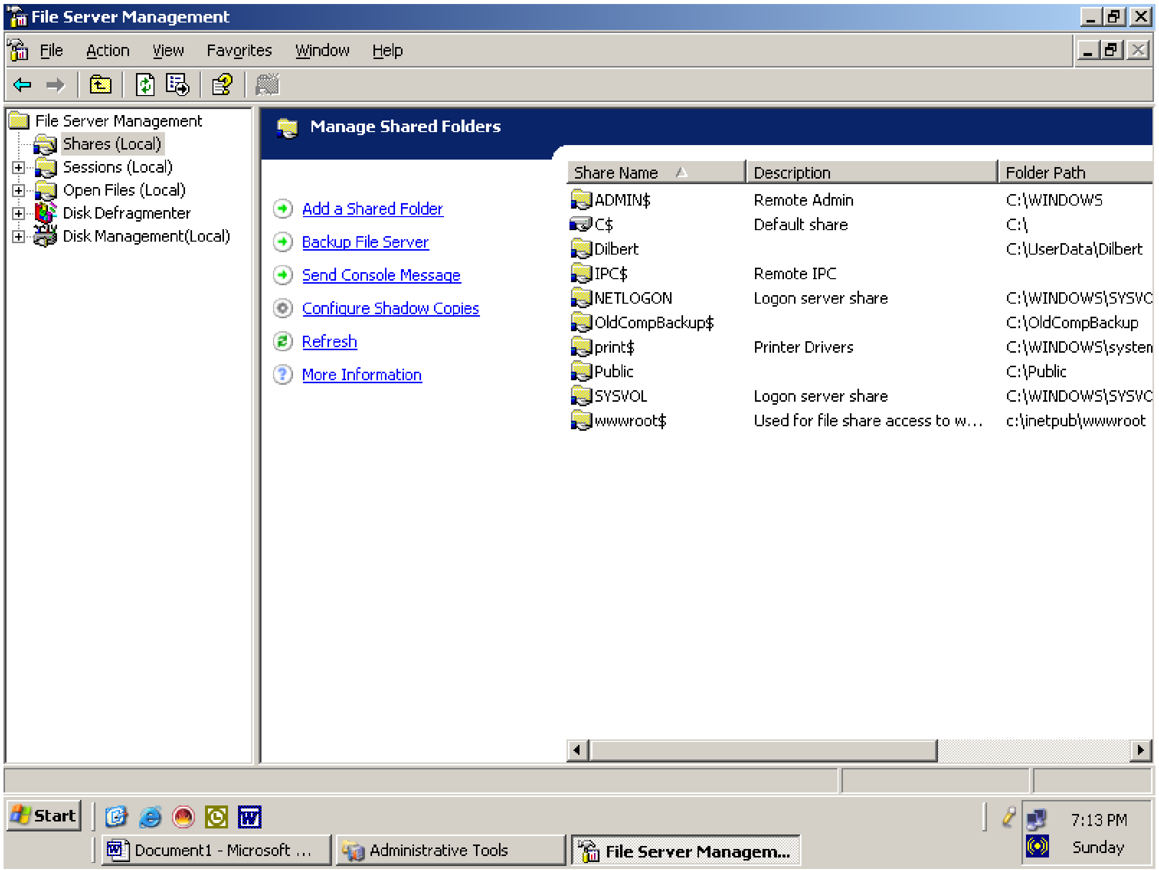
Execute	The user/group can execute the file if it is a program
Read	The user/group can read the file, but not make any changes to it
Write	The user/group can write to or create folders and files within a folder
Change Permissions	The user/group can modify the permissions of the file
Full Control	The user/group has all possible permissions on the file or folder
Traverse Folder	This applies to folders only; it permits or denies users to move through a folder to access another folder even if the user or group has no permissions on the traversed folder.
List Folder	Allows or denies someone to view the contents (all folders and files) of a folder
Read Attributes	Allows the viewing of the file or folder attributes (Read only, Hidden, Archive, etc.)
Read Extended Attributes	Extended attributes are usually assigned by programs that use the file
Create Folders	Allows the creation of folders
Write Attributes	Allows the modification of attributes.
Write Extended Attributes	Allows the modification of extended attributes
Delete Subfolders	Allows the deletion of subfolders and the files they contain, even if the delete permission is not granted.
Delete	Allows the deletion of files and folders.
Read Permissions	Allows the viewing of the file or folder's permissions.
Take Ownership	Allows the user or group to take ownership of the file.

The most commonly used permissions can be changed (if, of course, you have the Change Permissions permission on the object!) by clicking on the Permissions button of the sharing tab of the file or folder's properties menu. The more obscure permissions can be changed by clicking on the Advanced button of the properties message box.

Permissions can be granted, denied, or unassigned. Unassigned permission is the same as denied, unless the user or group is explicitly granted the permission through membership in another group.

By default, folders and files automatically inherit the permission settings of their container folder. This inheritance can be turned off, however. If the parent object does not have its permissions set (because it is not shared), a created child object automatically grants the Everyone group Read permission.

7.6 File Server Management

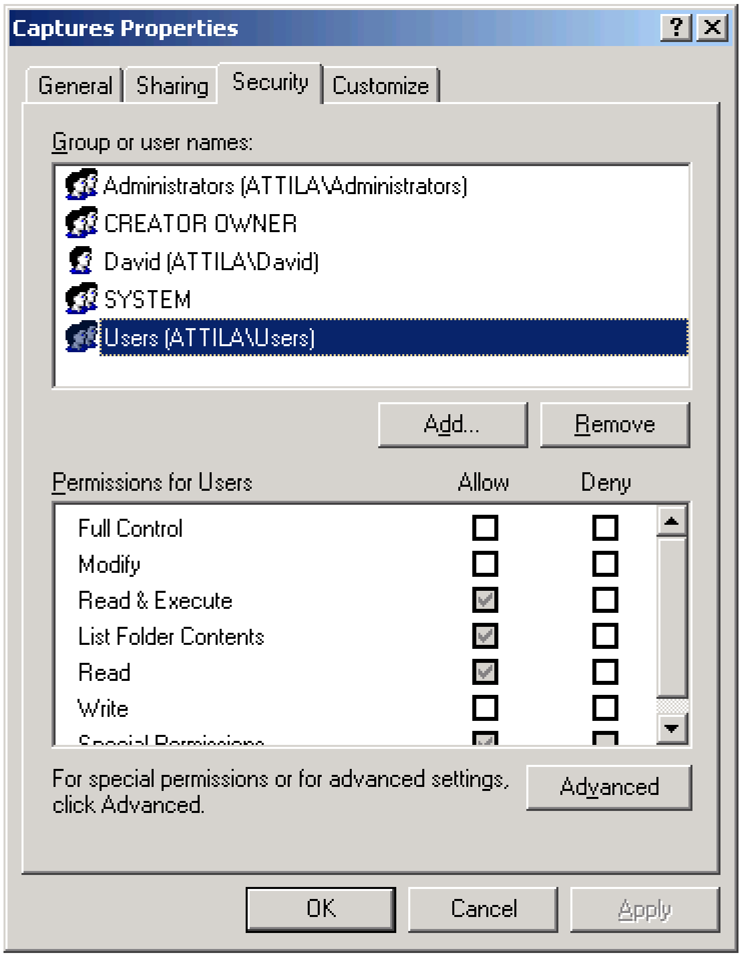


Share Name	Description	Folder Path
ADMIN$	Remote Admin	C:\WINDOWS
C$	Default share	C:\
Dilbert		C:\UserData\Dilbert
IPC$	Remote IPC	
NETLOGON	Logon server share	C:\WINDOWS\SYSVC
OldCompBackup$		C:\OldCompBackup
print$	Printer Drivers	C:\WINDOWS\systen
Public		C:\Public
SYSVOL	Logon server share	C:\WINDOWS\SYSVC
wwwroot$	Used for file share access to w...	c:\inetpub\wwwroot

7.7 Share Protections

In Windows, information is made available to other users on the network through the use of *Shares*. A share is simply a folder that people can access from the network. Generally, these shares are accessed by mapping a drive – a process where the share is given a drive letter and is used just as if it was another local hard drive.

Access to shares is controlled by permissions. There are two types of permissions; the first is share permissions, which determine who can do what with the share, and the second is NTFS security permissions, which determine who can do what with the files and folders within the share.



Group or user names:

- Administrators (ATTILA\Administrators)
- CREATOR OWNER
- David (ATTILA\David)
- SYSTEM
- Users (ATTILA\Users)

Permissions for Users	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	□	□
Special Permissions	□	□

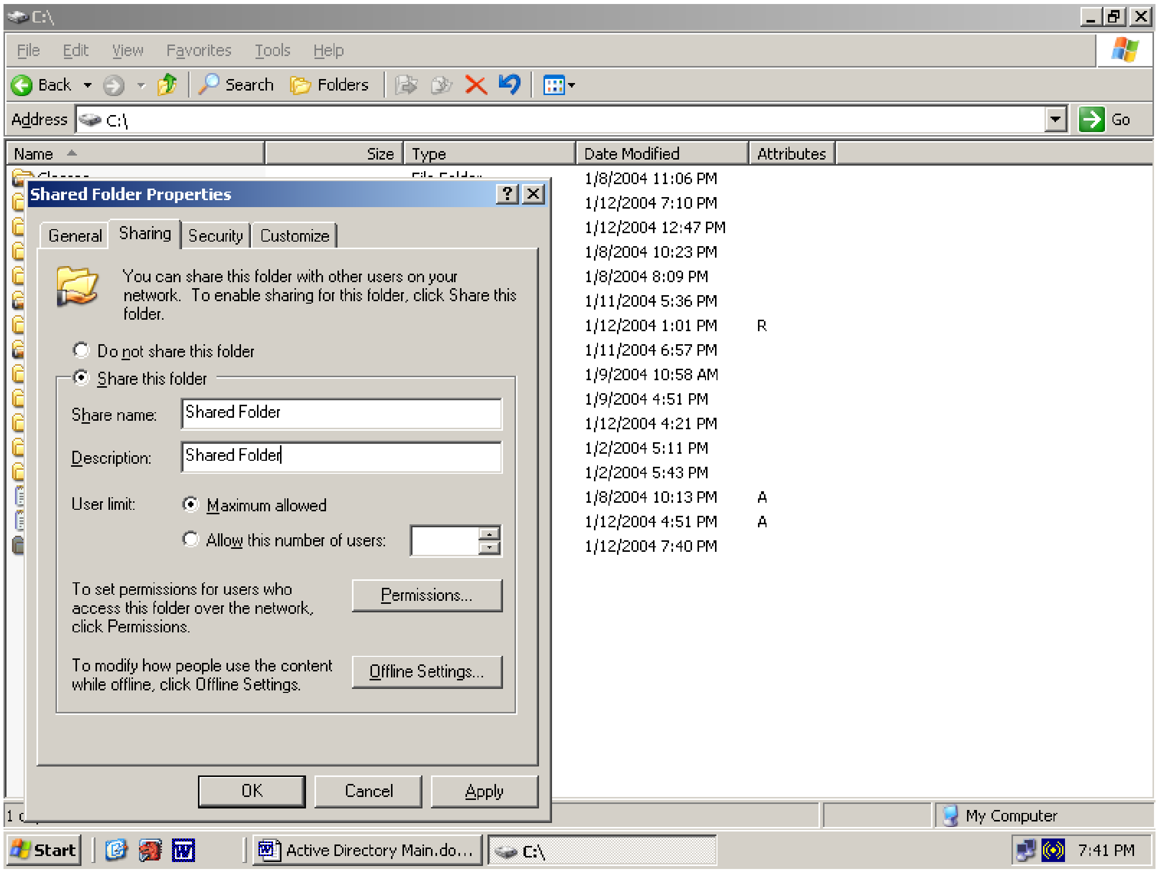
For special permissions or for advanced settings, click Advanced.

In the above example, members of the Users group on the machine called ATTILA (effectively, anyone who logs on to the machine) can read, execute, and list the contents of this folder called "captures". If you have full control over the folder, you can grant or revoke permissions to users and group at your pleasure. There are a few simple rules to keep in mind about share and NTFS permissions, namely:

1) No checkmarks = No access. Permissions are inherited. If you belong to a group that has read and write access to a folder, YOU have read and write access to the folder.
2) You can inherit permissions from multiple sources. You may belong to one group that only has read access, but if you belong to another group which has write permission, you *also* have write permission. Permissions can also be assigned to individual users.
3) The most restrictive permissions apply. If you belong to one group that has been granted permission to a file and another group which has been explicitly denied permission, you don't have permission.
4) No checkmarks=no access. If neither the Permit nor Deny checkboxes are checked for a particular level of access, that access is denied – unless it is specifically granted somewhere else.

Shared files and folders can and should be configured to limit access only to those who need it. This is an easy task; simply view the Sharing tab of the file or folder properties and add or remove whichever individuals or groups you wish and modify their permissions by selecting the appropriate checkboxes.

7.7.1 Shared Folder Properties:



Date Modified	Attributes
1/8/2004 11:06 PM	
1/12/2004 7:10 PM	
1/12/2004 12:47 PM	
1/8/2004 10:23 PM	
1/8/2004 8:09 PM	
1/11/2004 5:36 PM	
1/12/2004 1:01 PM	R
1/11/2004 6:57 PM	
1/9/2004 10:58 AM	
1/9/2004 4:51 PM	
1/12/2004 4:21 PM	
1/2/2004 5:11 PM	
1/2/2004 5:43 PM	
1/8/2004 10:13 PM	A
1/12/2004 4:51 PM	A
1/12/2004 7:40 PM	

Shared Folder Properties

General | Sharing | Security | Customize

You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Shared Folder

Description: Shared Folder

User limit: ● Maximum allowed

○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions. [Permissions...]

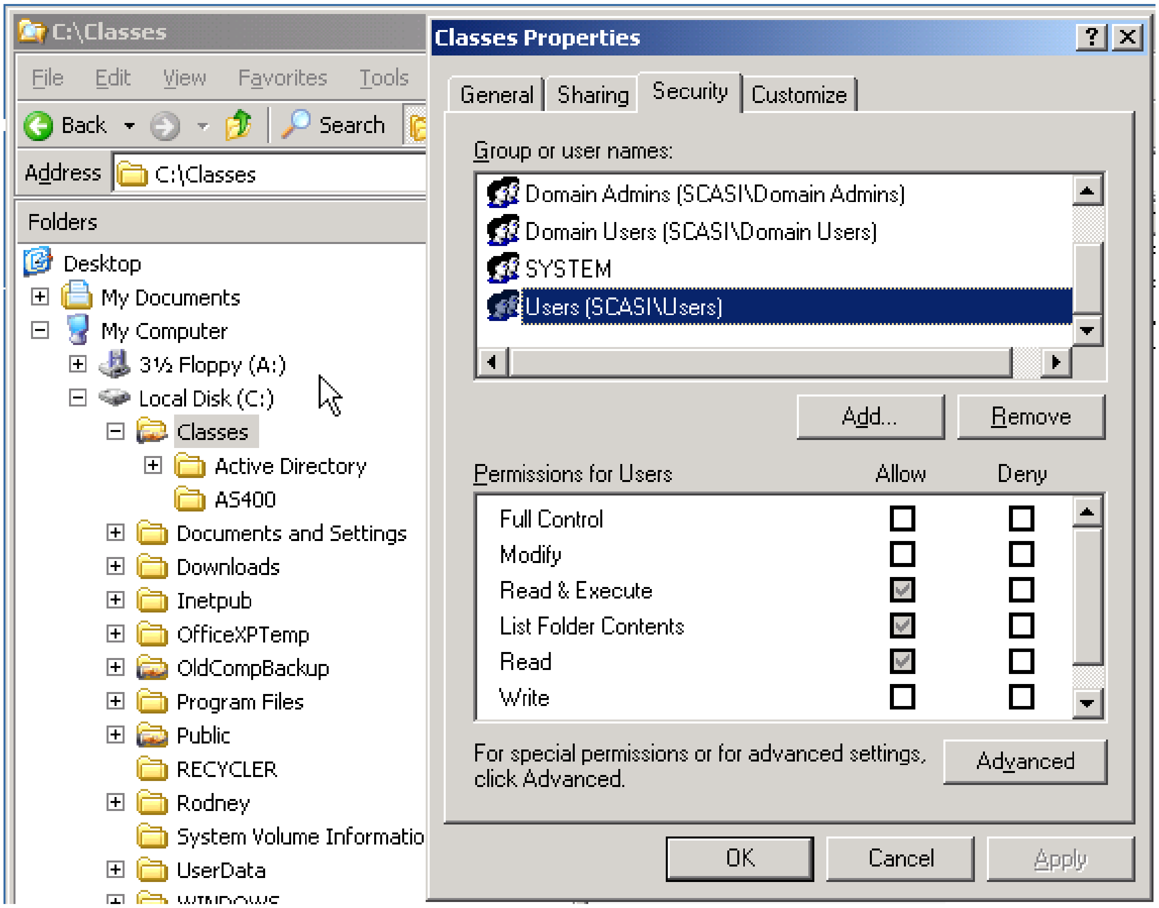
To modify how people use the content while offline, click Offline Settings. [Offline Settings...]

[OK] [Cancel] [Apply]

7.8 Directory and File Protections

Who should decide if your organization is going to violate federal and state laws?

A common gottcha auditors experience is being given access to a directory and still not being able to access the data. Often, the auditor userid/group is added to the security ACL on the directory, but the administrator forgets to add the userid/group to the sharing permissions as shown in the following two screen prints:

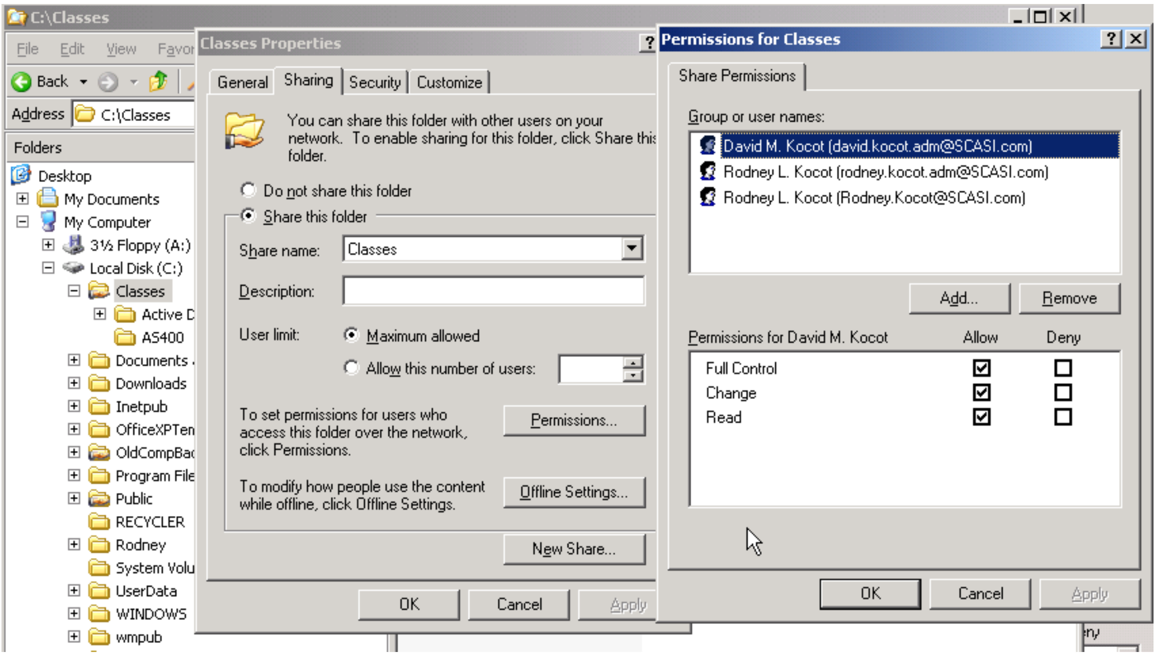


Group or user names:

- Domain Admins (SCASI\Domain Admins)
- Domain Users (SCASI\Domain Users)
- SYSTEM
- Users (SCASI\Users)

Permissions for Users	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	□	□

For special permissions or for advanced settings, click Advanced.



You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Classes

Description:

User limit: ● Maximum allowed

○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions.

To modify how people use the content while offline, click Offline Settings.

Group or user names:

- David M. Kocot (david.kocot.adm@SCASI.com)
- Rodney L. Kocot (rodney.kocot.adm@SCASI.com)
- Rodney L. Kocot (Rodney.Kocot@SCASI.com)

Permissions for David M. Kocot	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

7.9 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:
```

- ✓ Cacls z: shows the share protection.
- ✓ Cacls z:*.* shows the protection on files in the share root directory.
- ✓ Cacls z:*.* /T /C shows the protection on all the files on the disk.

In Vista CACLS is "depreciated" and Icacls should be used.

7.10 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
```

7.11 SubInACL.exe

Microsoft Security Descriptor Migration and Editing Tool.

7.12 Openfiles

```
C:\Documents and Settings\Rodney>openfiles /?

OPENFILES /parameter [arguments]

Description:
    Enables an administrator to list or disconnect files and folders
    that have been opened on a system.

Parameter List:
    /Disconnect      Disconnects one or more open files.

    /Query           Displays files opened locally or from shared folders.

    /Local           Enables / Disables the display of local open files.
                     Note: Enabling this flag adds performance overhead.

Examples:
    OPENFILES /Disconnect /?
    OPENFILES /Query /?
    OPENFILES /Local /?


C:\Documents and Settings\Rodney>openfiles

Files Opened Locally:
---------------------

ID    Process Name         Open File (Path\executable)
===== ==================== ==================================================
12    explorer.exe         C:\Documents and Settings\Rodney
556   explorer.exe         C:\Documents and Settings\Rodney\Desktop
560   explorer.exe         C:\Audits\K3DES\USBank
564   explorer.exe         C:\Documents and Settings\All Users\Desktop
568   explorer.exe         C:\..\Application Data\Microsoft\CD Burning
640   explorer.exe         C:\..\Content.IE5\index.dat
688   explorer.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
768   explorer.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
800   explorer.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
828   explorer.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
876   explorer.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
888   explorer.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
948   explorer.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
952   explorer.exe         C:\..\History\History.IE5\index.dat
956   explorer.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
1172  explorer.exe         C:\Documents and Settings\Rodney\PrintHood
1208  explorer.exe         C:\Documents and Settings\Rodney\Cookies\index.dat
1256  explorer.exe         C:\Documents and Settings\All Users\Start Menu
1384  explorer.exe         C:\Documents and Settings\Rodney\Start Menu
1408  explorer.exe         C:\..6595b64144ccf1df_1.0.2600.2180_x-ww_522f9f82
1728  explorer.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
```

```
1920  explorer.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
2008  explorer.exe         C:\Documents and Settings\Rodney\NetHood
2144  explorer.exe         C:\..\MSHist012007031220070313\index.dat
12    igfxtray.exe         C:\Documents and Settings\Rodney
60    igfxtray.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
12    hkcmd.exe            C:\Documents and Settings\Rodney
12    igfxpers.exe         C:\Documents and Settings\Rodney
12    SynTPLpr.exe         C:\Documents and Settings\Rodney
12    SynTPEnh.exe         C:\Documents and Settings\Rodney
56    SynTPEnh.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
12    SOUNDMAN.EXE         C:\Documents and Settings\Rodney
60    SOUNDMAN.EXE         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
12    PDVDServ.exe         C:\Documents and Settings\Rodney
60    PDVDServ.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
12    LaunchAp.exe         C:\Documents and Settings\Rodney
60    LaunchAp.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
52    Powerkey.exe         C:\Program Files\Launch Manager
12    HotkeyApp.exe        C:\Documents and Settings\Rodney
104   HotkeyApp.exe        C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
488   HotkeyApp.exe        C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
492   HotkeyApp.exe        C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
12    OSDCtrl.exe          C:\Documents and Settings\Rodney
56    OSDCtrl.exe          C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
12    WButton.exe          C:\Documents and Settings\Rodney
16    WButton.exe          C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
12    epm-dm.exe           C:\Documents and Settings\Rodney
60    epm-dm.exe           C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
12    wuauclt.exe          C:\WINDOWS\system32
16    wuauclt.exe          C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
28    wuauclt.exe          C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
128   wuauclt.exe          C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
156   wuauclt.exe          C:\WINDOWS\WindowsUpdate.log
…
532   wuauclt.exe          C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
12    eDSloader.exe        C:\Documents and Settings\Rodney
60    eDSloader.exe        C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
340   eDSloader.exe        C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
12    ccApp.exe            C:\Documents and Settings\Rodney
64    ccApp.exe            C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
488   ccApp.exe            C:\..\Microsoft\SystemCertificates\My
712   ccApp.exe            C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
736   ccApp.exe            C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
60    VPTray.exe           C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
288   VPTray.exe           C:\Program Files\Symantec AntiVirus
60    hpcmpmgr.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
76    hpcmpmgr.exe         C:\Program Files\HP\hpcoretech\hpcmerr.log
276   hpcmpmgr.exe         C:\Program Files\HP\hpcoretech
356   hpcmpmgr.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
360   hpcmpmgr.exe         C:\..\Content.IE5\index.dat
384   hpcmpmgr.exe         C:\Documents and Settings\Rodney\Cookies\index.dat
392   hpcmpmgr.exe         C:\..\History\History.IE5\index.dat
440   hpcmpmgr.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
444   hpcmpmgr.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
12    point32.exe          C:\Documents and Settings\Rodney
16    point32.exe          C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
84    point32.exe          C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
12    hptskmgr.exe         C:\WINDOWS\system32
60    hptskmgr.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
484   hptskmgr.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
504   hptskmgr.exe         C:\..\Content.IE5\index.dat
524   hptskmgr.exe         C:\Documents and Settings\Rodney\Cookies\index.dat
532   hptskmgr.exe         C:\..\History\History.IE5\index.dat
580   hptskmgr.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
584   hptskmgr.exe         C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
12    TrueCrypt.exe        C:\Documents and Settings\Rodney
60    TrueCrypt.exe        C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
88    WINWORD.EXE          C:\..\Microsoft Shared\PROOF\MSGR3EN.LEX
116   WINWORD.EXE          C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
212   WINWORD.EXE          C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
248   WINWORD.EXE          C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
488   WINWORD.EXE          C:\..\Microsoft\Templates\Normal.dot
496   WINWORD.EXE          C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
```

```
…
12    cmd.exe             C:\Documents and Settings\Rodney
96    cmd.exe             C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
12    openfiles.exe       C:\Documents and Settings\Rodney
1924  openfiles.exe       C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03


Files Opened Remotely via local share points:
---------------------------------------------
INFO: No shared open files found.
```

7.13 Resource Protections Audit Program

- Determine whether policy has been formalized and implemented for managing resource protections.
- Determine whether critical and sensitive resources have been identified.
- Identify critical and sensitive resources. (look at all web servers, network shares, applications, and databases.)
- Determine appropriate protection for critical and sensitive resources.
- Generate DIR, SubInACL and CALCS listings to determine security for resources.
- Determine whether critical and sensitive resources are protected appropriately.

8 Services and Privileged Programs

8.1 Services and Privileged Programs Overview

Microsoft and other vendors will often have descriptions of their services. The site www.BlackViper.com maintains a description of all Windows services.

8.2 Services and Privileged Programs Commands

8.2.1 Services.msc

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.

8.2.2 SC

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
        WAIT_HINT          : 0x0

SERVICE_NAME: ALG
DISPLAY_NAME: Application Layer Gateway Service
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0      (0x0)
        SERVICE_EXIT_CODE  : 0      (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: AppMgmt
DISPLAY_NAME: Application Management
        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
        WAIT_HINT          : 0x0

SERVICE_NAME: AudioSrv
DISPLAY_NAME: Windows Audio
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0      (0x0)
        SERVICE_EXIT_CODE  : 0      (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

8.3 Tasklist

```
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"
```

```
"spoolsv.exe","1748","Spooler"
"cvpnd.exe","1924","CVPND"
"OPHALDCS.EXE","1948","DCSLoader"
"DefWatch.exe","1964","DefWatch"
"MDM.EXE","2036","MDM"
"OSCMUtilityService.exe","136","OSCM Utility Service"
"SavRoam.exe","240","SavRoam"
"svchost.exe","340","stisvc"
"Rtvscan.exe","408","Symantec AntiVirus"
"CALMAIN.exe","596","CCALib8"
"explorer.exe","1324","N/A"
"alg.exe","724","ALG"
"igfxtray.exe","876","N/A"
"hkcmd.exe","1164","N/A"
"igfxpers.exe","1520","N/A"
"SynTPLpr.exe","1536","N/A"
"SynTPEnh.exe","1528","N/A"
"epm-dm.exe","1364","N/A"
"eDSloader.exe","1988","N/A"
"ccApp.exe","1936","N/A"
"VPTray.exe","2072","N/A"
"point32.exe","2120","N/A"
"taskmgr.exe","2720","N/A"
"wuauclt.exe","2956","N/A"
"TrueCrypt.exe","3004","N/A"
"notepad.exe","1296","N/A"
"WINWORD.EXE","2424","N/A"
"cmd.exe","3340","N/A"
"notepad.exe","2460","N/A"
"tasklist.exe","2360","N/A"
"wmiprvse.exe","2740","N/A"
```

The following script can enumerate all the services running on all the servers in a domain:

EnumerateAllServicesScript.txt

8.3.1 Schtasks /Query

Schtasks can be used to list all the scheduled tasks on the system. Schtasks /query shows by folder, the task name, status and next run time for each scheduled task. The Schtasks command works on the local and remote systems provided the user has appropriate access.

8.4 Services and Privileged Programs Audit Program

1. Determine whether policy and procedures have been formalized and implemented for managing services and privileged programs.
2. Obtain a list of authorized services, privileged programs and drivers.
3. Review the list of authorized services, privileged programs and drivers for appropriateness.
4. Generate a list of running services, privileged programs and drivers from each system in the domain.
5. Verify that only authorized and appropriate services, privileged programs and drivers are running on the systems.
6. Verify that required services such as antivirus are running on each system.

9 Network Access

Never connect a windows system directly to the internet. Always place a Windows system behind at least one firewall.

9.1 Network Configuration

A network links all your cyber resources like a road system links people to homes, buildings, parks and all other resources on land.   There are thousands components and ways to implement a network. A network diagram and documentation are necessary to obtain an understanding of the network.

9.1.1 Network Address Translation

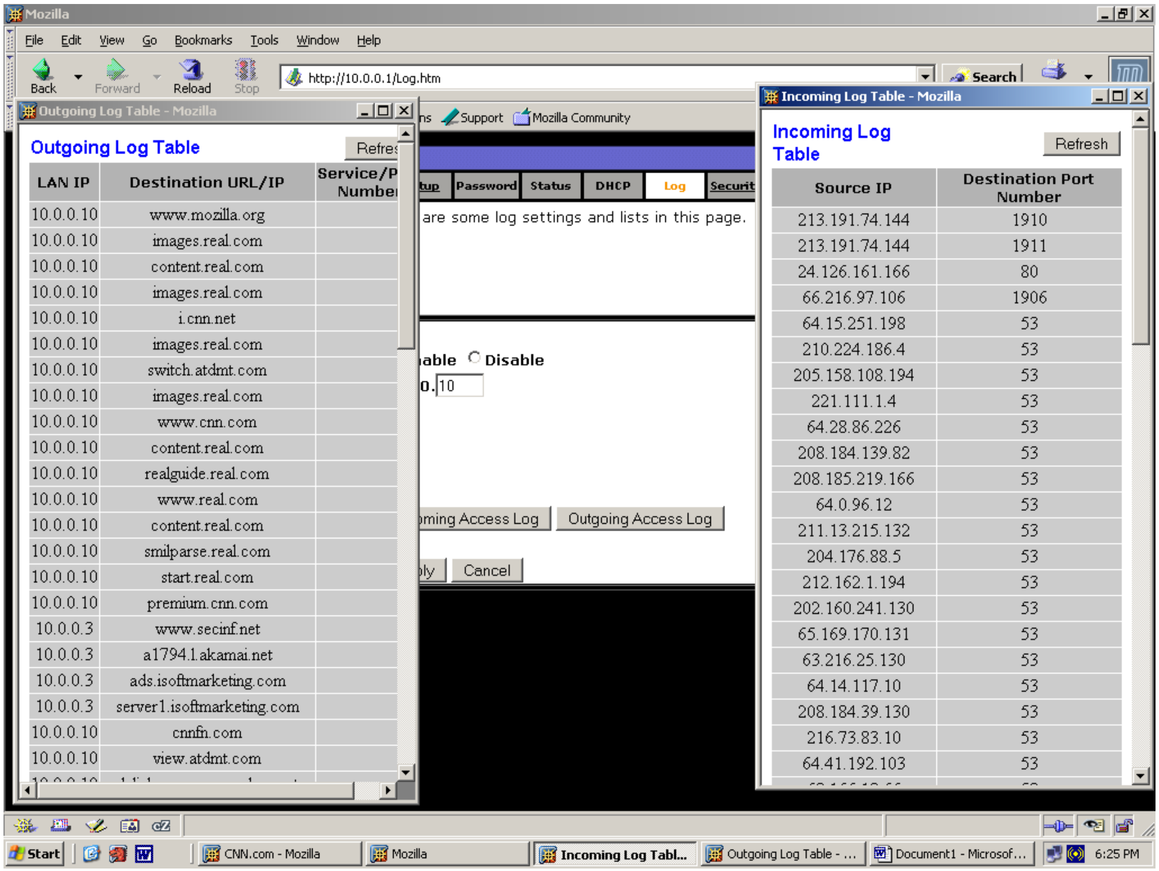
Network Address Translation (NAT) is a way of "hiding" a network of computers from the outside world. Instead of assigning a group of public addresses to hosts, a set of private addresses are used (in large organizations, these private addresses are usually 10.X.X.X). A router or gateway keeps a public address, and all the hosts on the network go through this device – using its public IP Address - to access outside resources. In some ways, NATing acts as a firewall; NATed networks are more secure than non-NATed networks, since it is much more difficult to determine the IP address of a host with a NATed address.

9.1.2 Routers and Firewalls

Routers and firewalls are the first line of defense against external attacks. Properly configured, they can greatly reduce the threat to a network. In addition, firewall and router logs can be helpful in determining the source of an attack.

Windows Server 2003 and Windows XP both come with an integrated firewall Most large organizations will use dedicated equipment for a firewall, and will find that this feature is unnecessary except on servers that communicate directly with outside networks (such as the internet)

Router Logs:



Outgoing Log Table - Mozilla

Outgoing Log Table

Refres

LAN IP	Destination URL/IP	Service/P Number
10.0.0.10	www.mozilla.org	
10.0.0.10	images.real.com	
10.0.0.10	content.real.com	
10.0.0.10	images.real.com	
10.0.0.10	i.cnn.net	
10.0.0.10	images.real.com	
10.0.0.10	switch.atdmt.com	
10.0.0.10	images.real.com	
10.0.0.10	www.cnn.com	
10.0.0.10	content.real.com	
10.0.0.10	realguide.real.com	
10.0.0.10	www.real.com	
10.0.0.10	content.real.com	
10.0.0.10	smilparse.real.com	
10.0.0.10	start.real.com	
10.0.0.10	premium.cnn.com	
10.0.0.3	www.secinf.net	
10.0.0.3	a1794.l.akamai.net	
10.0.0.3	ads.isoftmarketing.com	
10.0.0.3	server1.isoftmarketing.com	
10.0.0.10	cnnfn.com	
10.0.0.10	view.atdmt.com	

are some log settings and lists in this page.

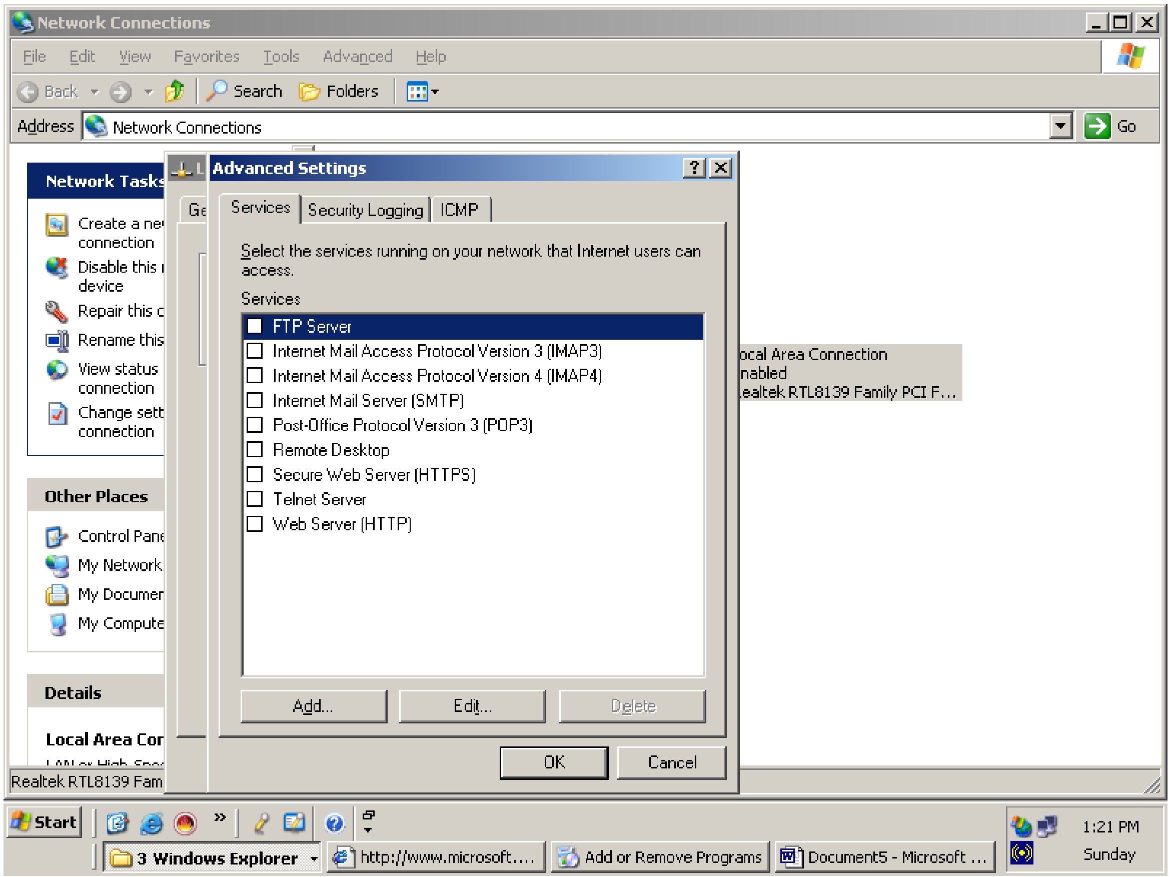
Incoming Log Table - Mozilla

Incoming Log Table

Refresh

Source IP	Destination Port Number
213.191.74.144	1910
213.191.74.144	1911
24.126.161.166	80
66.216.97.106	1906
64.15.251.198	53
210.224.186.4	53
205.158.108.194	53
221.111.1.4	53
64.28.86.226	53
208.184.139.82	53
208.185.219.166	53
64.0.96.12	53
211.13.215.132	53
204.176.88.5	53
212.162.1.194	53
202.160.241.130	53
65.169.170.131	53
63.216.25.130	53
64.14.117.10	53
208.184.39.130	53
216.73.83.10	53
64.41.192.103	53

Windows Server 2003 Fire Wall Advanced Settings:



Advanced Settings

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)

To access the firewall feature, go to the Network Connections applet, select the Advanced tab of the Properties box, and click the checkbox to enable it. To configure the firewall, click Settings and select which services or protocols you wish to enable.

9.1.3 Dynamic Host Configuration Protocol (DHCP)

DHCP leases IP addresses to workstations. DHCP can run in routers, servers, or other devices. Incorrect configuration of DHCP can cause devices and the network to be unavailable.

An alternate DHCP configuration is available in Windows workstations that allows an IP address to be specified if one can not be licensed.

9.1.4 GetMAC.exe

9.1.5 Hostname.exe

9.1.6 NSLookUp.exe

9.2 PathPing.exe

9.3 Network Commands

9.3.1 NET /?

```
C:\Documents and Settings\rodney.kocot.adm>net help
The syntax of this command is:

NET HELP
command
      -or-
NET command /HELP

   Commands available are:

   NET ACCOUNTS             NET HELP             NET SHARE
   NET COMPUTER             NET HELPMSG          NET START
   NET CONFIG               NET LOCALGROUP       NET STATISTICS
   NET CONFIG SERVER        NET NAME             NET STOP
   NET CONFIG WORKSTATION   NET PAUSE            NET TIME
   NET CONTINUE             NET PRINT            NET USE
   NET FILE                 NET SEND             NET USER
   NET GROUP                NET SESSION          NET VIEW

   NET HELP SERVICES lists some of the services you can start.
   NET HELP SYNTAX explains how to read NET HELP syntax lines.
   NET HELP command | MORE displays Help one screen at a time.
```

9.3.2 NET SHARE

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

Share name   Resource                        Remark

-------------------------------------------------------------------------------
IPC$                                         Remote IPC
print$       C:\WINDOWS\system32\spool\drivers
                                             Printer Drivers
ADMIN$       C:\WINDOWS                      Remote Admin
C$           C:\                             Default share
wwwroot$     c:\inetpub\wwwroot              Used for file share access to web
OldCompBackup$
             C:\OldCompBackup
Audits       C:\Audits
Classes      C:\Classes
Classes2     C:\Classes2
NETLOGON     C:\WINDOWS\SYSVOL\sysvol\SCASI.com\SCRIPTS
                                             Logon server share
Public       C:\Public
Shared Documents
             C:\Shared Documents
Software     C:\Software
SYSVOL       C:\WINDOWS\SYSVOL\sysvol        Logon server share
VPHOME       C:\PROGRA~1\SAV                 Symantec AntiVirus
VPLOGON      C:\PROGRA~1\SAV\logon           Symantec AntiVirus
WindowsSecClass
             C:\WindowsSecClass
HPCLJ450     IP_10.42.0.200         Spooled  HPCLJ4500
HPNetwork    USB001                 Spooled  hp deskjet 5100 series
The command completed successfully.
```

9.3.3 NET USE /H

NET USE /H provides instructions on how to use NET USE to use shared network resources.

9.3.4 NET USER

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

User accounts for \\SYSTEMS-SCASI

-------------------------------------------------------------------------------
ACTUser                  Administrator            ASPNET
david.kocot.adm          Dilbert                  IUSR_SERVER2
IUSR_SYSTEMS-SCASI       IWAM_SERVER2             krbtgt
Rodney.Kocot             rodney.kocot.adm         SQLDebugger
SUPPORT_388945a0         uklsajkgdvluflvubdsv     VUSR_SYSTEMS-SCAS
WehateGuests!
The command completed successfully.
```

9.3.5 NET VIEW

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

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

9.3.6 Ipconfig

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

9.3.7 Netstat

```
Netstat Help:

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\rodney.kocot.adm>netstat -h

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-e] [-n] [-o] [-s] [-p proto] [-r] [interval]

  -a            Displays all connections and listening ports.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.
```

```
Netstat Active Connections:

C:\Documents and Settings\rodney.kocot.adm>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    systems-scasi:smtp     systems-scasi.SCASI.com:0  LISTENING
  TCP    systems-scasi:domain   systems-scasi.SCASI.com:0  LISTENING
  TCP    systems-scasi:kerberos  systems-scasi.SCASI.com:0  LISTENING
  TCP    systems-scasi:pop3     systems-scasi.SCASI.com:0  LISTENING
  TCP    systems-scasi:epmap    systems-scasi.SCASI.com:0  LISTENING
  TCP    systems-scasi:ldap     systems-scasi.SCASI.com:0  LISTENING
  TCP    systems-scasi:microsoft-ds  systems-scasi.SCASI.com:0  LISTENING
  TCP    systems-scasi:kpasswd  systems-scasi.SCASI.com:0  LISTENING
  TCP    systems-scasi:593      systems-scasi.SCASI.com:0  LISTENING
  TCP    systems-scasi:ldaps    systems-scasi.SCASI.com:0  LISTENING
….
  TCP    systems-scasi:3268     systems-scasi.SCASI.com:0  LISTENING
  TCP    systems-scasi:3269     systems-scasi.SCASI.com:0  LISTENING
  TCP    systems-scasi:epmap    systems-scasi.SCASI.com:4342  ESTABLISHED
  TCP    systems-scasi:netbios-ssn  systems-scasi.SCASI.com:0  LISTENING
  TCP    systems-scasi:ldap     systems-scasi.SCASI.com:3457  ESTABLISHED
…
  UDP    systems-scasi:4500     *:*
  UDP    systems-scasi:domain   *:*
  UDP    systems-scasi:kerberos  *:*
  UDP    systems-scasi:ntp      *:*
  UDP    systems-scasi:netbios-ns  *:*
  UDP    systems-scasi:netbios-dgm  *:*
  UDP    systems-scasi:389      *:*
  UDP    systems-scasi:kpasswd  *:*
  UDP    systems-scasi:domain   *:*
  UDP    systems-scasi:ntp      *:*
  UDP    systems-scasi:1036     *:*
  UDP    systems-scasi:3456     *:*
```

9.3.8 Nbtstat

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


Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP
 addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refr
esh

  RemoteName   Remote host machine name.
  IP address   Dotted decimal representation of the IP address.
  interval     Redisplays selected statistics, pausing interval seconds
               between each display. Press Ctrl+C to stop redisplaying
               statistics.
```

9.3.9 Ping

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\rodney.kocot.adm>ping yahoo.com

Pinging yahoo.com [66.218.71.198] with 32 bytes of data:

Reply from 66.218.71.198: bytes=32 time=19ms TTL=241
Reply from 66.218.71.198: bytes=32 time=19ms TTL=241
Reply from 66.218.71.198: bytes=32 time=19ms TTL=241
Reply from 66.218.71.198: bytes=32 time=18ms TTL=241

Ping statistics for 66.218.71.198:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 18ms, Maximum = 19ms, Average = 18ms
```

9.3.10 Tracert

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

Tracing route to yahoo.com [66.218.71.198]
over a maximum of 30 hops:

  1    19 ms     9 ms    34 ms  10.234.160.1
  2    10 ms    11 ms    10 ms  bar01-p5-1-0.tjgahe1.ca.attbb.net [24.130.64.45]

  3    16 ms     9 ms    10 ms  bar01-p4-0.lsanhe5.ca.attbb.net [24.130.2.1]
  4    15 ms    12 ms    11 ms  bic02-d6-0.lsanhe3.ca.attbb.net [24.130.64.6]
  5    11 ms    16 ms    22 ms  bic01-p4-0.lsanhe3.ca.attbb.net [24.130.0.62]
  6    10 ms    12 ms    11 ms  12.119.9.5
  7    12 ms    12 ms    13 ms  tbr1-p012802.la2ca.ip.att.net [12.123.199.233]
  8    10 ms    11 ms    14 ms  gbr5-p100.la2ca.ip.att.net [12.122.11.138]
  9    11 ms    10 ms    14 ms  gar3-p360.la2ca.ip.att.net [12.123.28.194]
 10    10 ms    11 ms    16 ms  so-1-0.core2.losangeles1.level3.net [64.152.193.81]
 11    37 ms    11 ms    13 ms  so-5-3-0.bbr1.losangeles1.level3.net [209.247.9.
149]
 12    19 ms    19 ms    19 ms  unknown.level3.net [209.247.9.114]
 13    20 ms    19 ms    21 ms  ge-9-1.ipcolo3.sanjose1.level3.net [64.159.2.73]

 14    20 ms    19 ms    22 ms  unknown.level3.net [64.152.69.30]
 15    19 ms    20 ms    18 ms  w1.rc.vip.scd.yahoo.com [66.218.71.198]

Trace complete.
```

9.3.11 Netsh

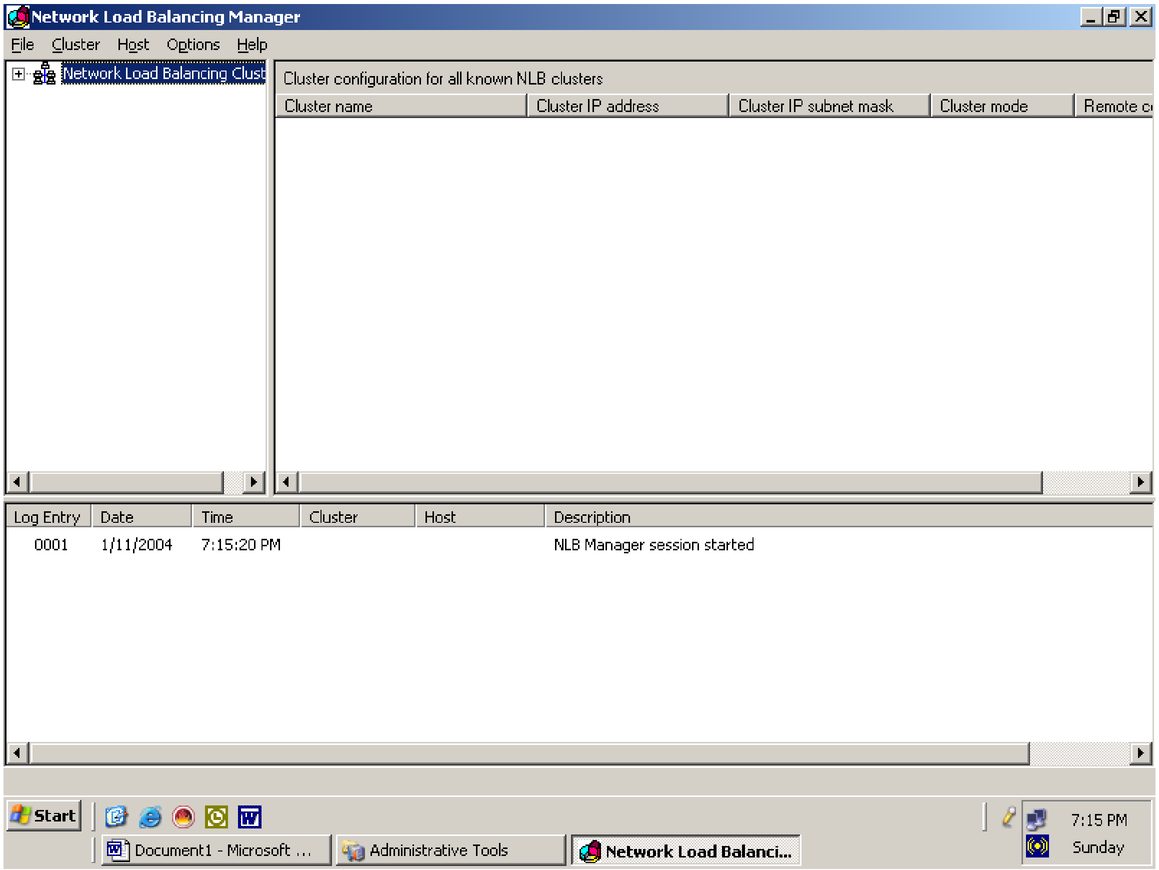
netsh ?
netsh show alias
netsh show helper

9.4 NMAP

```
C:\SDrive\Apps\NMAP>nmap ONTLT01

Starting nmap 3.75 ( http://www.insecure.org/nmap ) at 2007-03-06 17:13 Pacific
Standard Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0

Nmap run completed -- 1 IP address (0 hosts up) scanned in 5.640 seconds

C:\SDrive\Apps\NMAP>

C:\SDrive\Apps\NMAP>nmap 10.42.100.2

Starting nmap 3.75 ( http://www.insecure.org/nmap ) at 2007-03-06 17:17 Pacific
Standard Time
Interesting ports on 10.42.100.2:
(The 1662 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
80/tcp open  http

Nmap run completed -- 1 IP address (1 host up) scanned in 34.250 seconds
```

```
C:\SDrive\Apps\NMAP>

C:\SDrive\Apps\NMAP>nmap
Nmap 3.75 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sV Version scan probes open ports determining service & app names/versions
  -sR RPC scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: 1-1024,1080,6666,31337
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -6 scans via IPv6 rather than IPv4
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
  --win_help Windows-specific features
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES

C:\SDrive\Apps\NMAP>nmap -P0 10.42.11.14

Starting nmap 3.75 ( http://www.insecure.org/nmap ) at 2007-03-06 17:25 Pacific
Standard Time
All 1663 scanned ports on ontqb1.sysconsec.com (10.42.11.14) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 340.396 seconds

C:\SDrive\Apps\NMAP>


C:\SDrive\Apps\NMAP>nmap 10.42.100.2

Starting nmap 3.75 ( http://www.insecure.org/nmap ) at 2007-03-06 17:17 Pacific
Standard Time
Interesting ports on 10.42.100.2:
(The 1662 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
80/tcp open  http

Nmap run completed -- 1 IP address (1 host up) scanned in 34.250 seconds

C:\SDrive\Apps\NMAP>ping ontqb1
Ping request could not find host ontqb1. Please check the name and try again.

C:\SDrive\Apps\NMAP>ping ontqb1

Pinging ontqb1.sysconsec.com [10.42.11.14] with 32 bytes of data:

Reply from 10.42.11.14: bytes=32 time=23ms TTL=127
Reply from 10.42.11.14: bytes=32 time=30ms TTL=127
Reply from 10.42.11.14: bytes=32 time=23ms TTL=127
Reply from 10.42.11.14: bytes=32 time=25ms TTL=127

Ping statistics for 10.42.11.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 30ms, Average = 25ms
```

9.5 Network Load Balancing Manager

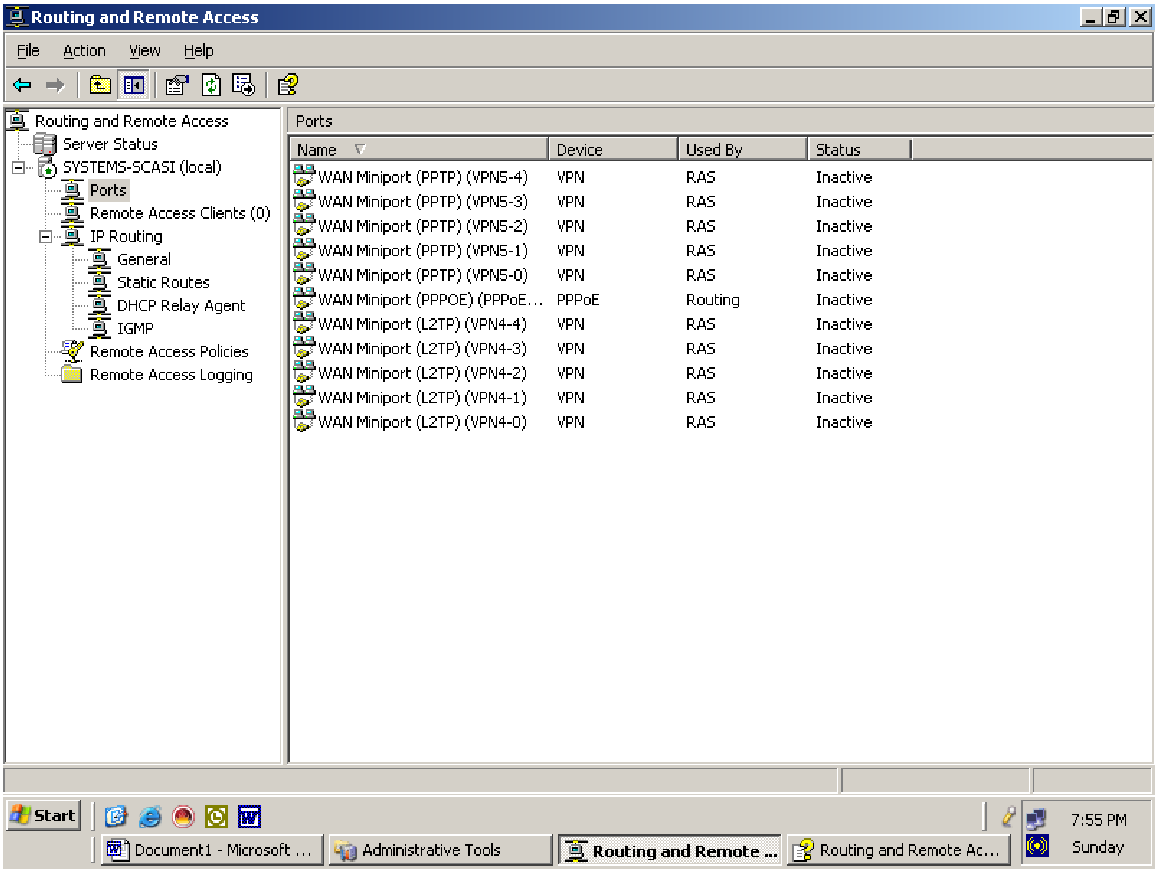


Cluster configuration for all known NLB clusters

Cluster name	Cluster IP address	Cluster IP subnet mask	Cluster mode	Remote c

Log Entry	Date	Time	Cluster	Host	Description
0001	1/11/2004	7:15:20 PM			NLB Manager session started

9.6 Routing and Remote Access



Name	Device	Used By	Status
WAN Miniport (PPTP) (VPN5-4)	VPN	RAS	Inactive
WAN Miniport (PPTP) (VPN5-3)	VPN	RAS	Inactive
WAN Miniport (PPTP) (VPN5-2)	VPN	RAS	Inactive
WAN Miniport (PPTP) (VPN5-1)	VPN	RAS	Inactive
WAN Miniport (PPTP) (VPN5-0)	VPN	RAS	Inactive
WAN Miniport (PPPOE) (PPPoE...	PPPoE	Routing	Inactive
WAN Miniport (L2TP) (VPN4-4)	VPN	RAS	Inactive
WAN Miniport (L2TP) (VPN4-3)	VPN	RAS	Inactive
WAN Miniport (L2TP) (VPN4-2)	VPN	RAS	Inactive
WAN Miniport (L2TP) (VPN4-1)	VPN	RAS	Inactive
WAN Miniport (L2TP) (VPN4-0)	VPN	RAS	Inactive

9.7 Sniffers

9.7.1 Sniffer Data Display

```
 ZSUMMARYDDDelta TDDDFrom Toshiba PortableDDDDDDDDDDDDDDFrom
FCDDDDDDDDDDDDDDDDDD?
 3   747    3.9765  NCP C Login SUPERVISOR                              3
 3   748    0.5511                            NCP R Verification faile 3
 3   749    0.0018  NCP C Check server version                          3
 3   750    0.0021                            NCP R OK               3
 3   751    0.6288  NCP C End of task                                3

@DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
DDDDDDDDDDDDDDDDDDDDDDDDDY

ZDETAILDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
DDDDDDDDDDDDDDDDDDDDDDDD?
 3 NCP:  ----- Login Request -----                              3
 3 NCP:                                                    3
3 NCP:  Request/sub-function code = 23,0                            3
3 NCP:                                                     3
3 NCP:  Name = "SUPERVISOR"                                         3
@DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDFrame 747 of
2046DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDY
ZHEXDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
DDDDDDDDDDDDDDDDASCIIDDDD?
3 0000  F5 FC 00 44 FA 00 E7 05  FF FF 00 3C 00 11 00 00  ...D.......<....     3
3 0010  00 01 00 00 00 00 00 FC  04 51 00 00 00 01 00 00  .........Q......     3
3 0020  00 00 00 F5 40 03 22 22  43 07 01 00 17 00 15 00  ....@.""C.......     3
3 0030  0A 53 55 50 45 52 56 49  53 4F 52 08 54 45 53 54  .SUPERVISOR.TEST     3
3 0040  50 41 53 53                               PASS                3
@DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDFrame 747 of
2046DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDY


                    Use TAB to select windows
1       2 Set          4 Zoom  5       6Disply 7 Prev  8 Next          10 New
  Help    mark           in     Menus   options  frame   frame            capture
```

9.7.2 Sniffer Packet Dump:

```
- - - - - - - - - - - - - - - - Frame 747 - - - - - - - - - - - - - - - - -
SUMMARY  Delta T    From Toshiba Portable              From FC
   747    3.9765  DLC Syscode=FA, size=68 bytes
                  NCP Frag F=00 (Complete), Seq=1511
                  XNS NetWare Request N=67 C=7 T=1
                  NCP C Login SUPERVISOR

DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 747 arrived at  12:05:43.0682 ; frame size is 68 (0044 hex) bytes.
DLC:  Destination: Station FC
DLC:  Source     : Station F5, Toshiba Portable
DLC:  ARCNET system code = FA
DLC:
FRAG: ----- NCP ARCNET fragmentation header -----
FRAG:
FRAG: Split flags = 00 (Complete)
FRAG: Sequence number = 1511
FRAG:
XNS:  ----- XNS Header -----
XNS:
XNS:  Checksum = FFFF
XNS:  Length = 60
XNS:  Transport control = 00
XNS:          0000 .... = Reserved
XNS:          .... 0000 = Hop count
XNS:  Packet type = 17 (Novell NetWare)
XNS:
XNS:  Dest   net = 00000001, host = 0000000000FC, socket = 1105 (NetWare Server)
XNS:  Source net = 00000001, host = 0000000000F5, socket = 16387 (4003)
XNS:
XNS:  ----- Novell Advanced NetWare -----
XNS:
XNS:  Request type = 2222 (Request)
XNS:  Seq no=67   Connection no=7    Task no=1
XNS:
NCP:  ----- Login Request -----
NCP:
NCP:  Request/sub-function code = 23,0
NCP:
NCP:  Name = "SUPERVISOR"
NCP:  Password = "TESTPASS"
NCP:
NCP:  [Normal end of NetWare "Login Request" packet.]
NCP:
```

```
ADDR  HEX                                        ASCII
0000  F5 FC 00 44 FA 00 E7 05  FF FF 00 3C 00 11 00 00  ...D.......<....
0010  00 01 00 00 00 00 00 FC  04 51 00 00 00 01 00 00  .........Q......
0020  00 00 00 F5 40 03 22 22  43 07 01 00 17 00 15 00  ....@.""C.......
0030  0A 53 55 50 45 52 56 49  53 4F 52 08 54 45 53 54  .SUPERVISOR.TEST
0040  50 41 53 53                                      PASS
```

9.8 FTP

The File Transfet Protocol is used extensively by business to transfer files between systems. Because packets are so easily sniffed it is wise to use a secure FTP protocol. FileZilla is a free secure FTP solution. Filezilla can be found at http://filezilla-project.org/.

9.9 Dialup

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.

9.10 Wireless

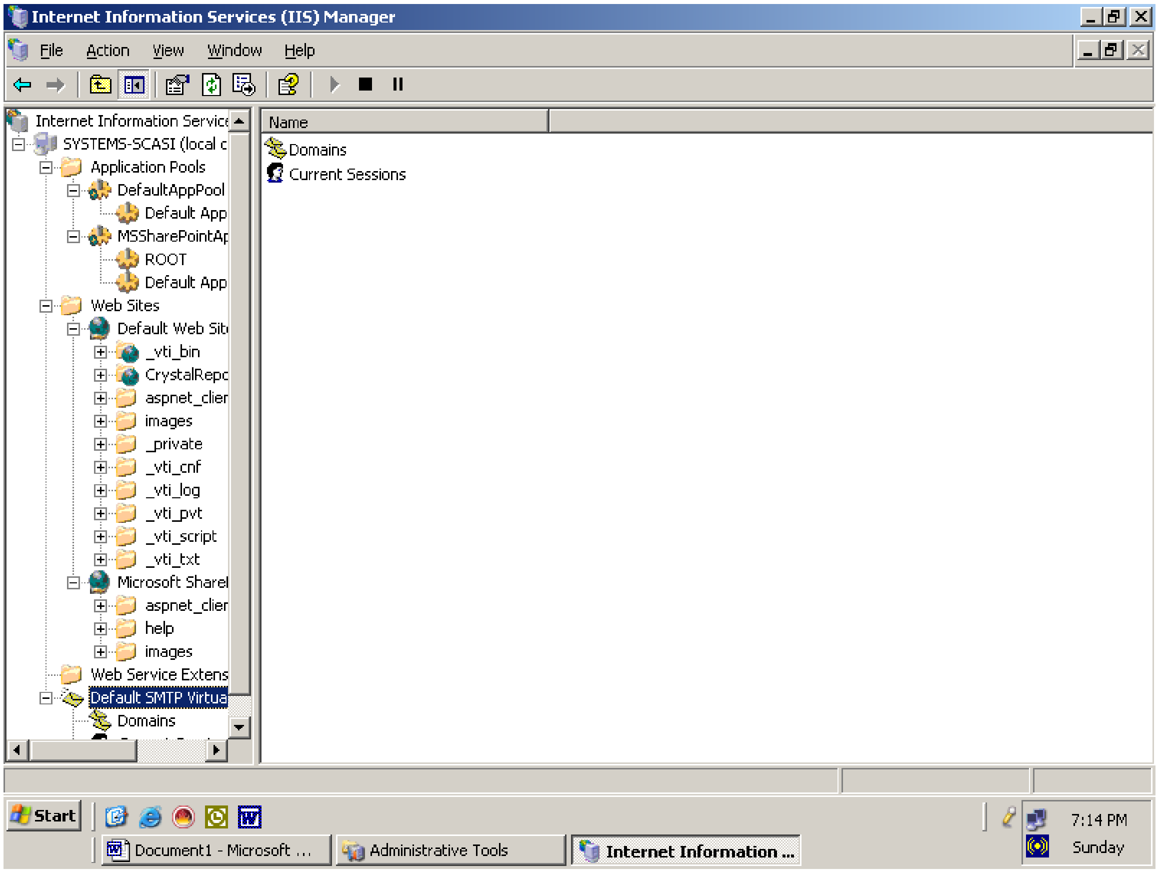
New wireless standards are evolving into more secure protocols. If wireless is in use review the configuration for appropriate implementation.

Search the internet for the current level of security and vulnerabilities for the wireless protocols in use. Many system managers believe that WPA and WPA2 are secure, yet, a Russian company, Elcomsoft sells a product called Elcomsoft Distributed Password Recovery that breaks WPA and WPA2 security.

An unsecured wireless network can be easily implemented by any user. Periodically, monitor for unauthorized wireless networks.

Can any wireless network be secure?

9.11 Internet Information Services Manager



9.12 Network Security Audit Program

- Obtain a copy of the network policies, standards and procedures.
- 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, standards and procedures
- War dial
- Check for unauthorized wireless end points
- Scan systems for unauthorized and inappropriate ports.
- Verify that the standards are appropriate and complied with.

10 Logging and Monitoring

Windows 2000 and 2003 Both have a detailed logging and monitoring system that allows domain administrators and auditors to track everything from unsuccessful logon attempts to free disk space. All of them can be configured to track or ignore whatever events or statistics you please.

Far and away the event log we should be most concerned with is the security log. Other logs include the System, Application, DNS Server, Directory Service, and File Replication Service logs.

Be forewarned, however, that the more detail you request in your event logs, the faster they will consume disk space; in one week, our three computer two user domain logged almost 50,000 security events, consuming seventeen megabytes

10.1 Reviewing Logs

10.1.1 EventQuery.vbs

EventQuery.vbs can be downloaded from the Microsoft web site. The eventquery script can be used to dump the event logs from local and remote systems:

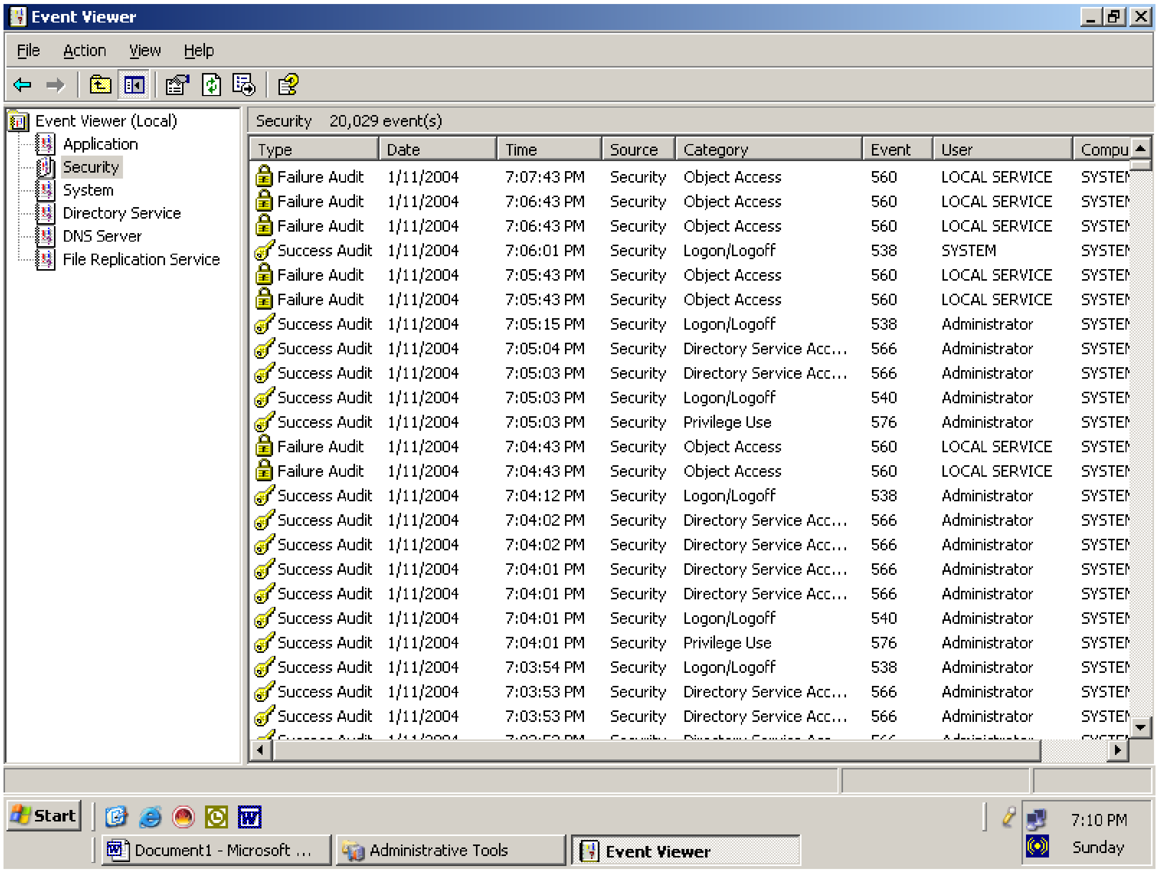
```
C:\> cscript c:\windows\system32\eventquery.vbs
```

10.1.2 Log Parser

A Microsoft utility that can be used to query logs and data sources in the Microsoft Windows environment.

10.1.3 Event Viewer – Security Log

Event Viewer- Security Log

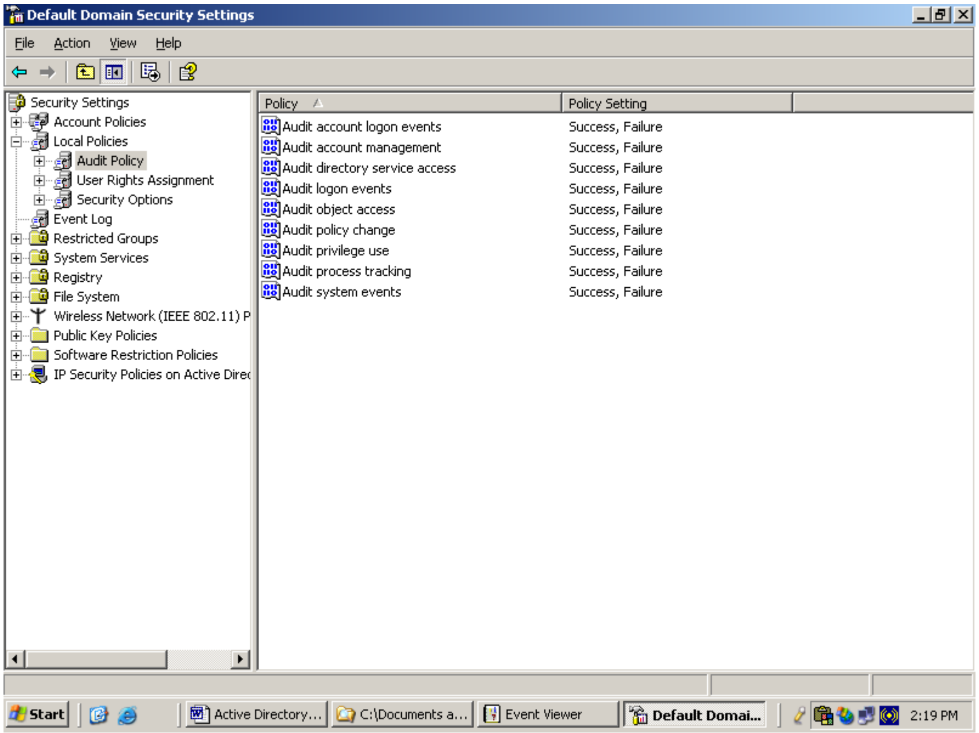


Security 20,029 event(s)

Type	Date	Time	Source	Category	Event	User	Compu
Failure Audit	1/11/2004	7:07:43 PM	Security	Object Access	560	LOCAL SERVICE	SYSTEM
Failure Audit	1/11/2004	7:06:43 PM	Security	Object Access	560	LOCAL SERVICE	SYSTEM
Failure Audit	1/11/2004	7:06:43 PM	Security	Object Access	560	LOCAL SERVICE	SYSTEM
Success Audit	1/11/2004	7:06:01 PM	Security	Logon/Logoff	538	SYSTEM	SYSTEM
Failure Audit	1/11/2004	7:05:43 PM	Security	Object Access	560	LOCAL SERVICE	SYSTEM
Failure Audit	1/11/2004	7:05:43 PM	Security	Object Access	560	LOCAL SERVICE	SYSTEM
Success Audit	1/11/2004	7:05:15 PM	Security	Logon/Logoff	538	Administrator	SYSTEM
Success Audit	1/11/2004	7:05:04 PM	Security	Directory Service Acc...	566	Administrator	SYSTEM
Success Audit	1/11/2004	7:05:03 PM	Security	Directory Service Acc...	566	Administrator	SYSTEM
Success Audit	1/11/2004	7:05:03 PM	Security	Logon/Logoff	540	Administrator	SYSTEM
Success Audit	1/11/2004	7:05:03 PM	Security	Privilege Use	576	Administrator	SYSTEM
Failure Audit	1/11/2004	7:04:43 PM	Security	Object Access	560	LOCAL SERVICE	SYSTEM
Failure Audit	1/11/2004	7:04:43 PM	Security	Object Access	560	LOCAL SERVICE	SYSTEM
Success Audit	1/11/2004	7:04:12 PM	Security	Logon/Logoff	538	Administrator	SYSTEM
Success Audit	1/11/2004	7:04:02 PM	Security	Directory Service Acc...	566	Administrator	SYSTEM
Success Audit	1/11/2004	7:04:02 PM	Security	Directory Service Acc...	566	Administrator	SYSTEM
Success Audit	1/11/2004	7:04:01 PM	Security	Directory Service Acc...	566	Administrator	SYSTEM
Success Audit	1/11/2004	7:04:01 PM	Security	Directory Service Acc...	566	Administrator	SYSTEM
Success Audit	1/11/2004	7:04:01 PM	Security	Logon/Logoff	540	Administrator	SYSTEM
Success Audit	1/11/2004	7:04:01 PM	Security	Privilege Use	576	Administrator	SYSTEM
Success Audit	1/11/2004	7:03:54 PM	Security	Logon/Logoff	538	Administrator	SYSTEM
Success Audit	1/11/2004	7:03:53 PM	Security	Directory Service Acc...	566	Administrator	SYSTEM
Success Audit	1/11/2004	7:03:53 PM	Security	Directory Service Acc...	566	Administrator	SYSTEM
Success Audit	1/11/2004	7:03:53 PM	Security	Directory Service Acc...	566	Administrator	SYSTEM

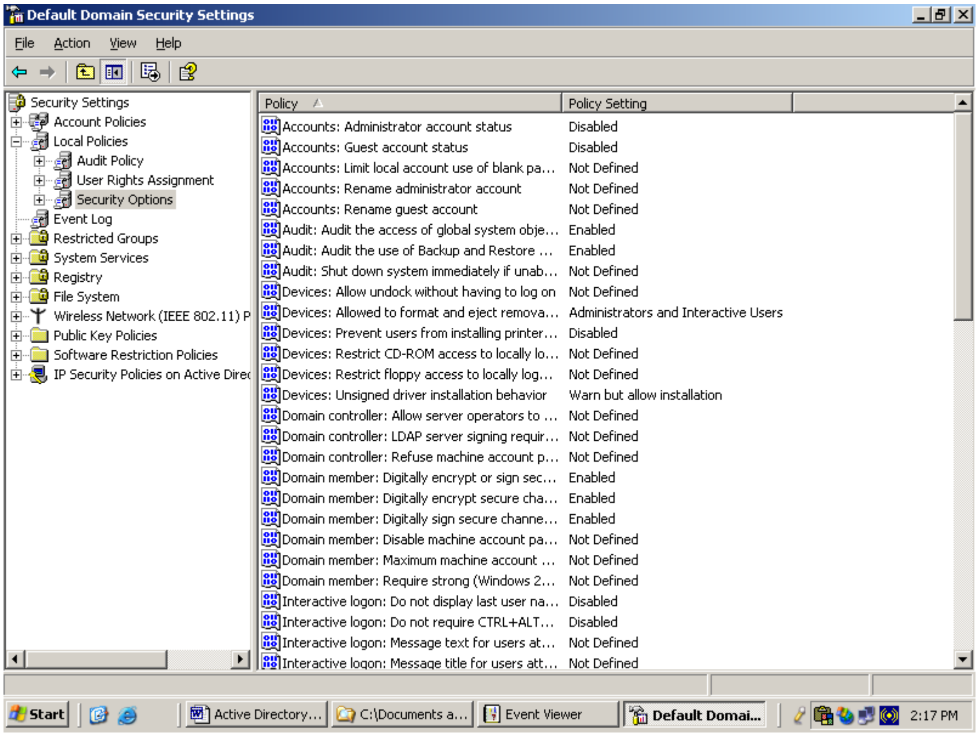
10.1.4 Security Log Settings

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

Security Options



Policy	Policy Setting
Accounts: Administrator account status	Disabled
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank pa...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system obje...	Enabled
Audit: Audit the use of Backup and Restore ...	Enabled
Audit: Shut down system immediately if unab...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject remova...	Administrators and Interactive Users
Devices: Prevent users from installing printer...	Disabled
Devices: Restrict CD-ROM access to locally lo...	Not Defined
Devices: Restrict floppy access to locally log...	Not Defined
Devices: Unsigned driver installation behavior	Warn but allow installation
Domain controller: Allow server operators to ...	Not Defined
Domain controller: LDAP server signing requir...	Not Defined
Domain controller: Refuse machine account p...	Not Defined
Domain member: Digitally encrypt or sign sec...	Enabled
Domain member: Digitally encrypt secure cha...	Enabled
Domain member: Digitally sign secure channe...	Enabled
Domain member: Disable machine account pa...	Not Defined
Domain member: Maximum machine account ...	Not Defined
Domain member: Require strong (Windows 2...	Not Defined
Interactive logon: Do not display last user na...	Disabled
Interactive logon: Do not require CTRL+ALT...	Disabled
Interactive logon: Message text for users at...	Not Defined
Interactive logon: Message title for users att...	Not Defined

10.2 Baseline Security Analyzer

10.2.1 Baseline Security Analyzer Help

```
C:\Program Files\Microsoft Baseline Security Analyzer 2>mbsacli /?
Microsoft Baseline Security Analyzer
Version 2.0.1 (2.0.6706.0)
(C) Copyright 2002-2006 Microsoft Corporation. All rights reserved.

MBSACLI [/target | /r | /d domain] [/n option] [/o file] [/qp] [/qe] [/qr]
        [/qt] [/listfile file] [/xmlout] [/wa | /wi] [/catalog file] [/nvc]
        [/nai] [/nm] [/nd] [/?]

MBSACLI [/l] [/ls] [/lr file] [/ld file] [/unicode] [/nvc] [/?]

Description:
        This is a command line interface for Microsoft Baseline Security
        Analyzer

Parameter List:
        /target         domain\computer Scan named computer.

        /target         IP              Scan named IP address.

        /r              IP-IP           Scan named IP addresses range.

        /listfile       file            Scan named IP address or computer
                                        listed in the specified file.

        /d              domain          Scan named domain.

        /n              option          Select which scans to NOT perform.
                                        All checks are performed by default.
                                        Valid values:
                                        "OS", "SQL", "IIS", "Updates",
                                        "Password",
                                        Can be concatenated with "+" (no
                                        spaces).

        /wa                             Show only updates approved on the
                                        Update Services server.

        /wi                             Show all updates even if not approved
                                        on the Update Services server.

        /nvc                            Do not check for a new version of MBSA.

        /o              filename        Output XML file name template.
                                        Default: %D% - %C% (%T%).

        /qp                             Don't display scan progress.

        /qt                             Don't display the report by default
                                        following a single-computer scan.

        /qe                             Don't display error list.

        /qr                             Don't display report list.

        /q                              Do not display any of the preceding
                                        items.

        /unicode                        Output Unicode.

        /u              username        Scan using the specified username.

        /p              password        Scan using the specified password.
        /catalog        filename        Specifies the data source that contains
                                        the available security update
                                        information.

        /nai                            Do not update the prerequisite Windows
                                        Update Agent components during a scan.

        /nm                             Do not configure computers to use the
                                        Microsoft Update site for scanning.

        /nd                             Do not download any files from the
                                        Microsoft Web site when scanning.

        /xmlout                         Run in updates only mode using only
                                        mbsacli.exe and wusscan.dll. Only these
                                        switches can be used with this option:
                                        /catalog, /wa, /wi, /nvc, /unicode

        /l                              List all reports available.

        /ls                             List reports from the latest scan.

        /lr             filename        Display overview report.

        /ld             filename        Display detailed report.

        /?                              Display this help/usage.

Executing MBSACLI with no parameters scans the local computer for all checks
and displays the report in text-mode.

Examples:
    MBSACLI
    MBSACLI /n Password+IIS+OS+SQL
    MBSACLI /d MyDomain
    MBSACLI /target 200.0.0.1
    MBSACLI /r 200.0.0.1-200.0.0.50
    MBSACLI /listfile export.txt
    MBSACLI /ld "Domain - Computer (03-01-2002 12-00 AM)"
    MBSACLI >c:\results.txt
    MBSACLI /catalog c:\wsusscn2.cab /nai /nvc
    MBSACLI /wa
    MBSACLI /xmlout /catalog c:\temp\wsusscn2.cab /unicode >results.xml
```

10.2.2 Baseline Security Analyzer Output

```
C:\Program Files\Microsoft Baseline Security Analyzer 2> MBSACLI

Computer name: SYSCONSEC\ONTLT01
IP address: 10.42.100.2
Security report name: SYSCONSEC - ONTLT01 (3-6-2007 3-53 PM)
Scan date: 3/6/2007 3:53 PM
Scanned with MBSA version: 2.0.6706.0
Security update catalog: Microsoft Update
Catalog synchronization date:
Security assessment: Severe Risk

  Security Updates Scan Results

          Issue:  Office Security Updates
          Score:  Check failed (critical)
          Result: 9 security updates are missing.

               Security Updates

                       | MS06-039 | Missing | Security Update for Office 2003 (KB914455) | Moderate |
                       | MS06-054 | Missing | Security Update for Publisher 2003 (KB894542) | Important |
                       | MS06-058 | Missing | Security Update for PowerPoint 2003 (KB923091) | Important |
                       | MS06-061 | Missing | Security Update for Office 2003 (KB924424) | Critical |
                       | MS07-002 | Missing | Security Update for Excel 2003 (KB925257) | Important |
                       | MS07-003 | Missing | Security Update for Outlook 2003 (KB924085) | Important |
                       | MS07-013 | Missing | Security Update for Office 2003 (KB920813) | Important |
                       | MS07-015 | Missing | Security Update for Office 2003 (KB929064) | Important |
                       | MS07-014 | Missing | Security Update for Word 2003 (KB929057) | Important |

               Current Update Compliance

                       | 902848 | Installed | Outlook Live 2003 Service Pack 2 |  |
                       | 887622 | Installed | Visio 2003 Service Pack 2 |  |
                       | 887619 | Installed | OneNote 2003 Service Pack 2 |  |
                       | 887620 | Installed | Project 2003 Service Pack 2 |  |
                       | 887618 | Installed | Office 2003 Service Pack 2 for Proofing Tools |  |
                       | 887616 | Installed | Office 2003 Service Pack 2 |  |
                       | MS06-012 | Installed | Security Update for Excel 2003 (KB905756) | Critical |
                       | 920115 | Installed | Service Pack 3 for Business Contact Manager Update and Small
Business Accounting |  |

          Issue:  SQL Server Security Updates
          Score:  Check passed
          Result: No security updates are missing.

               Current Update Compliance

                       | MS06-061 | Installed | MSXML 4.0 SP2 Security Update (925672) | Critical |

          Issue:  Windows Security Updates
          Score:  Check failed (critical)
          Result: 13 security updates are missing. 3 service packs or update rollups are missing.

               Security Updates

                       | MS06-075 | Missing | Security Update for Windows XP (KB926255) | Important |
                       | MS06-076 | Missing | Cumulative Security Update for Outlook Express for Windows XP
(KB923694) | Important |
                       | MS06-078 | Missing | Security Update for Windows Media Player 6.4 (KB925398) | Critical |
                       | MS06-078 | Missing | Security Update for Windows XP (KB923689) | Critical |
                       | MS07-004 | Missing | Security Update for Windows XP (KB929969) | Critical |
                       | MS07-006 | Missing | Security Update for Windows XP (KB928255) | Important |
                       | MS07-008 | Missing | Security Update for Windows XP (KB928843) | Critical |
                       | MS07-007 | Missing | Security Update for Windows XP (KB927802) | Important |
                       | MS07-012 | Missing | Security Update for Windows XP (KB924667) | Important |
                       | MS07-009 | Missing | Security Update for Windows XP (KB927779) | Critical |
                       | MS07-013 | Missing | Security Update for Windows XP (KB918118) | Important |
                       | MS07-011 | Missing | Security Update for Windows XP (KB926436) | Important |
                       | MS07-016 | Missing | Cumulative Security Update for Internet Explorer 6 for Windows XP
(KB928090) | Critical |

               Update Rollups and Service Packs

                       | 931836 | Missing | Update for Windows XP (KB931836) |  |
                       | 890830 | Missing | Windows Malicious Software Removal Tool - February 2007 (KB890830) |
|
                       | 926874 | Missing | Windows Internet Explorer 7.0 for Windows XP |  |

               Current Update Compliance

                       | MS04-044 | Installed | Security Update for Windows XP (KB885835) | Important |
                       | MS05-033 | Installed | Security Update for Windows XP (KB896428) | Moderate |
                       | MS05-036 | Installed | Security Update for Windows XP (KB901214) | Critical |
                       | MS05-018 | Installed | Security Update for Windows XP (KB890859) | Important |
                       | MS05-026 | Installed | Security Update for Windows XP (KB896358) | Critical |
                       | MS05-040 | Installed | Security Update for Windows XP (KB893756) | Important |
                       | MS05-041 | Installed | Beta 6.2 Installer version Security Update for Windows XP
(KB899591) | Important |
                       | MS05-041 | Installed | Security Update for Windows XP (KB899591) | Moderate |
                       | MS05-042 | Installed | Security Update for Windows XP (KB899587) | Moderate |
                       | MS05-043 | Installed | Security Update for Windows XP (KB896423) | Critical |
                       | MS05-051 | Installed | Security Update for Windows XP (KB902400) | Important |
                       | MS05-048 | Installed | Security Update for Windows XP (KB901017) | Important |
                       | MS05-045 | Installed | Security Update for Windows XP (KB905414) | Moderate |
                       | MS05-047 | Installed | Security Update for Windows XP (KB905749) | Important |
                       | MS05-049 | Installed | Security Update for Windows XP (KB900725) | Important |
                       | MS05-053 | Installed | Security Update for Windows XP (KB896424) | Critical |
                       | MS05-050 | Installed | Security Update for Windows XP (KB904706) | Critical |
                       | MS06-002 | Installed | Security Update for Windows XP (KB908519) | Critical |
                       | MS06-001 | Installed | Security Update for Windows XP (KB912919) | Critical |
                       | MS06-008 | Installed | Security Update for Windows XP (KB911927) | Important |
                       | MS06-009 | Installed | Security Update for Windows XP (KB901190) | Important |
                       | MS06-006 | Installed | Security Update for Windows Media Player Plug-in (KB911564) |
Important |
                       | MS06-016 | Installed | Cumulative Security Update for Outlook Express for Windows XP
(KB911567) | Important |
                       | MS06-014 | Installed | Security Update for Windows XP (KB911562) | Critical |
                       | MS06-015 | Installed | Security Update for Windows XP (KB908531) | Critical |
                       | MS06-024 | Installed | Security Update for Windows Media Player 9 (KB917734) | Critical |
                       | MS06-030 | Installed | Security Update for Windows XP (KB914389) | Important |
                       | MS06-023 | Installed | Security Update for Windows XP (KB917344) | Critical |
                       | MS06-022 | Installed | Security Update for Windows XP (KB918439) | Critical |
                       | MS06-018 | Installed | Security Update for Windows XP (KB913580) | Low |
                       | MS06-032 | Installed | Security Update for Windows XP (KB917953) | Important |
                       | MS06-025 | Installed | Security Update for Windows XP (KB911280) | Important |
                       | MS06-036 | Installed | Security Update for Windows XP (KB914388) | Critical |
                       | MS06-051 | Installed | Security Update for Windows XP (KB917422) | Critical |
                       | MS06-050 | Installed | Security Update for Windows XP (KB920670) | Important |
                       | MS06-041 | Installed | Security Update for Windows XP (KB920683) | Critical |
                       | MS06-045 | Installed | Security Update for Windows XP (KB921398) | Moderate |
                       | MS06-046 | Installed | Security Update for Windows XP (KB922616) | Critical |
                       | MS06-043 | Installed | Security Update for Outlook Express for Windows XP (KB920214) |
Critical |
                       | MS06-052 | Installed | Security Update for Windows XP (KB919007) | Important |
                       | MS06-053 | Installed | Security Update for Windows XP (KB920685) | Moderate |
                       | MS06-055 | Installed | Security Update for Windows XP (KB925486) | Critical |
                       | MS06-063 | Installed | Security Update for Windows XP (KB923414) | Important |
                       | MS06-065 | Installed | Security Update for Windows XP (KB924496) | Moderate |
                       | MS06-057 | Installed | Security Update for Windows XP (KB923191) | Critical |
                       | MS06-061 | Installed | Security Update for Windows XP (KB924191) | Critical |
                       | MS06-064 | Installed | Security Update for Windows XP (KB922819) | Low |
                       | MS06-068 | Installed | Security Update for Windows XP (KB920213) | Critical |
                       | MS06-070 | Installed | Security Update for Windows XP (KB924270) | Low |
                       | MS06-071 | Installed | MSXML 4.0 SP2 Security Update (KB927978) | Critical |
                       | 890830 | Installed | Windows Malicious Software Removal Tool - November 2006 (KB890830) |
|
                       | MS06-067 | Installed | Cumulative Security Update for Internet Explorer for Windows XP
(KB922760) | Critical |
                       | MS06-069 | Installed | Security Update for Flash Player (KB923789) | Critical |
                       | MS06-066 | Installed | Security Update for Windows XP (KB923980) | Important |


  Operating System Scan Results

    Administrative Vulnerabilities

          Issue:  Local Account Password Test
          Score:  Check passed
          Result: Some user accounts (1 of 4) have blank or simple passwords, or could not be analyzed.

                 Detail:
                       | User | Weak Password | Locked Out | Disabled |
                       | Guest | Weak | - | Disabled |
                       | HelpAssistant | - | - | Disabled |
                       | SUPPORT_388945a0 | - | - | Disabled |
                       | zadmin | - | - | - |
          Issue:  File System
          Score:  Check passed
          Result: All hard drives (1) are using the NTFS file system.

                 Detail:
                       | Drive Letter | File System |
                       | C: | NTFS |
          Issue:  Password Expiration
          Score:  Check failed (non-critical)
          Result: Some user accounts (2 of 4) have non-expiring passwords.

                 Detail:
                      | User |
                      | Guest |
                      | zadmin |
                      | HelpAssistant |
                      | SUPPORT_388945a0 |
          Issue:  Guest Account
          Score:  Check passed
          Result: The Guest account is disabled on this computer.

          Issue:  Autologon
          Score:  Check passed
          Result: Autologon is not configured on this computer.

          Issue:  Restrict Anonymous
          Score:  Check passed
          Result: Computer is properly restricting anonymous access.

          Issue:  Administrators
          Score:  Check failed (non-critical)
          Result: More than 2 Administrators were found on this computer.

                 Detail:
                      | User |
                      | SYSCONSEC\rodney.adm |
                      | SYSCONSEC\zadmin |
                      | zadmin |
          Issue:  Windows Firewall
          Score:  Best practice
          Result: Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all
network connections.

                 Detail:
                      | Connection Name | Firewall | Exceptions |
                      | All Connections | On | Programs |
                      | Local Area Connection | On | Programs* |
                      | Local Area Connection 2 | On | Programs* |
                      | Sprint PCS Vision - Novatel Wireless | On | Programs* |
                      | Wireless Network Connection | On | Programs* |
          Issue:  Automatic Updates
          Score:  Best practice
          Result: Automatic Updates are managed through Group Policy on this computer.

          Issue:  Incomplete Updates
          Score:  Best practice
          Result: No incomplete software update installations were found.

       Additional System Information

          Issue:  Windows Version
          Score:  Best practice
          Result: Computer is running Windows 2000 or greater.

          Issue:  Auditing
          Score:  Best practice
          Result: Logon Success and Logon Failure auditing are both enabled.

          Issue:  Shares
          Score:  Best practice
          Result: 2 share(s) are present on your computer.

                 Detail:
                      | Share | Directory | Share ACL | Directory ACL |
                      | ADMIN$ | C:\WINDOWS | Admin Share | BUILTIN\Users -  RX, BUILTIN\Power Users -  RWXD,
BUILTIN\Administrators -  F, NT AUTHORITY\SYSTEM -  F |
                      | C$ | C:\ | Admin Share | BUILTIN\Administrators -  F, NT AUTHORITY\SYSTEM -  F,
BUILTIN\Users -  RX, Everyone -  RX |
          Issue:  Services
          Score:  Best practice
```

```
         Result: Some potentially unnecessary services are installed.

               Detail:
                     | Service | State |
                     | Telnet | Stopped |

Internet Information Services (IIS) Scan Results
      IIS is not running on this computer.

SQL Server Scan Results
      SQL Server and/or MSDE is not installed on this computer.

Desktop Application Scan Results

      Administrative Vulnerabilities

         Issue:  IE Zones
         Score:  Check passed
         Result: Internet Explorer zones have secure settings for all users.

         Issue:  Macro Security
         Score:  Check passed
         Result: 4 Microsoft Office product(s) are installed. No issues were found.

               Detail:
                     | Issue | User | Advice |
                     | Microsoft Office Excel 2003 | All Users | No security issues were found. |
                     | Microsoft Office Outlook 2003 | All Users | No security issues were found. |
                     | Microsoft Office PowerPoint 2003 | All Users | No security issues were found. |
                     | Microsoft Office Word 2003 | All Users | No security issues were found. |
```

10.3 File Integrity Monitoring

A comparison of host/file security monitors can be found at: http://la-samhna.de/library/scanners.html.

10.4 Open Source Host Based Intrusion Detection System (OSSEC)

http://www.ossec.net/wiki/index.php/OSSEC

10.5 Free PC Audits

http://www.belarc.com/free_download.html?/try/ib.CIS.cgi provides a free program to profile and review the software on a PC.

There are many web sites that provide valuable services – and a few web sites that are not trustworthy.

10.6 Logging and Monitoring Audit Procedures

- Determine whether Logging and Monitoring policies, standards and procedures are formalized, appropriate and implemented.
- Verify that all systems are logging activity and all logs are reviewed.
- Verify that a log server is used and that it is protected.
- Verify that file integrity software is used to monitor unauthorized modifications to operating systems, databases and application components.
- Review procedures for follow-up and resolution of events.
- Review procedures for the unthinkable.

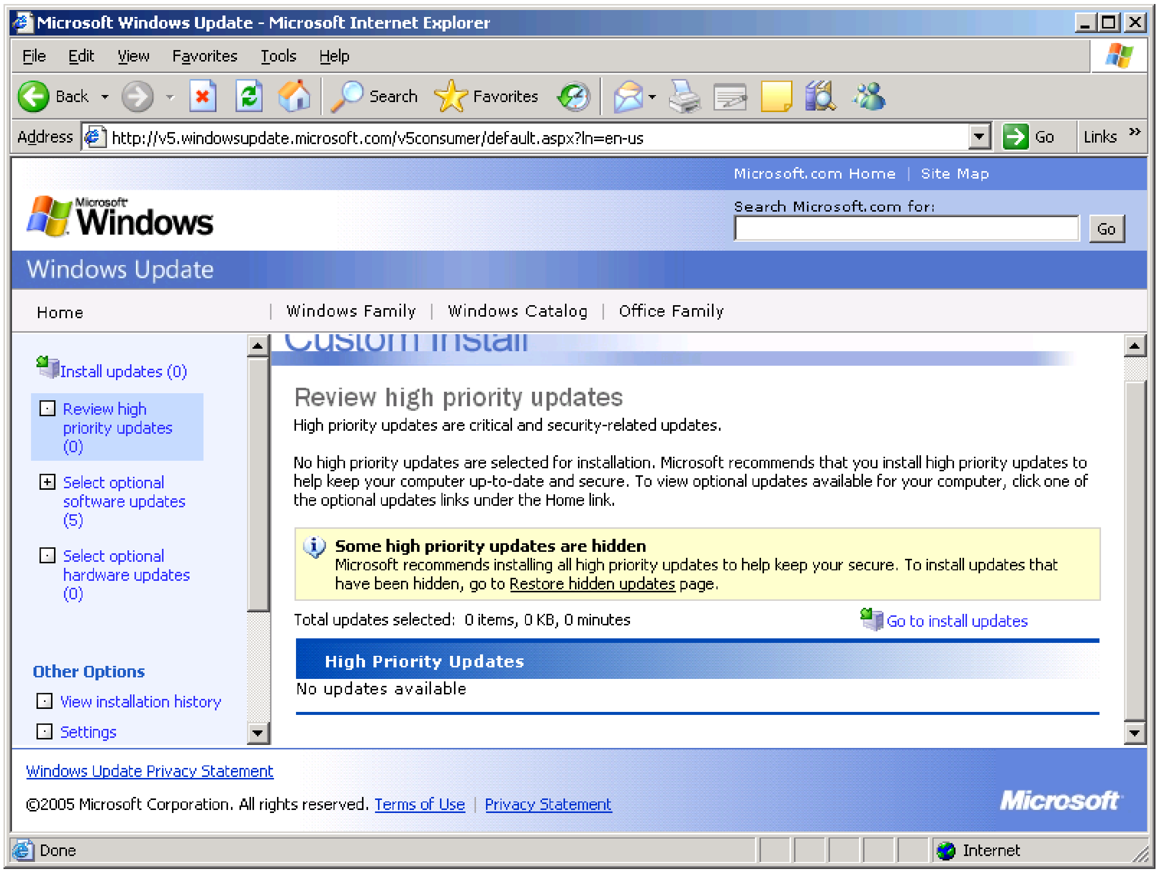
11 Backup and Contingency Planning

11.1 Backup and Contingency Planning Audit Program

- Obtain backup and COP plans and procedures for each component in the LAN 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 LAN environment are implemented
- Select a sample of programs and data from each component in the LAN 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

12 Patch Management

Worms like MSBlaster and Sasser do tens of millions of dollars in damage when they are released. Sadly, the damage is entirely preventable by simply running Microsoft's free Windows Update utility. Every month, Microsoft releases a security bulletin that publicizes security vulnerabilities in Windows and the fact that patches for these vulnerabilities are now available.


Microsoft Windows Update - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links
Microsoft.com Home | Site Map
Microsoft Windows
Search Microsoft.com for:
Go
Windows Update
Home | Windows Family | Windows Catalog | Office Family
Custom Install
Install updates (0)
Review high priority updates (0)
Select optional software updates (5)
Select optional hardware updates (0)
Other Options
View installation history
Settings
Go to install updates
Microsoft
Done
Internet

Address: http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx?ln=en-us

Review high priority updates

High priority updates are critical and security-related updates.

No high priority updates are selected for installation. Microsoft recommends that you install high priority updates to help keep your computer up-to-date and secure. To view optional updates available for your computer, click one of the optional updates links under the Home link.

Some high priority updates are hidden
Microsoft recommends installing all high priority updates to help keep your secure. To install updates that have been hidden, go to Restore hidden updates page.

Total updates selected: 0 items, 0 KB, 0 minutes

High Priority Updates
No updates available

Windows Update Privacy Statement

©2005 Microsoft Corporation. All rights reserved. Terms of Use | Privacy Statement

Figure: Windows Update

There are a variety of methods available to make sure that all the Windows machines on a given network are up to date on patches. One is to pay homeless people off the street minimum wage to come in after hours and run Windows Update on every single computer in the office individually. While I have seen one large company (which shall remain nameless) do this, most take the wiser course and use an automated patch management system.

12.1 Patch Management Systems

The cheapest of these is Microsoft's Software Update Service (SUS), which is free and very easy to administer, but lacks the flexibility of some of the tools which cost money. Other, more expensive patch management systems include Microsoft's Software Management Service (SMS), HFNetchekPro by Shavlik Technologies (shavlik.com), and Bigfix (bigfix.com).

Unfortunately, simply deploying a patch management service isn't enough. Often, for one reason or another, many computers don't get update patches as they would in a perfect world. These unpatched hosts must be tracked down. Many commercial patch management systems include a patch verification system. Microsoft offers a free tool for this process, the Microsoft Baseline Security Analyzer (MBSA, available at http://www.microsoft.com/technet/security/tools/mbsahome.mspx).

12.2 Don't Forget Application Patches!

In addition to Windows, applications also have security vulnerabilities. For instance, several months ago, Microsoft reported a vulnerability in the way the Microsoft Office suite rendered .jpeg images, which required a patch.

12.3 Patcher Beware

Be forewarned, however, that patches have been known to break things. Many large organizations have been extremely reluctant to deploy Windows XP Service Pack 2, for instance, since it has been known in some cases to turn $800 computers into worthless hunks of plastic; many of the security enhancements (including activating XP's integrated software firewall) that are incorporated with Service Pack 2 make computers so secure that many networked applications stop running until one setting or another is tweaked. While this can be a serious headache, with enough testing (read: 'overtime'), the problem can usually be overcome.

A full rundown of Microsoft's patch management systems and recommendations is available here: http://www.microsoft.com/technet/security/topics/patch/default.mspx

12.4 Patch Management Audit Program

Determine that policies, standards and procedures for Patch Management are formalized, appropriate and implemented.

13 Miscellaneous Tools

13.1 Active Directory Scripting

Create a file with a VBS extension that contains the VBScript commands you want executed. At the command prompt use cscript to execute the VBScript file.

```
Option Explicit
Dim dom
Dim ou
Dim user
Dim concat
Dim obj
Dim UserObj

Function FindAndBind()
   Dim myobj
   Set myObj = GetObject("LDAP://rootDSE")
   FindAndBind=myObj.get("defaultNamingContext")
End Function

FindAndBind
Dom = FindAndBind

Concat = "LDAP://CN=Users, " & dom
Wscript.echo "The concatenated DN is " & concat
Set obj = GetObject(Concat) 'Binding to the user s object
Wscript.echo "Its Class is " & obj.class
Wscript.echo "It contains the following objects:"
for each UserObj in obj
        wscript.echo UserObj.class & " " & UserObj.name
Next
```

13.2 VBScript to List Users and Groups

Create a file with a VBS extension that contains the VBScript commands you want executed. At the command prompt use cscript to execute the VBScript file.

ListAllUsersAndGroups.vbs Source:

```
Option Explicit
Dim dom
Dim ou
Dim user
Dim concat
Dim obj
Dim UserObj

Function FindAndBind()
   Dim myobj
   Set myObj = GetObject("LDAP://rootDSE")
   FindAndBind=myObj.get("defaultNamingContext")
End Function

FindAndBind
Dom = FindAndBind

Concat = "LDAP://CN=Users, " & dom
Wscript.echo "The concatenated DN is " & concat
Set obj = GetObject(Concat) 'Binding to the user s object
Wscript.echo "Its Class is " & obj.class
Wscript.echo "It contains the following objects:"
for each UserObj in obj
          wscript.echo UserObj.class & " " & UserObj.name
Next
```

ListAllUsersAndGroups.vbs Execution

```
C:\Classes\Active Directory>cscript ListAllUsersAndGroups.vbs
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

The concatenated DN is LDAP://CN=Users, DC=SCASI,DC=com
Its Class is container
It contains the following objects:
user CN=ACTUser
user CN=Administrator
user CN=ASPNET
group CN=Cert Publishers
group CN=Debugger Users
group CN=DHCP Administrators
group CN=DHCP Users
group CN=DnsAdmins
group CN=DnsUpdateProxy
group CN=Domain Admins
group CN=Domain Computers
group CN=Domain Controllers
group CN=Domain Guests
group CN=Domain Users
group CN=Enterprise Admins
group CN=Group Policy Creator Owners
user CN=Guest
group CN=HelpServicesGroup
user CN=IUSR_SERVER2
user CN=IUSR_SYSTEMS-SCASI
user CN=IWAM_SERVER2
user CN=krbtgt
group CN=OWS_2778318560_admin
group CN=RAS and IAS Servers
group CN=Schema Admins
user CN=SQLDebugger
user CN=SUPPORT_388945a0
group CN=TelnetClients
group CN=VS Developers
user CN=VUSR_SYSTEMS-SCAS
```

13.2.1 Scriptomatic

Scriptomatic is a Microsoft tool that writes WMI scripts in VBScript, Perl, Python or Jscript. Besides creating scripts, Scriptomatic teaches how to write WMI scripts.

13.2.2 WMI Code Creator

This is a Microsoft tool that creates scripts in VBScript, C#, and VB.NET that use WMI. This tool also provides the ability to browse through WMI name spaces and classes to find their methods, properties, qualifiers and descriptions.

13.3 Active Directory API

14 Add On Security Products

Virus Software is an absolute must!
Anti-Spam, Anti-Malware and Anti-Adware programs are additional layers of security.
Firewalls can restrict attacks on systems and must be used in networks

14.1 DumpSec

DumpSec by Sumarsoft is an easy to use security auditing program that reviews file system and other types of protections, audit settings, users, groups and other security settings.

14.2 Sys-Secure

Sys-Secure provides an easy to understand report of information and vulnerabilities for various systems including Windows. There is no software to install because it uses output from easy to use scripts and commands. www.sys-secure.com

14.3 Encryption

A very good lists and reviews of encryption products can be found at http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software and http://en.wikipedia.org/wiki/List_of_cryptographic_File_Systems.

14.3.1 GnuPG

GnuPG (GPG) is a complete and free implementation of the Open PGP standard as defined in RFC4880. GPG can be found at www.gnupg.org.

14.3.2 FileZilla

14.3.3 TrueCrypt

14.4 Add On Security Products Audit Program

- Determine whether any add on security products are used to enhance security in the LAN environment
- Identify the features of any add on security products
- Determine which features of 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

15 System Management

15.1 Chkdsk

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Rodney>chkdsk /?
Checks a disk and displays a status report.


CHKDSK [volume[[path]filename]]] [/F] [/V] [/R] [/X] [/I] [/C] [/L[:size]]


  volume          Specifies the drive letter (followed by a colon),
                  mount point, or volume name.
  filename        FAT/FAT32 only: Specifies the files to check for fragmentation
.
  /F              Fixes errors on the disk.
  /V              On FAT/FAT32: Displays the full path and name of every file
                  on the disk.
                  On NTFS: Displays cleanup messages if any.
  /R              Locates bad sectors and recovers readable information
                  (implies /F).
  /L:size         NTFS only:  Changes the log file size to the specified number
                  of kilobytes.  If size is not specified, displays current
                  size.
  /X              Forces the volume to dismount first if necessary.
                  All opened handles to the volume would then be invalid
                  (implies /F).
  /I              NTFS only: Performs a less vigorous check of index entries.
  /C              NTFS only: Skips checking of cycles within the folder
                  structure.

The /I or /C switch reduces the amount of time required to run Chkdsk by
skipping certain checks of the volume.

C:\Documents and Settings\Rodney>chkdsk /V
The type of the file system is NTFS.
Volume label is ACER.

WARNING!  F parameter not specified.
```

```
Running CHKDSK in read-only mode.

CHKDSK is verifying files (stage 1 of 3)...
File verification completed.
CHKDSK is verifying indexes (stage 2 of 3)...
Index verification completed.
Detected minor inconsistencies on the drive.  This is not a corruption.
CHKDSK is verifying security descriptors (stage 3 of 3)...
Cleaning up 284 unused index entries from index $SII of file 9.
Cleaning up 284 unused index entries from index $SDH of file 9.
Cleaning up 284 unused security descriptors.
Security descriptor verification completed.

  37182442 KB total disk space.
  31311445 KB in 77843 files.
     29168 KB in 15986 indexes.
         0 KB in bad sectors.
    194566 KB in use by the system.
     65536 KB occupied by the log file.
   5647262 KB available on disk.

       512 bytes in each allocation unit.
  74364884 total allocation units on disk.
  11294525 allocation units available on disk.

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

15.2 Defrag

```
Defragmentation – Defrag /?

C:\Documents and Settings\Rodney>defrag /?
Usage:
defrag <volume> [-a] [-f] [-v] [-?]
  volume  drive letter or mount point (d: or d:\vol\mountpoint)
  -a      Analyze only
  -f      Force defragmentation even if free space is low
  -v      Verbose output
  -?      Display this help text

C:\Documents and Settings\Rodney>
C:\Documents and Settings\Rodney>
C:\Documents and Settings\Rodney>
C:\Documents and Settings\Rodney>
C:\Documents and Settings\Rodney>
C:\Documents and Settings\Rodney>
C:\Documents and Settings\Rodney>defrag c:
Windows Disk Defragmenter
Copyright (c) 2001 Microsoft Corp. and Executive Software International, Inc.

Analysis Report
    35.46 GB Total,  5.38 GB (15%) Free,  17% Fragmented (34% file fragmentation
)

Defragmentation Report
    35.46 GB Total,  5.37 GB (15%) Free,  13% Fragmented (26% file fragmentation
)

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

15.3 Virtual Machines

While virtual machines (VM) are out of the scope of this class the following information should be reviewed if your organization is using virtual machines.

Hypervisor VM Security information can be found at the following URLs:

- http://www.vmware.com/security/
- http://www.vmware.com/resources/techresources/cat/91

On standard ESX servers the service console is hardened linux. With ESXi the OS is stripped down and there's no service console but there is a remote command line interface. For almost everything you can do from the VirtualCenter GUI, there is a command line utility to do the same or more so you can write batch files to call the various VMware commands.

On ESX server the service console can be accessed via SSH which means you can use PUTTY or your favorite SSH client to run commands and capture output. On the VirtualCenter side you have granular control at the individual guest level and permissions can also be inherited from containers, resource pools and data centers (top level containers).

VMware does not recommend installing any 3rd party linux updates or linux updates from other vendors. They suggest you only get your patches from them.

VMWare can write to a syslog server (documented in the hardening guide) and can sync to NTP servers for time. The firewall is on by default.

VMware product documentation can be found at the following URL:
http://www.vmware.com/support/pubs/

16 Application Security

16.1 Web Application Security

Applications can have all the same issues as operating systems. Consider the Open Web Application Security Project (OWASP) top ten documented at http://www.owasp.org/index.php/Main_Page

ParosProxy can be used to scan web applications for vulnerabilities. ParosProxy can be found at http://www.parosproxy.org/index.shtml.

A very cool tool is for reviewing web applications is NTObjectives which can be found at http://www.NTObjectives.com/

16.2 Application Database Security

Data in application databases can often be accessed with ODBC using Access or Excel.

16.3 Application Configuration Files

Ini and other configuration files often contain sensitive information including userids and passwords.

Active Directory Application Mode (ADAM) and Active Directory Lightweight Directory Services (AD LDS)

17 Other Sources of Information/Bibliography

Introduction to Windows 10

www.Microsoft.com 10

http://www.computerhope.com/history/windows.htm 10

http://www.cerias.purdue.edu/ 11

http://www.cert.org/ 11

http://www.cisecurity.org/ 11

http://www.csrc.ncsl.nist.gov/ 11

http://www.first.org/ 11

http://www.fraud.org/ 11

http://www.itgi.org/ 11

http://www.nist.org/ 11

http://www.pcisecuritystandards.com/ 11

http://www.SANS.org/ 12

http://www.us-cert.gov/reading_room/ 12

http://www.nist.gov/ 12

Physical Security 15

http://www.openwall.com/john/ 15

Active Directory and the Global Catalog 17

Domains, Forests, and Trees 22

http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx 22

http://En.Wikipedia.com/Active_Directory#Trust 22

Security Settings and Group Policy Objects 24

User Profiles, Groups, and Organizational Units 35

http://www.beginningtoseethelight.org/ntsecurity/index.php 40

Resource Protections 44

Services and Privileged Programs 55

www.BlackViper.com 55

Network Access 59

Logging and Monitoring 75

http://la-samhna.de/library/scanners.html 83

http://www.ossec.net/wiki/index.php/OSSEC 83

http://www.belarc.com/free_download.html?/try/ib.CIS.cgi 83

Backup and Contingency Planning 85

Patch Management 86

Miscellaneous Tools 88

Add On Security Products 92

http://www.sys-secure.com/ 92

http://en.wikipedia.org/wiki/Comparison of disk encryption software/ 92

http://www.wikipedia.org/wiki/List of cryptographic File Systems/ 92

http://www.gnupg.org/ 92

System Management 94

http://www.vmware.com/security/..96
http://www.vmware.com/resources/techresources/cat/91 96
http://www.vmware.com/support/pubs/ 97
Application Security 98
http://www.owasp.org/index.php/Main_Page 98
http://www.parosproxy.org/index.shtml...98
http://www.ntobjectives.com/ 98
Other Sources of Information 99

>>>>>>>>>>>>>>>>> Microsoft.com <<<<<<<<<<<<<<<<<
Windows 2000 Support Center:
Windows 2003 Support Center
Windows 2008 Support Center
http://support.microsoft.com/default.aspx?scid=fh;[ln];win2000&product=msall

Active Directory, Robbie Allen & Alistair Lowe-Norris, 2003, O'Reilly & Associates
Little Black Book of Windows 2000 Security, Ian McLean, Coriolis, 2000
Active Directory Programming, Charles Oppermann, Microsoft Press, 2001
Active Directory Programming, Gil Kirkpatrick, Sams Publishing, 2000
Windows 2000 Active Directory, Joe Casad, McGraw-Hill, 2000
Inside Windows 2003 Server, William Boswell, Addison-Wesley, 2003
Scripting Windows 2000, Jeffrey Honeyman, McGraw-Hill, 2000
The Ultimate Windows 2003 System Administrator's Guide, Robert Williams and Mark Walla, Addison-Wesley, 2003

18 Windows Information Request List

Sys-Secure for Windows Request List

This document describes the files required from a Windows domain controller to generate a complete Sys-Secure report. A directory should be created and the output from all the commands and scripts should be put into the directory. Many of the commands can be put into BAT files to save time.

Caution. The following commands have been tested and used on hundreds of systems in tens of shops with no problems. Prior to running in a production environment each command should be reviewed and tested to ensure a complete understanding of the command and identify any possible impact to your environment. If misused, some of the following commands could make a system unusable.

The information generated by these commands is very sensitive. Protect the directory containing this information. Encrypt the data while it is stored and while in transit. After this data has been processed, back up an encrypted copy of the data to CD or DVD and delete it from the network.

Note that depending on the configuration of your system some of these files can be very large. Make sure that you have enough disk space. (The largest system reviewed to date used 800 megabytes. The smallest system used 250 kilobytes)

Most of the following commands require Administrator, Domain Administrator and/or Enterprise Administrator access. The RunAs command can be used to specify a userid to be used for execution of a command.

1. Use LDIFDE to dump the contents of Active Directory from the domain controller. The output file name should be the name of your domain controller and an ldf extension.

```
ldifde –f < DomainControllerName >.ldf –s <DomainControllerName>
```

2. Use the script '"getlocaluserinformation.vbs" to list the characteristics of each user on the system. Pipe this output to the file <DomainControllerName>UserInfo.txt

```
Cscript getlocaluserinformation.vbs > <DomainControllerName>UserInfo.txt
```

3. Use the script '"GetAllTSAccounts.vbs" to list the characteristics of each TS Account on the system. Pipe this output to the file <DomainControllerName>TSAccountInfo.txt:

```
Cscript GetAllTSAccounts.vbs > <DomainControllerName> TSAccountInfo.txt
```

4. Use GPMC.MSC to export GPOs to HTML documents. Select each GPO and use the menu option <Action><Save Report>, specify the directory, file name (should be the name of the GPO), and Save As HTML Type.

5. Use GPRESULT to show the Group Policy Objects in effect on each server in the environment.

6. Use the following command line commands to generate information about computer specific information on the domain controller and selected servers. (The following commands have been put into a BAT file named “runallnetcommands.bat”.)

a. Net Accounts > NetAccounts.Log
b. Net Config Server > NetConfigServer.Log
c. Net Config WorkStation > NetConfigWorkstation.Log
d. Net Group > NetGroup.Log
e. Net LocalGroup > NetLocalGroup.Log
f. Net Share > NetShare.log
g. Net Statistics Server > NetStatisticsServer.Log
h. Net Statistics WorkStation > NetStatisticsWorkStation.Log
i. Net Time > NetTime.Log
j. Net Use > NetUse.Log
k. Net User > NetUser.Log
l. Net View /Domain > NetViewDomain.Log
m. Net View > NetView.Log
n. NetStat –a > NetStatA.Log
o. NetStat -a -b -n > NetStatABN.Log
p. arp -a > ArpA.Log
q. tasklist /V /FO CSV > TaskListVFOCSV.Log
r. netsh show helper > netshShowHelper.txt
s. netsh show alias > netshShowAlias.txt
t. schtasks /query > schtasksquery.txt
u. set > set.txt

7. Run the script “GetServicesWMIQuery.vbs” using CScript to list all services running on the server. Pipe the output to <SystemName>ServicesWMI.txt:

```
cscript GetServicesWMIQuery.vbs > <SystemName>ServicesWMI.txt
```

8. Export the registry to a reg file using Regedit.exe or Regedt32.exe.

9. Use SubInAcl.exe (Available from Microsoft) to generate a report of registry key security.

```
SubInACL /verbose=1 /outputlog=SubInACLKeyReg<SystemName>.txt /keyreg * /display
```

10. Use SubInAcl.exe (Available from Microsoft) to generate a report of registry sub-key security.

```
SubInACL /verbose=1 /outputlog=subinaclSubKeyReg<SystemName>.txt /subkeyreg * /display
```

11. Use the CACLS command to generate a report of file security for every file on the system to <SystemName>-<DriveLetter>-FilesCACLS.Log where <SystemName> is the name of the system the file list is from. DriveLetter is the letter of the drive the list is from. Use the /T and /C options. For Example:

```
Cacls C:*.* /T /C >> <SystemName>-C-FilesCACLS.Log
```

12. Use the CACLS command to generate a report of file security for each disk on the system to <SystemName>-<DriveLetter>-DiskCACLS.Log where <SystemName> is the name of the system the file list is from. DriveLetter is the letter of the drive the list is from. For Example:

```
Cacls C:  >> <SystemName>-C-DiskCACLS.log
```

13. Use the script “SystemInfoWMIQuery.vbs” to get system information. For Example:

```
Cscript SystemInfoWMIQuery.vbs > <SystemName>SystemInfo.txt
```

14. Use the script “OSInfoWMIQuery.vbs” to get system information. For Example:

```
Cscript OSInfoWMIQuery.vbs > <SystemName>OSInfo.txt
```

15. Use the script “LogicalShareInfoWMIQuery.vbs” to get system information. For example:

```
Cscript LogicalShareInfoWMIQuery.vbs > <SystemName>LogicalShareInfo.txt
```

16. Use the script “DomainInfoWMIQuery.vbs” to get domain information. For example:

```
Cscript DomainInfoWMIQuery.vbs > <SystemName>DomainInfo.txt
```

17. Use the Java –version command to get the Java version number. For example:

```
Java –version > <SystemName>JavaVersion.txt
```

18. Use one of the following methods to provide information about the trust relationships of this computer:

a. Use the Active Directory Domains and Trusts MMC snap-in. Expand all the nodes and press the print screen <PrtSc> button. Save the screen print by opening a word document and using Control-V (<Ctl><V>) to paste the screen print into the document. For each domain listed, right click and select Properties. Click the Trust tab and then press the print screen <PrtSC> button. Save all the print screens from his step to a Word Document named <ComputerName>ADTrusts.Doc.

b. Use the Active Directory Users and Computers MMC Snap-in. On the View menu option click Advanced. In the left pane expand the contents and locate the System container. In the right pane locate all the entries that have the value “Trusted Domain” in the Type column. Right click each “Trusted Domain” and select Properties. Press the print screen <PrtSc> keyboard button.

Save the screen print by going to a word document and using Control-V (<Ctl><V>) to paste the screen print into the document.

c. Use the NLTest tool from the resource kit to report on all the trusted domains.

18.1 RunAllNetCommands.bat

```
Net Accounts > NetAccounts.Log
Net Config Server > NetConfigServer.Log
Net Config WorkStation > NetConfigWorkstation.Log
Net Group > NetGroup.Log
Net LocalGroup > NetLocalGroup.Log
Net Share > NetShare.log
Net Statistics Server > NetStatisticsServer.Log
Net Statistics WorkStation > NetStatisticsWorkStation.Log
Net Time > NetTime.Log
Net Use > NetUse.Log
Net User > NetUser.Log
Net View /Domain > NetViewDomain.Log
Net View > NetView.Log
NetStat -a > NetStatA.Log
NetStat -a -b -n > NetStatABN.Log
arp -a  > ArpA.Log
tasklist /V /FO CSV > TaskListVFOCSV.Log
netsh show helper > netshShowHelper.txt
netsh show alias > netshShowAlias.txt
schtasks /query > schtasksquery.txt
set > set.txt
```