Windows Active Directory & Vista

Presented by:

Rodney Kocot K3DES Systems Control and Security Incorporated <u>Rodneykocot@gmail.com</u> 818-370-0442

Presented to the:

Information Systems Audit and Control Association San Francisco Chapter

At the:

Hotel Nikko San Francisco, California

Copyright © 2004 by Rodney Kocot, All Rights Reserved

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:
 - o Issue/Information Title
 - Description
 - \circ Finding
 - Detail Information
 - o Risk
 - Recommendation

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

Table of Contents

1	Introduction to Windows	9
1.1	Why is Security Important?	9
1.2	Windows History	9
1.3	Which Windows are you Looking Through?	10
1.4	Active Directory	10
1.5	Security Standards	10
1.6	Introduction to Windows Audit Steps	11
1.6	5.1 Background	11
1.6	5.2 Documentation	11
1.6	5.3 Listings	11
1.6	6.4 Risk Analysis	11
1.6	6.5 High Level Audit Program	12
2	Physical Security	13
2.1	Key Katcher	13
2.2	Unix Boot Software	13
2.3	Physical Security Audit Steps	14
3	Active Directory and the Global Catalog	15
3.1	Active Directory Details	15
3.2	The Schema	16
3.2	2.1 Registering the Schema Manager MMC DLL:	16
3.2	2.2 Active Directory Schema Snap-in:	16
3.3	Active Directory Structure	17
3.4	Active Directory Dump Utilities - LDIFDE	17
3.5	The Global Catalog (GC)	17
3.6	Light Weight Directory Access Protocol (LDAP)	17
3.7	Enumeration of Active Directory Information	17
3.7	7.1 Script to Dump Active Directory Information	18
3.7	7.2 Script to Dump Active Directory Information Output	18
4	Domains, Forests, and Trees	20
4.1	Trust Relationships	
4.2	Active Directory Domains and Trusts	21
5	Security Settings and Group Policy Objects	22
5.1	Microsoft Management Console (MMC)	22
5.2	Snap-ins	23
5.3	Manage Your Server Wizard:	23
5.4	Default Domain Controller Security Settings	24
5.5	Password Security Settings	25
5.6	Default Domain Controller Security Settings:	26
5.7	Event Log Configuration	27
5.8	More Default Security Settings	
5.9	Group Policy Objects (GPOs)	28
6	User Profiles, Groups, and Organizational Units	31
6.1	User Profiles	
6.1	1.1 Active Directory Users and Computers:	31
6.1	1.2 New Object – User - Identifying Information:	32

6.1	.3 New Object - User - Password	33
6.1	.4 Adding Users to Groups	34
6.1	.5 Administrators	35
6.1	.6 Security Accounts Manager (SAM)	35
6.2	Groups	36
6.3	Global Groups	36
6.3	.1 NET GROUP	36
6.4	Local Groups	37
6.4	.1 NET LOCALGROUP	37
7	Resource Protections	38
7.1	NTFS Security	38
7.2	Encrypting File System	38
7.3	DFS – Distributed File System	38
7.4	File Security Properties	39
7.5	Permission options	40
7.6	File Server Management	41
7.7	Share Protections	41
7.7	.1 Shared Folder Properties:	43
7.8	Directory and File Protections	43
7.9	BAT File to List Share Protections	45
7.10	Output From BAT File to List Share Protections	45
7.1	0.1 Openfiles	46
7.11	Resource Protections Audit Program	48
8	Services and Privileged Programs	49
8.1	Services and Privileged Programs Overview	49
8.2	Services and Privileged Programs Commands	49
8.2	.1 Services.msc	49
8.2	.2 SU	49
8.3	1 askiist	
8.4	Services and Privileged Programs Audit Program	
9	Network Access	32
9.1	1 Network Address Translation	32
9.1	2 Poutors and Eirowells	32 52
9.1	2 Dynamic Host Configuration Protocol (DHCP)	52 54
0.1	Network Commands	
9.2	1 NFT /?	55
9.2	2 NET SHARE	55
9.2	3 NET USE /H	56
9.2	4 NET USER	50
9.2	5 NET VIEW	57
9.2	6 Inconfig	57
9.2	7 Netstat	
9.2	8 Nhtstat	<i>5</i> / 59
9.2	9 Ping	59 59
92	10 Tracert	60
9.3	NMAP	60
-		

9.4	Network Load Balancing Manager	62
9.5	Routing and Remote Access	63
9.6	Sniffers	64
9.6	.1 Sniffer Data Display	64
9.6	.2 Sniffer Packet Dump:	65
9.7	Dialup	66
9.8	Wireless	66
9.9	Internet Information Services Manager	67
9.10	Network Security Audit Program	67
10	Logging and Monitoring	68
10.1	Reviewing Logs	68
10.	1.1 EventQuery.vbs	
10.	1.2 Event Viewer – Security Log	69
10.	1.3 Security Log Settings	70
10.2	Baseline Security Analyzer	71
10.	2.1 Baseline Security Analyzer Help	71
10.	2.2 Baseline Security Analyzer Output	72
10.3	File Integrity Monitoring	76
10.4	Open Source Host Based Intrusion Detection System (OSSEC)	76
10.5	Free PC Audits	76
11	Backup and Contingency Planning	77
11.1	Backup and Contingency Planning Audit Program	77
12	Patch Management	78
12.1	Patch Management Systems	78
12.2	Don't Forget Application Patches!	79
12.3	Patcher Beware	79
13	Miscellaneous Tools	80
13.1	Active Directory Scripting	80
13.2	VBScript to List Users and Groups	81
13.3	Active Directory API	82
14	Add On Security Products	83
14.1	Add On Security Products Audit Program	
15	System Management	84
15.1	Chkdsk	
15.2	Defrag	86
16	Application Security	
16.1	Web Application Security	87
16.2	Application Database Security	
16.3	Application Configuration Files	
17	Other Sources of Information/Bibliography	87

Table of Illustrations

Introduction to Windows	9
Physical Security	13
Key Katcher	13
Active Directory and the Global Catalog	15
Registering the Schema Manager MMC DLL	16
Active Directory Schema Snap-in	16
LDIFDE Sample Output	17
Script to Dump Active Directory Information	
Script to Dump Active Directory Information Output	
Domains, Forests, and Trees	
Active Directory Domains and Trusts	21
Security Settings and Group Policy Objects	
Microsoft Management Console (MMC)	
Manage Your Server Wizard	
Password Security Settings	
Default Domain Controller Security Settings	
Event Log Configuration	
Default Domain Controller Security Settings	
User Profiles, Groups, and Organizational Units	
Active Directory Users and Computers	
New Object – User - Identifying Information	
New Object - User - Password	
Net Group	
Net Localgroup	
Resource Protections	
Distributed File System	
File Security Properties	
File Server Management	
Shared Folder Properties	
Directory ACL	
Share ACL	
BAT File to List Share Protections.	
Output From BAT File to List Share Protections	
Openfiles	
Services and Privileged Programs	
sc query state= all	
Tasklist	
Network Access	
Router Logs	
Windows Server 2003 Fire Wall Advanced Settings	
Net Help	55
Net Share	
Net User	
Net View	

September 22, 2008

Netstat -help	57
Netstat Active Connections	58
Nbtstat protocol statistics and TCP/IP connections	59
Ping	59
Tracert	60
Nmap	60
Network Load Balancing Manager	62
Routig and Remote Access	63
Sniffer Data Display	64
Sniffer Packet Dump	65
Internet Information Services (IIS) Manager	67
Logging and Monitoring	68
Event Viewer - Security Log	69
Audit Policy	70
Security Options	70
Baseline Security Analyzer Help	71
Baseline Security Analyzer Output	72
Backup and Contingency Planning	77
Patch Management	78
Miscellaneous Tools	80
ListAllUsersAndGroups.vbs Source	81
ListAllUsersAndGroups.vbs Execution	82
Add On Security Products	83
System Management	84
Application Security	87
Other Sources of Information	87

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

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: <u>http://www.computerhope.com/history/windows.htm</u>

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 tress and domain forests.

1.5 Security Standards

http://www.cisecurity.org/

http://www.pcisecuritystandards.com/

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

http://www.nist.gov/

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 copies of, or access to, all policies, standards and procedures.

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
- 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
 - \checkmark 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.

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

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.

September 22, 2008

2.3 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.
- 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.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 Director	y Schema [systems-s	casi.SCASI.com]\Classes]	×
Eile Action View Favorites Window	Help		×
		securityObject Properties	×
Console Root Computer Management (Local) Active Directory Users and Computers [syster Active Directory Sites and Services [syster Active Directory Domains and Trusts Active Directory Domains and Trusts Distributed File System Distributed File System DNS Event Viewer (Local) Event Viewer (Local) Active Directory Schema [systems-scasi.S(Active Directory Schema [systems-scasi.S(Attributes	Name Name SamDomain SamDomainBase SamDomainBase	General Relationship Attributes Default Security securityObject securityObject Description: Security-Object Cgmmon Name: Security-Object & 500 OID: 1.2.840.113556.1.5.1 Class Type: Abstract Category gecurityObject securityObject Change Show objects of this class while browsing Class is active	
	■a top ■a trustedDomain ■a typeLibrary ■a user	OK Cancel Apply Structural Active Type-Library Structural Active User	
		· · · · · · · · · · · · · · · · · · ·	<u> </u>
🖉 Start 🛛 🞯 🧔 👘 Active Directory.	C:\Documents a	. 🔤 C:\WINDOWS\s 🌇 Console1 - [Co 🗍 🖉 🖼 😏 🐼 1:14	PM

September 22, 2008

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 objectClas	objectClas: distinguish instanceTy whenCreat whenChan subRefs uSNCreate repsFrom uSNChang name =SCASI domainDN: DC=SCASI 5 20040109C 200405232 DC=Forest 4098 X'0100000 118853 SCASI =Users, container CN=Users, 4 20040109C 20040109020431.0Z 4304 4304 Users =Comp: container CN=Comp: 4 20040109C 20040109020431.0Z 4305 4305 Computers =Doma organizatio OU=Doma 4 20040109C 20040109020431.0Z 4411 4411 Domain Cc =Syster container CN=Syster 4 20040109C 20040109020431.0Z 4306 4306 System =LostAr lostAndFou CN=LostAr 4 20040109C 20040109020431.0Z 4302 4302 LostAndFo =Infrast infrastructu CN=Infrast 4 20040109C 20040109020431.0Z 4412 4412 Infrastructu =Eoreig container CN=Eoreig 4 20040109C 20040109020431.0Z 4413 4413 EoreignSer				
DC=SCASIdomainDN	NobjectClas: distinguish: instanceTy whenCreat whenChan subRefsuSNCreate repsFromuSNChang nameC=SCASI domainDN: DC=SCASI5 20040109C 200405232 DC=Forest4098 X'010000118853 SCASIN=Users, containerCN=Users,4 20040109C 20040109020431.0Z43044304 UsersN=Compi containerCN=Compi4 20040109C 20040109020431.0Z43054305 ComputersJ=Doma organizatio OU=Doma4 20040109C 20040109020431.0Z44114411 Domain CcN=Syster containerCN=Syster4 20040109C 20040109020431.0Z43064306 SystemN=LostAr lostAndFou CN=LostAr4 20040109C 20040109020431.0Z43024302 LostAndFoN=Infrast infrastructu CN=Infrast4 20040109C 20040109020431.0Z44124412 InfrastructuN=Foreig containerCN=Foreig4 20040109C 20040109020431.0Z44134413 ForeignSec				
CN=Users, container	CN=Users,	4 200401090200401090204	31.0Z 4304	4304 Users	
CN=Comp container	CN=Comp	4 200401090200401090204	31.0Z 4305	4305 Computers	
OU=Doma organizatio	OU=Doma	4 200401090200401090204	31.0Z 4411	4411 Domain Cc	
CN=Syster container	CN=Syster	4 200401090200401090204	31.0Z 4306	4306 System	
CN=LostAr lostAndFor	CN=LostAr	4 200401090200401090204	31.0Z 4302	4302 LostAndFo	
CN=Infrast infrastructu	ICN=Infrast	4 200401090200401090204	31.0Z 4412	4412 Infrastructu	
CN=Foreig container	CN=Foreig	4 200401090200401090204	31.0Z 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 colltems = 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 Verimary Domain Controller Flag: True DS Time Service Flag: True DS Writable Flag: True Name: Domain: SCASI Primary Owner Contact: Rodney Kocot

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.
- ✓ <u>http://En.Wikipedia.com/Active_Directory#Trust</u>

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

Active	Directory Domains and Tr	usts				_ 8 ×
<u>File A</u> cti	ion <u>V</u> iew <u>H</u> elp					
\leftrightarrow	🗈 📧 🖻 🗟 🔮					
Chive E	Directory Domains and Trusts	SCASI.com	CASI.com			
- 0 5 0	ASI.com	Name	Туре			
			There ar	e no items to show in this	view.	
•	•					
🛃 Start	🕝 🥌 🥘 🔟				2 🖾 🥑 🛱 🛃	11:00 AM
	Manage Your Ser	👔 Administrative Tools	C:\Classes\Activ	Active Director	🔄 Active Directory	Monday

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.

🚡 Management Console - [Console Root\A	ctive Directory Us	ers and Compute	rs [systems-scasi.SCASI.co	m]\SCASI.com\Users]
📸 Eile Action View Favorites Window	Help			×
	包 🖉 🚵 💎	🗟 ն		
Console Root	Name	Туре	Description	
🗄 🦓 Active Directory Domains and Trusts	🖸 ACTUser	User	Account used to launch th	
🕀 📆 Active Directory Sites and Services [syste	🜆 Administrator	User	Built-in account for admini	
Active Directory Users and Computers [s	S ASPNET	User	Account for running ASP	
E···· Saved Queries	🕵 Cert Publishers	Security Group	Members of this group are	
E B SCASI.com	Debugger Users	Security Group	Debugger users can debu	
Buildin	DHCP Adminis	Security Group	Members who have admini	
Domaio Controllers	DHCP Users	Security Group	Members who have view	
	20 DisAdmins	Security Group	DNS Administrators Group	
	🕵 DnsUpdatePr	Security Group	DNS clients who are permi	
	🕵 Domain Admins	Security Group	Designated administrators	
🕀 🎉 Distributed File System	🕵 Domain Comp	Security Group	All workstations and serve	
DNS	🕵 Domain Contr	Security Group	All domain controllers in th	
😥 🗊 Default Domain Controllers Policy [system]	🕵 Domain Guests	Security Group	All domain guests	
🗄 📑 💕 Default Domain Policy [systems-scasi.SC4	🕵 Domain Users	Security Group	All domain users	
🗄 🕀 🏐 Internet Information Services (IIS) Mana	🕵 Enterprise Ad	Security Group	Designated administrators	
🕀 💐 IP Security Monitor	🕼 Group Policy	Security Group	Members in this group can	
E Security Policies on Active Directory	🌆 Guest	User	Built-in account for guest	
Performance Logs and Alerts	🕵 HelpServices	Security Group	Group for the Help and Su	
E Security Configuration and Analysis	IUSR_SERVER2	User	Built-in account for anony	
E Security Templates	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	_1
	-		<u></u>	
2 🏄 Start 🛛 🞯 🐖 👘 🕅 Active Direc	tory Main.do	Management C	onsole	, 🛃 💽 11:01 AM

Microsoft Management Console (MMC)

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:



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

5.4 Default Domain Controller Security Settings

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

Uncle Bill's Default Security Settings:



September 22, 2008

5.5 Password Security Settings

🚡 Default Domain Security Setting	IS		_ 8 ×
<u>File Action View H</u> elp			
← → 1 🗈 🖪 😼 🔮			
Security Settings	Policy A	Policy Setting	
Account Policies Account Lockout Policy File System Services Account Account Account Account Account Account Account Policies Account Account Account Account Account Policies Account Account Account Account Account Account Account Account Policies Account Account Account Account Account Account Account Account Policies Account Accoun	Enforce password history Maximum password age Minimum password age Minimum password length Password must meet complexity requirements Store passwords using reversible encryption	24 passwords remembered 42 days 1 days 7 characters Enabled Disabled	
🥂 Start 🛛 🚱 🥌 🎮 🔞			📑 🗞 7:16 PM
Document1 - Mi] Fun Facts abou 🔄 Document5 - Mi 🙀 Ac	Iministrative 🎁 Default Doma	🛛 🤌 🥸 🔯 🛛 Friday

5.6 Default Domain Controller Security Settings:

Default Domain Controller Security Sel	ttings		_16
e <u>A</u> ction ⊻iew <u>H</u> elp			
🔿 🗈 🖪 🗙 🗗 🗟			
Security Settings Polic	cy 🛆	Policy Setting	
Account Policies	Maximum application log size	Not Defined	
🖞 Local Policies 🛛 🙀 🕅	Maximum security log size	Not Defined	
E - 2 Audit Policy	Maximum system log size	Not Defined	
Ger Rights Assignment	Prevent local guests group from accessing application log	Not Defined	
+ Security Options	Prevent local guests group from accessing security log	Not Defined	
P Event Log	Prevent local guests group from accessing system log	Not Defined	
Suctam Services	Retain application log	Not Defined	
B Penictry	Retain security log	Not Defined	
Default Domain Controller Security Settings ie Action Yew Help Image: Security Settings Policy / Policy Settings Policy Settings Image: Security Settings Policy / Policy Settings Not Define Image: Security Options Image: Security Options Not Define Image: Security Policies Image: Security Image: Security Policies Not Define Image: Security Policies on Active Direct Image: Security Policies on Active Direct Image: Security Policies on Active Direct Image: Security Policie	Not Defined		
Y Wireless Network (IEEE 802.11) P	Retention method for application log	Not Defined	
Public Key Policies	Retention method for security log	Not Defined	
Software Restriction Policies	Retention method for system log	Not Defined	
IP Security Policies on Active Direc			
2			
itart 🛛 🚱 🙈 🕅 🔯		1 1	7.28

5.7 Event Log Configuration



5.8 More Default Security Settings

🚡 Default Domain Controller Securi	ty Settings		
<u>File Action View H</u> elp			
⇔ → 🗈 🖬 🗙 📽 😫	1		
월 Security Settings	Policy A	Policy Setting	
🗄 🛃 Account Policies	Accounts: Administrator account status	Not Defined	
🖃 🛃 Local Policies	Accounts: Guest account status	Not Defined	
E al Audit Policy	Accounts: Limit local account use of blank pa	Not Defined	
🖽 🔄 User Rights Assignment	Accounts: Rename administrator account	Not Defined	
Security Options	Accounts: Rename quest account	Not Defined	
Event Log	Audit: Audit the access of global system obje	Not Defined	
H G Sustan Samiana	Audit: Audit the use of Backup and Restore	Not Defined	
	Audit: Shut down system immediately if unab	Not Defined	
The system	Devices: Allow undock without having to log on	Not Defined	
₩ Wireless Network (IEEE 802.11) P	BDevices: Allowed to format and eject remova	Not Defined	
The Public Key Policies	BODevices: Prevent users from installing printer	Not Defined	
Software Restriction Policies	BODevices: Restrict CD-ROM access to locally lo	Not Defined	
🗄 🧕 IP Security Policies on Active Dire	BODevices: Restrict floppy access to locally log	Not Defined	
22	BDevices: Unsigned driver installation behavior	Not Defined	
	Bomain controller: Allow server operators to	Not Defined	
	Domain controller: LDAP server signing requir	None	
	Bomain controller: Refuse machine account p	Not Defined	
	Bomain member: Digitally encrypt or sign sec	Enabled	
	Bomain member: Digitally encrypt secure cha	Not Defined	
	Bomain member: Digitally sign secure channe	Not Defined	
	Bomain member: Disable machine account pa	Not Defined	
	Bomain member: Maximum machine account	Not Defined	
	Domain member: Require strong (Windows 2	Not Defined	
	Interactive logon: Do not display last user na	Not Defined	
	Binteractive logon: Do not require CTRL+ALT	Not Defined	
•I I I	RM Interactive Jacons Massage toyt for users at	Not Dofinad	
🛃 Start 🛛 🚱 🥌 🥌 👿			🗾 🍪 7:31 PM
Document1 - Mi	Fun Facts abou 🐻 Document5 - Mi 🖏 Ad	ministrative Charles Default Doma	a 🕖 🌺 🔘 🛛 Friday

5.9 Group Policy Objects (GPOs)

The Group Policy Object (GPO) Editor or the Group Policy Management Console are used to manage Group Policy Objects.

Group Policy Objects can be exported to an MS Excel file.

Group Policy Objects are assigned to users at logon and to workstations at boot.

The GPO hierarchy is Local > Site > Domain > OU > OU > OU > ...

Inheritance of GPO settings goes down the list.

Lower levels can block non-enforced settings.

Higher levels can enforce settings down through the organization.

GPRESULT can be used to show what GPOs 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:
```

September 22, 2008

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

User Group Policy results for:						
SCASI\rodney.kocot.ad	m					
Domain Name: Domain Type:	SCASI Windows NT v4					
Roaming profile: Local profile:	(None) C:\Documents and Settings\rodney.kocot.adm					
The user is a member	of the following security groups:					
LookupAccountSid failed \Everyone BUILTIN\Users BUILTIN\Adminis NT AUTHORITY\IN NT AUTHORITY\Au \LOCAL	with 1789. trators TERACTIVE thenticated Users					
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 "Scri	pts" settings from these GPOs:					
New Group Polic	y Object					

Computer Group Policy results for:						
SCASI\WLSCASI0004\$						
Domain Name: Domain Type:	SCASI Windows NT v4					
The computer is a member of the following security groups:						
BUILTIN\Adminis \Everyone BUILTIN\Users NT AUTHORITY\NE NT AUTHORITY\Au LookupAccountSid failed LookupAccountSid failed	TWORK thenticated Users with 1789. with 1789.					

September 22, 2008

Г

```
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>
```

6 User Profiles, Groups, and Organizational Units

6.1 User Profiles

6.1.1 Active Directory Users and Computers:

Active Directory Users and Com	outers					
Jele Action View Window E	ielp				그러스	
⊢→ 🖻 📧 🐰 💼 🗡 🖆	" 🖸 🗟 🦉] 📆 🛍 🖓 🍕				
🖇 Active Directory Users and Computer	Users 32 objects	Users 32 objects				
Saved Queries	Name	Туре	Description		2	
SCASI.com	🕵 ACTUser	User	Account used to launch th			
⊞… <mark>∭</mark> Builtin	🖸 🖸 Administrator	User	Built-in account for admini			
🗄 🧰 Computers	S 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	Нарру			
	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			
	Brterprise Ad	Security Group	Designated administrators			
	Group Policy	Security Group	Members in this group can		_	
	Suest	User	Built-in account for guest			
	HelpServices	Security Group	Group for the Help and Su			
	115_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 '			
	Basic Inc	e	e (a)			
				J		
🖥 Start 🛛 🚱 🥌 🥘 🔯					🧳 🗾 6:52 PM	
Documenti - Microsoft	d droinisteat		Active Disectory Lices		Supday	

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."

	tive Directory U	sorg Isers and Com	nuters			ľ
Nev	v Object - User			×		
VI	Create	in: SCASI.co	m/Users	=		
E -	Eirst name:	David	Initials: M	tio	on	
	Last name:	Kocot	•	, s er	of this group are r users can debu	
	Full name: David M. Kocot		s	s who have admini		
	- Internet and		mi	inistrators Group		
david.kocot.adm			@SCASI.com	te	ts who are permi ed administrators	
, User logon name (pre- <u>W</u> indows 2000				st	ations and serve n controllers in th	
	SCASI		david.kocot.adm) air	n guests	
-				te	ed administrators	
			< <u>₿</u> ack <u>N</u> ext > 0	Sancel ac	in this group can count for guest	
-			GIIS WPG Security Group	pr	r the Help and Su er Process Group	
			IUSR_SYSTE User	Built-in ac	count for anony	
			WIWAM_SYSTE User	Built-in ac Microsoft	count for Intern SharePoint role '	
			RAS and IAS Security Group	Servers in Designate	n this group can ed administrators	
•		•	SUPPORT_38 User	This is a v	rendor's account	
irt	🕝 🥭 🧕 🗍	2 🖾 🥑	5			2 3 10
	Document2 - I	Microsoft	🦪 Manage Your Server 🔤 🎻 A	ctive Directo	ory User	The The

6.1.3 New Object - User - Password



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.

6.1.4 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.

Do	cument3 - Microsoft Word		
File	Active Directory Users and	Computers	- D ×
I D	Gile Action View Window	Domain Admins Properties	_ _ ð ×
	⇔ ⇒ 🗈 📧 👗 🛍 >	General Members Member Of Managed By	
	Active Directory Users and Com	Members	
-	Saved Queries	Name Active Directory Folder	<u> </u>
	Builtin	2 Administrator SCASI.com/Users	he computer/domain
1	Computers	😰 David M. Kocot SCASI.com/Users	ed to publish certificates to the Ac
2	Domain Controllers		ses on this machine, both locally a
			access to DHCP service
N			ss to the DHCP service
			erform dynamic undates on behal
-			omain
			to the domain
1			
2			nterprise
7			group policy for the domain
			the computer/domain
4		Add Hemove	nter
			ess to Internet Information Servi
		OK Cancel Apply	ation Services to start out of prov
2			r web 'http://systems-scasi'
1		Servers in this group can access n	emote access properties of users 🗾
≣ ⊠			
Page			
🕂 St	tart 🛛 🚱 🥭 🥌 🖉 😢 🧯		🍓 🛃 11:00 PM
	Document3 - Microsoft	Manage Your Server Active Directory User	💽 Thursday

6.1.5 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 antivirus 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.

6.1.6 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 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.
```

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

🔄 \\SYSTEMS-SCASI\Public					_ & ×
Eile Edit View Favorites I	ools Help				
🕒 Back 🔻 🕤 👻 🍠 Searc	th 🜔 Folders 🛛 🖽 🕶				
Address 浸 \\SYSTEMS-SCASI\Publ	lic				💌 🛃 Go
Folders	× Name *	Size	Туре	Date Modified	Attributes
Desktop My Documents My Computer My Network Places Entire Network Microsoft Terminal Service Microsoft Windows Network Microsoft Windows Network	Text from 51.txt Distributed File 5y File Action View C C C C C C C C C C C C C	0 KB /stem Help 3 2 2 10 3 10 3 10 3 10 10 10 10 10 10 10 10 10 10 10 10 10	Text Document	1/11/2004 6:57 PM	A
 Server2 Server2 Systems-scasi Dilbert Public Systems - scasi Public Systems - scasi Printers and F Scheduled Ta Scheduled Ta Timothyk Meb Client Network Recycle Bin 	=ax¢		MS-SCASI\Public Enable	d -	
Type: Text Document Date Modified:	1/11/2004 6:57 PM Size: 0 bytes		0 by	rtes 👩 Internet	1
🟄 Start 🕝 🏉 💽 👿 🖻 Document1 - Micr	🦏 Administrative Tools 🏠 \\S	YSTEMS-SCAS	Active Directory	Distributed File	6:58 PM Sunday

7.4 File Security Properties



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	The user/group can modify the permissions of the file
Permissions	
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	Extended attributes are usually assigned by programs that use the file
Attributes	
Create Folders	Allows the creation of folders
Write Attributes	Allows the modification of attributes.
Write Extended	Allows the modification of extended attributes
Attributes	
Delete	Allows the deletion of subfolders and the files they contain, even if
Subfolders	the delete permission is not granted.
Delete	Allows the deletion of files and folders.
Read	Allows the viewing of the file or folder's permissions.
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



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.

otures Properties		?
ieneral Sharing Security C	Customize	
Group or user names:		
🚮 Administrators (ATTILA\A	dministrators)	
🖸 CREATOR OWNER		
🖸 David (ATTILA\David)		
SYSTEM		
f Users (ATTILA\Users)		
	A <u>d</u> d	<u>R</u> emove
Permissions for Users	Allow	Deny
Full Control		
Modify		
Read & Execute	4	
List Folder Contents	10	
Read	\checkmark	
Write		
Coopial Permissions		<u> </u>
For special permissions or for a click Advanced.	dvanced settings,	Ad <u>v</u> anced
 П (К	Cancel	1 Apple
		111111

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.
- 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:



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:



🔄 C:\Classes 🔤		_ □ ×	1
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vor	Classes Properties	Permissions for Classes	<u>?</u> ×
🔇 Back 🝷 🕤 🚽 🏂 🍃	General Sharing Security Customize	Share Permissions	1
Address C:\Classes Folders Desktop Des	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	Group or user names:	
	Description: User limit: Maximum allowed Allow this number of users: To set permissions for users who access this folder over the network, click Permissions. Cick Permissions. To modify how people use the content while offline, click Offline Settings.	Add <u>B</u> ern <u>Permissions for David M. Kocot</u> Allow Den Full Control Change Read M	ove
C RECYCLER ⊡ Rodney C System Volu	N <u>e</u> w Share	Ŗ	
E UserData E Control	OK Cancel Apply	OK Cancel	Apply
🗉 🧰 wmpub 🚽			iny

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

7.10 Output From BAT File to List Share Protections

Local name Z: Remote name \\SERVER01\APPLICATION Resource type Disk OK Status # 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

7.10.1 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.
                      Displays files opened locally or from shared folders.
    /Ouerv
                      Enables / Disables the display of local open files.
    /Local
                      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
                            C:\Documents and Settings\All Users\Desktop
564
      explorer.exe
568
      explorer.exe
                            C:\..\Application Data\Microsoft\CD Burning
640
      explorer.exe
                            C:\..\Content.IE5\index.dat
688
      explorer.exe
                            C:\..6595b64144ccfldf_6.0.2600.2982_x-ww_ac3f9c03
768
      explorer.exe
                            C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
                            C:\..6595b64144ccfldf_6.0.2600.2982_x-ww_ac3f9c03
C:\..6595b64144ccfldf_6.0.2600.2982_x-ww_ac3f9c03
800
      explorer.exe
828
      explorer.exe
                            C:\..6595b64144ccfldf_6.0.2600.2982_x-ww_ac3f9c03
C:\..6595b64144ccfldf_6.0.2600.2982_x-ww_ac3f9c03
876
      explorer.exe
888
      explorer.exe
948
      explorer.exe
                            C:\..6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
952
      explorer.exe
                             C:\..\History\History.IE5\index.dat
956
                            C:\..6595b64144ccf1df 6.0.2600.2982 x-ww ac3f9c03
      explorer.exe
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:\..6595b64144ccfldf_1.0.2600.2180_x-ww_522f9f82
                            C:\..6595b64144ccfldf_6.0.2600.2982_x-ww_ac3f9c03
C:\..6595b64144ccfldf_6.0.2600.2982_x-ww_ac3f9c03
1728
      explorer.exe
1920 explorer.exe
2008
      explorer.exe
                            C:\Documents and Settings\Rodney\NetHood
2144 explorer.exe
                            C:\..\MSHist012007031220070313\index.dat
                            C:\Documents and Settings\Rodney
C:\..6595b64144ccfldf_6.0.2600.2982_x-ww_ac3f9c03
12
      igfxtray.exe
60
      iqfxtray.exe
12
      hkcmd.exe
                            C:\Documents and Settings\Rodney
12
                             C:\Documents and Settings\Rodney
      iqfxpers.exe
12
      SynTPLpr.exe
                            C:\Documents and Settings\Rodney
                            C:\Documents and Settings\Rodney
C:\..6595b64144ccfldf 6.0.2600.2982 x-ww ac3f9c03
12
      SynTPEnh.exe
56
      SvnTPEnh.exe
12
      SOUNDMAN.EXE
                            C:\Documents and Settings\Rodney
                             C:\..6595b64144ccfldf_6.0.2600.2982_x-ww_ac3f9c03
60
      SOUNDMAN.EXE
12
      PDVDServ.exe
                             C:\Documents and Settings\Rodney
                             C:\..6595b64144ccfldf 6.0.2600.2982 x-ww ac3f9c03
60
      PDVDServ.exe
12
                            C:\Documents and Settings\Rodney
      LaunchAp.exe
                             C:\..6595b64144ccf1df 6.0.2600.2982 x-ww ac3f9c03
60
      LaunchAp.exe
52
                            C:\Program Files\Launch Manager
      Powerkey.exe
12
      HotkeyApp.exe
                            C:\Documents and Settings\Rodney
```

September 22, 2008

104	HotkeyApp.exe	C:\6595b64144ccf1df 6.0.2600.2982 x-ww ac3f9c03
188	Hotkow/pp ove	C·\ 6595b64144ccf1df 6 0 2600 2982 y-two ac3f9c03
400	HOLKEYAPP.exe	C.(6595D04144CC11d1_0.0.2000.2982_x-ww_ac519C05
492	HotkeyApp.exe	C:\6595b64144ccfldf_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
1.0	WDutton	C. Decuments and Cattings Dedney
12	WBULLOII.exe	C. (Documents and Settings (Rodney
16	WButton.exe	C:\6595b64144ccfldf_6.0.2600.2982_x-ww_ac3f9c03
12	epm-dm.exe	C:\Documents and Settings\Rodney
60	epm-dm exe	C·\ 6595b64144ccfldf 6 0 2600 2982 x-ww ac3f9c03
1.0	cpin ant.cxc	C:\WINDOWC\ austom22
12	wuaucit.exe	C: \WINDOWS\SYSTEMS2
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
150	wuducit.cxc	C.\NINDONO\Nindevelledete_ler
120	wuaucit.exe	C: (WINDOWS \WINdowsUpdate.log
532	wuauclt.exe	C:\6595b64144ccf1df 6.0.2600.2982 x-ww ac3f9c03
1.2	opgloador ovo	C:\Decuments and Settings\Bedney
12	ebsidadei.exe	C. Documents and Settings (Rodney
60	eDSloader.exe	C:\6595b64144ccfldf_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
61		$C_{\rm c}$ (Second of the second seco
400	ccapp.exe	C.(0395004144CC1101_0.0.2000.2902_X=WW_dC519C03
488	ccApp.exe	C:\\Microsoft\SystemCertificates\My
712	ccApp.exe	C:\6595b64144ccf1df_6.0.2600.2982 x-ww ac3f9c03
736	ccApp.exe	$C \cdot = 6595b64144ccf1df_{6} = 0.2600.2982 \times www.ac3f9c03$
60	VPTrav evo	$C \cdot = 6595664144 \text{ coff} \text{ df} = 6.0, 2600, 2002, w_{-www} = 20260 \text{ coff} = 2002 \text{ coff} = 20260 \text{ coff} = 2002 cof$
00	vrilay.exe	C.(
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	hpompmgr out	C:\Dragram Files\UD\bragramtesb
270	npempingr.exe	
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
202	he meneral and	C. \ _\uistam \uistam TE\\isdam dat
392	npcmpmgr.exe	C:\\History\History.lbs\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	noint32 eve	C:\Documents and Settings\Bodney
10	points2.exe	$C_{\rm c}$ (bocamenes) and becerings (noticely
ТЮ	point32.exe	C:\6595b64144CCI1dI_6.0.2600.2982_x-ww_aC319C03
84	point32.exe	C:\6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
12	hptskmgr.exe	C:\WINDOWS\system32
60	hotskmar eve	(.) 6595b64144ccf1df 6 0 2600 2982 x-ww ac3f9c03
404	het a lemone and	C:\C505b04144CC11d1_0.0.2000.2002_x ww_dc515C05
484	nptskmgr.exe	C:\6595b64144CCI1dI_6.0.2600.2982_x-ww_aC319C03
504	hptskmgr.exe	C:\\Content.IE5\index.dat
524	hptskmgr.exe	C:\Documents and Settings\Rodney\Cookies\index.dat
532	hptekmar ovo	C.) \Wistory\Wistory IE5\index dat
552	IIpcskiigi.exe	
580	nptskmgr.exe	C:\0595D04144CCI1dI_0.0.2600.2982_x-ww_ac319c03
584	hptskmgr.exe	C:\6595b64144ccfldf_6.0.2600.2982_x-ww_ac3f9c03
12	TrueCrypt.exe	C:\Documents and Settings\Rodney
60	TrueCrypt eye	(.) 6595b64144ccf1df 6 0 2600 2982 x-ww ac3f9c03
00	TIGGOLYPU.EXC	
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 EXF	(.) 6595b64144ccfldf 6 0 2600 2982 y-www.ac3f9c03
400	HINNORD BALL	a.)
488	WINWORD.EXE	C:\\Microsoft\Templates\Normal.dot
496	WINWORD.EXE	C:\6595b64144ccfldf 6.0.2600.2982 x-ww ac3f9c03
12	and eve	C. Documents and Settings Podney
12	CIIId. EAC	
96	cmd.exe	C:\6595664144cc11df_6.0.2600.2982_x-ww_ac3f9c03
12	openfiles.exe	C:\Documents and Settings\Rodney
1924	openfiles.exe	C:\6595b64144ccfldf 6.0.2600.2982 x-ww ac3f9c03
1		
l .		
Files	Opened Remotely via	local share points:
TNFO.	No shared open files	found
TIME O:	no snareu open illes	, <u>tounu</u> .

7.11 Resource Protections Audit Program

- 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 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 <u>www.BlackViper.com</u> 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
	WATT HINT	• 0x0
		. 040
SERVICE	NAME: ALG	
DISPLAY	NAME: Application	Laver Gateway Service
		: 10 WIN32 OWN PROCESS
	STATE	: 4 RUNNING
	21112	(STOPPABLE, NOT PAUSABLE, IGNORES SHUTDOWN)
	WIN32 EXIT CODE	: 0 (0x0)
	SERVICE EXIT CODE	(0)
	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 Aud:	io
-		: 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"

8.4 Services and Privileged Programs Audit Program

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

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:

Eile Edit Vie Back - For	ew <u>Go</u> <u>Bookmarks</u> <u>Iools</u> <u>Window</u> ward <u>Reload</u> <u>Stop</u> <u>Mttp://10</u>	Help .0.0.1/Log.htm		
Back For	ward - Reload Stop // http://10).0.0.1/Log.htm	1000	
Back For	ward Reload Stop			🧑 Search 🛛 🛸 👻 📶
and the second se	id Lable - Mozilia	t=ted	🙀 Incoming Log Table - Moz	zilla 📃 🔤 🎽
Outgoing Lo	Log Table	LIX hs Zupport Mozilla Community	Incoming Log Table	Refresh
LAN IP	Destination URL/IP	ice/P Imbei tup Password Status DHCP Log <u>Securit</u>	Source IP	Destination Port Number
10.0.0.10	www.mozilla.org	are some log settings and lists in this page.	213.191.74.144	1910
10.0.0.10	images.real.com		213.191.74.144	1911
10.0.0.10	content.real.com		24.126.161.166	80
10.0.0.10	images.real.com		66.216.97.106	1906
10.0.0.10	i.cnn.net		64.15.251.198	53
10.0.0.10	images.real.com		210.224.186.4	53
10.0.0.10	switch.atdmt.com		205.158.108.194	53
10.0.0.10	images.real.com	U-110	221.111.1.4	53
10.0.0.10	www.cnn.com		64.28.86.226	53
10.0.0.10	content.real.com		208.184.139.82	53
10.0.0.10	realguide.real.com		208.185.219.166	53
10.0.0.10	www.real.com		64.0.96.12	53
10.0.0.10	content.real.com	pming Access Log Outgoing Access Log	211.13.215.132	53
10.0.0.10	smilparse.real.com		204.176.88.5	53
10.0.0.10	start.real.com	bly Cancel	212.162.1.194	53
10.0.0.10	premium.cnn.com		202.160.241.130	53
10.0.0.3	www.secinf.net		65.169.170.131	53
10.0.0.3	a 1794.1 akamai net		63.216.25.130	53
10.0.0.3	ads isoftmarketing com		64.14.117.10	53
10.0.0.3	server1.isoftmarketing.com		208.184.39.130	53
10.0.0.10	cnnfn.com		216.73.83.10	53
10.0.0.10	view.atdmt.com		64.41.192.103	53
100010				
1 III. V.				
Start 0	CNN com - Mostilla	Mazilla		ph1 - Microsof

Windows Server 2003 Fire Wall Advanced Settings:



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.

9.2 Network Commands

9.2.1 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 ACCOUNTS NET HELPMSG NET START NET COMPUTER NET HELPMSG NET START NET CONFIG NET LOCALGROUP NET STATISTICS NET CONFIG SERVER NET NAME NET STOP 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 FILE NET SEND NET USER NET GROUP NET SESSION NET VIEW NET HELP SERVICES lists some of the services you can start. NET HELP SOMMAN AND NET HELP Syntax lines. NET HELP command | MORE displays Help one screen at a time.

9.2.2 NET SHARE

C:\Documents and Settings\rodney.kocot.adm>net share Share name Resource Remark _____ TPCS Remote IPC print\$ C:\WINDOWS\system32\spool\drivers Printer Drivers ADMIN\$ C:\WINDOWS C\$ C:\ wwwroot\$ c:\inetpub\wwwroot Remote Admin Default share Used for file share access to web OldCompBackup\$ C:\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 VPHOMEC:\PROGRA~1\SAVSymantec AntiVirusVPLOGONC:\PROGRA~1\SAV\logonSymantec AntiVirus WindowsSecClass C:\WindowsSecClass HPCLJ450 IP_10.42.0.200 Spooled HPCLJ4500 HPNetwork USB001 Spooled hp deskjet 5100 series The command completed successfully.

9.2.3 NET USE /H

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

9.2.4 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.
```

9.2.5 NET VIEW

```
C:\Documents and Settings\rodney.kocot.adm>net view
Server Name Remark
\\SERVER2
\\SYSTEMS-SCASI
The command completed successfully.
```

9.2.6 Ipconfig

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

9.2.7 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.
               Displays the owning process ID associated with each connection.
  -0
  -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.
                Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
  -s
               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 systems-scasi:smtp systems-scasi.SCASI.com:0 LISTENING TCP systems-scasi:domain systems-scasi.SCASI.com:0 LISTENING TCP TCP systems-scasi:kerberos systems-scasi.SCASI.com:0 LISTENING TCPsystems-scasi:pop3systems-scasi.SCASI.com:0LISTENINGTCPsystems-scasi:epmapsystems-scasi.SCASI.com:0LISTENINGTCPsystems-scasi:ldapsystems-scasi.SCASI.com:0LISTENING TCP systems-scasi:microsoft-ds systems-scasi.SCASI.com:0 LISTENING TCP systems-scasi:kpasswd systems-scasi.SCASI.com:0 LISTENING TCPsystems-scasi:593systems-scasi.SCASI.com:0LISTENINGTCPsystems-scasi:ldapssystems-scasi.SCASI.com:0LISTENING 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 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 UDP systems-scasi:389 *:* UDP systems-scasi:kpasswd *:* UDP *:* systems-scasi:domain UDP systems-scasi:ntp *:* UDP systems-scasi:1036 *:* UDP systems-scasi:3456 *:*

9.2.8 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] ]
       (adapter status) Lists the remote machine's name table given its name
  -a
       (Adapter status) Lists the remote machine's name table given its
  -A
                        IP address.
                        Lists NBT's cache of remote [machine] names and their IP
      (cache)
  -C
 addresses
                        Lists local NetBIOS names.
  -n
      (names)
      (resolved)
                       Lists names resolved by broadcast and via WINS
  -r
  -R (Reload)
                       Purges and reloads the remote cache name table
      (Sessions)
                       Lists sessions table with the destination IP addresses
Lists sessions table converting destination IP
  -S
  -s
      (sessions)
                        addresses to computer NETBIOS names.
  -RR (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refr
esh
              Remote host machine name.
  RemoteName
               Dotted decimal representation of the IP address.
  IP address
  interval
               Redisplays selected statistics, pausing interval seconds
               between each display. Press Ctrl+C to stop redisplaying
               statistics.
```

9.2.9 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=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
```

9.2.10 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:
       19 ms
                 9 ms
                         34 ms
                               10.234.160.1
  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-d6-0.1sanhe3.ca.attbb.net [24.130.64.6]
      11 ms
  5
                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
                12 ms
  7
      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 ms
                        13 ms so-5-3-0.bbr1.losangeles1.level3.net [209.247.9.
      37 ms
 11
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 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 -PO
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)
```

September 22, 2008

```
* -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.
 -PO 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
\star -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 ontqbl.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
```

9.4 Network Load Balancing Manager

Network	c Load Balaı	ncing Mana	iger					_ 8 ×
Eile ⊆luste	r H <u>o</u> st Og	tions <u>H</u> elp						19
E gig Netv	vork Load Bal	ancing Clust	Cluster configurat	ion for all known N	LB clusters			
1.0			Cluster name	1	Cluster IP address	Cluster IP subnet mask	Cluster mode	Remote ci
				1	** 0-			<u> </u>
Log Entry	Date	Time	Cluster	Host	Description	anan da an est		
	1/11/2004	7:15:20 P	M		NLB Manager session	n started		Þ
at Start	🕑 🍠 🦲) 💽 证 ent1 - Micros	oft 🛛 🏹 Admi	inistrative Tools	🖪 Network Lo	ad Balanci	/ 🛃	7:15 PM Sunday

9.5 Routing and Remote Access

Routing and Remote Access					_ 8 ×
Eile Action View Help					
	3				
🚊 Routing and Remote Access	Ports				
Server Status	Name 🗸	Device	Used By	Status	
SYSTEMS-SCASI (local) Ports	WAN Miniport (PPTP) (VPN5-4)	VPN	RAS	Inactive	
Remote Access Clients (0)	WAN Miniport (PPTP) (VPN5-3)	VPN	RAS	Inactive	
	WAN Miniport (PPTP) (VPN5-2)	VPN	RAS	Inactive	
General	WAN Miniport (PPTP) (VPN5-1)	VPN	RAS	Inactive	
Static Routes	WAN Miniport (PPTP) (VPN5-0)	VPN	RAS	Inactive	
DHCP Relay Agent	WAN Miniport (PPPOE) (PPPoE	PPPoE	Routing	Inactive	
IGMP	WAN Miniport (L2TP) (VPN4-4)	VPN	RAS	Inactive	
Remote Access Policies	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	
🥂 Start 🛛 🚱 🥌 💽 🐨				2	7:55 PM
Document1 - Microsof	ft 🛛 🦏 Administrative Tools	🚊 Routing	g and Remote	😰 Routing and Remote Ac	🔊 Sunday

9.6 Sniffers

9.6.1 Sniffer Data Display

ZSUMMARYDDDelta TDDDFrom Toshiba PortableDDDDDDDDDDDDDDDFrom
FCDDDDDDDDDDDDD?
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
@DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
DDDDDDDDDDDDDDDDDDDD
ZDETAILDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
DDDDDDDDDDDDDDDDDD?
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
@DDDDDDDDDDDDDDDDDDDDDDDDDDDFrame 747 of
2046DDDDDDDDDDDDDDDDDDDDDDDDDDDDD
ZHEXDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
DDDDDDDDDDDDDASCIIDDDD?
3 0000 F5 FC 00 44 FA 00 E7 05 FF FF 00 3C 00 11 00 00D
3 0010 00 01 00 00 00 00 FC 04 51 00 00 00 01 00 00Q 3
3 0020 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
@DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
2046DDDDDDDDDDDDDDDDDDDDDDDDDDDD
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

9.6.2 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), Seg=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 = 1511FRAG: XNS: ----- XNS Header -----XNS: XNS: Checksum = FFFF XNS: Length = 60XNS: Transport control = 000000 = Reserved XNS: $\dots 0000 = \text{Hop count}$ XNS: XNS: Packet type = 17 (Novell NetWare) XNS: XNS: Dest net = 00000001, host = 000000000FC, socket = 1105 (NetWare Server) XNS: Source net = 00000001, host = 000000000F5, 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 = 23,0NCP: 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 FC 04 51 00 00 00 01 00 00Q.....
Q.....

 0020 00 00 F5 40 03 22 22 43 07 01 00 17 00 15 00@.""C......
@.""C......

 0030 0A 53 55 50 45 52 56 49 53 4F 52 08 54 45 53 54 .SUPERVISOR.TEST
@ASS

9.7 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.

9.8 Wireless

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

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

9.9 Internet Information Services Manager



9.10 Network Security Audit Program

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

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

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 Event Viewer – Security Log

Event Viewer- Security Log

Event Viewer (Local)	Security 20.029 event(s)							
Application	Туре	Date	Time	Source	Category	Event	User	Compu
Discurity	Failure Audit	1/11/2004	7:07:43 PM	Security	Object Access	560	LOCAL SERVICE	SYSTEM
System	🔒 Failure Audit	1/11/2004	7:06:43 PM	Security	Object Access	560	LOCAL SERVICE	SYSTEM
Directory Service	🔒 Failure Audit	1/11/2004	7:06:43 PM	Security	Object Access	560	LOCAL SERVICE	SYSTEM
DNS Server	Success Audit	1/11/2004	7:06:01 PM	Security	Logon/Logoff	538	SYSTEM	SYSTEM
File Replication Service	🔒 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	SYSTE
	Success Audit	1/11/2004	7:04:02 PM	Security	Directory Service Acc	566	Administrator	SYSTE
	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	SYSTE
	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
	Ar	111120004	7.00.F0 PM	C	Disease Constant Are	F//	A desta de la composition de l	CUCTE
								Þ

10.1.3 Security Log Settings

Audit Policy

http://www.commainweighter.com/actions	5		
Eile Action View Help			
⇔ → 🗈 🖪 😼 🔮			
📴 Security Settings	Policy A	Policy Setting	[
Account Policies Local	Audit account logon events Audit account management Audit directory service access Audit logon events Audit object access Audit policy change Audit privilege use Audit process tracking Audit system events	Success, Failure Success, Failure Success, Failure Success, Failure Success, Failure Success, Failure Success, Failure Success, Failure Success, Failure	
 ▲ ▲ Start ● ● ● ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲	Directory 😋 Ci\Documents a 🛐 B	vent Viewer	2 🛱 🖏 🗊 🐼 2:19 PM





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 [/1] [/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 ΙP Scan named IP address. IP-IP /r Scan named IP addresses range. /listfile Scan named IP address or computer file 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). Show only updates approved on the /wa 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. Output XML file name template. /0 filename Default: %D% - %C% (%T%). Don't display scan progress. /qp Don't display the report by default /at following a single-computer scan. Don't display error list. /qe Don't display report list. /qr /q Do not display any of the preceding items. /unicode Output Unicode. /u username Scan using the specified username. Scan using the specified password. password /p

September 22, 2008

/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
/1		List all reports available.
/1s		List reports from the latest scan.
/lr	filename	Display overview report.
/1d	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 /n Passo MBSACLI /d MyDor MBSACLI /target MBSACLI /r 200.0 MBSACLI /listfii MBSACLI /listfii MBSACLI /ld "Dor MBSACLI /catalog MBSACLI /wa MBSACLI /wa	word+IIS+OS+SQL main 200.0.0.1 0.0.1-200.0.0.50 Le export.txt main - Computer (C ults.txt g c:\wsusscn2.cab /catalog c:\temp\	3-01-2002 12-00 AM)" /nai /nvc wsusscn2.cab /unicode >results.xml

10.2.2 Baseline Security Analyzer Output

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

Computer name: SYSCONSEC\ONTLTO1

IP address: 10.42.100.2

Security report name: SYSCONSEC - ONTLTO1 (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

Issue: Missing | Security Update for Office 2003 (KB914455) | Moderate |
```
Security Update for Publisher 2003 (KB894542) | Important | MS06-054 | Missing | 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 | 1 | 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 | MS04-043 | Installed | Security Update for Windows XP (KB873339) | Important | | MS04-041 | Installed | Security Update for Windows XP (KB885836) | Important | | MS05-007 | Installed | Security Update for Windows XP (KB888302) | Important | MS05-009 | Installed | Security Update for Windows Messenger (KB887472) | Moderate | | MS05-013 | Installed | Security Update for Windows XP (KB891781) | Important | 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 |

September 22, 2008

<pre>(HES9992) Important S00-44 Francisk Security Update for Window XF WES9593) Moderate X039-43 Installed Security Update for Window XF WES9593 Moderate X039-43 Installed Security Update for Window XF WES9593 Installed X039-43 Installed Security Update for Window XF WES9593 Installed X039-44 Installed Security Update for Window XF WES9593 Installed X039-44 Installed Security Update for Window XF WES9593 Installed X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed Security Update for Window XF WES9579 Important X039-46 Installed </pre>		MS05-041	Installed	Beta 6.2 Installer version Security Update for Windows XP
<pre>important important i</pre>	(KB899591) Important	MODE 041		L Occupitor Undets for Windows VD (VD000501) L Madamata L
<pre>i H05-053 installed Security Optic for Kindow SP (R050420) Teportant H05-053 installed Security Update for Kindow SP (R050400) Teportant H05-053 installed Security Update for Kindow SP (R050400) Teportant H05-053 installed Security Update for Kindow SP (R050414) Moderate H05-053 installed Security Update for Kindow SP (R050414) Moderate H05-053 installed Security Update for Kindow SP (R050414) Moderate H05-053 installed Security Update for Kindow SP (R050414) Urtical H05-053 installed Security Update for Kindow SP (R050414) Urtical H05-051 installed Security Update for Kindow SP (R050414) Urtical H05-051 installed Security Update for Kindow SP (R050414) Urtical H05-051 installed Security Update for Kindow SP (R050431) Urtical H05-051 installed Security Update for Kindow SP (R050431) Urtical H05-051 installed Security Update for Kindow SP (R050431) Urtical H05-051 installed Security Update for Kindow SP (R050431) Urtical H05-051 installed Security Update for Kindow SP (R050431) Urtical H05-051 installed Security Update for Kindow SP (R050431) Urtical H05-051 installed Security Update for Kindow SP (R050431) Urtical H05-051 installed Security Update for Kindow SP (R050431) Urtical H05-051 installed Security Update for Kindow SP (R050431) Urtical H05-051 installed Security Update for Kindow SP (R050438) Urtical H05-051 installed Security Update for Kindow SP (R050438) Urtical H05-051 installed Security Update for Kindow SP (R050438) Urtical H05-051 installed Security Update for Kindow SP (R050438) Urtical H05-051 installed Security Update for Kindow SP (R050438) Urtical H05-051 installed Security Update for Kindow SP (R050438) Urtical H05-051 installed Security Update for Kindow SP (R050438) Urtical H05-051 installed Security Update for Kindow SP (R050438) Urtical H05-051 installed Security Up</pre>		MS05-041	Installed	Security Update for Windows XP (KB899591) Moderate
<pre>i 800-001 installed j Becurity Optic for Windows XP (R000200) i Important </pre>		MS05-043	Installed	Security Update for Windows XP (KB896423) Critical
<pre>i M03-040 Teatalled Security Optate for Window XP (MS00107) Teating </pre>		MS05-051	Installed	Security Update for Windows XP (KB902400) Important
<pre>km03-643 [head-line] Security Optice for Windows YP (KS03544) [Monotant] km03-643 [head-line] Security Optice for Windows YP (KS035749) [Important] km03-643 [head-line] Security Optice for Windows YP (KS035749) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS035749) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS035749) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS035749) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS035749) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS035749) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS03574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS04574) [Opticant] km03-640 [head-line] Security Optice for Windows YP (KS0</pre>		MS05-048	Installed	Security Update for Windows XP (KB901017) Important
<pre>i M030-047 i Installed i Security Update for Windows XP (M030723) i Tmportant </pre>		MS05-045	Installed	Security Update for Windows XP (KB905414) Moderate
<pre> Mc03=049 Tabilled Security Update for Windows XP (M200020) Table11 Mc00=051 Tabilled Security Update for Windows XP (M200400) Table11 Mc00=051 Tabilled Security Update for Windows XP (M201100) Tmportant Mc00=061 Table1100 Security Update for Windows XP (M201100) Tmportant Mc00=061 Table1100 Security Update for Windows XP (M201100) Tmportant Mc00=061 Table1100 Security Update for Windows XP (M201100) Tmportant Mc00=061 Table1100 Security Update for Windows XP (M201100) Tmportant Mc00=061 Table1100 Security Update for Windows XP (M201100) Cfitical Mc00=011 Table1100 Security Update for Windows XP (M201100) Cfitical Mc00=012 Table1100 Security Update for Windows XP (M201100) Cfitical Mc00=012 Table1100 Security Update for Windows XP (M201100) Cfitical Mc00=012 Table1100 Security Update for Windows XP (M201100) Cfitical Mc00=012 Table1100 Security Update for Windows XP (M201100) Tmportant Mc00=012 Table1100 Security Update for Windows XP (M201200) Cfitical Mc00=012 Table1100 Security Update for Windows XP (M201200) Table110 Mc00=012 Table1100 Security Update for Windows XP (M201200) Table110 Mc00=012 Table1100 Security Update for Windows XP (M201200) Tmportant Mc00=013 Table1100 Security Update for Windows XP (M201200) Tmportant Mc00=014 Table1100 Security Update for Windows XP (M201200) Tmportant Mc00=014 Table1100 Security Update for Windows XP (M201200) Tmportant Mc00=014 Table1100 Security Update for Windows XP (M201200) Tmportant Mc00=014 Table1100 Security Update for Windows XP (M201200) Tmportant Mc00=014 Table1100 Security Update for Windows XP (M201200) Tmportant Mc00=015 Table1100 Security Update for Windows XP (M201200) Tmportant Mc00=016 Table1100 Security Update for Windows XP (M201200) Tmportant Mc00=016 Table1100 Security Update for Windows XP (M20</pre>		MS05-047	Installed	Security Update for Windows XP (KB905749) Important
<pre> M000-033 Installed Security Update for Windows XP (M009406) Critical M000-033 Installed Security Update for Windows XP (M009406) Critical M000-038 Installed Security Update for Windows XP (M001100) Inportant M000-016 Installed Security Update for Windows XP (M001100) Important M000-016 Installed Security Update for Windows XP (M001100) Important M000-016 Installed Security Update for Windows XP (M001100) Important M000-016 Installed Security Update for Windows XP (M001100) Critical M000-016 Installed Security Update for Windows XP (M001100) Critical M000-016 Installed Security Update for Windows XP (M001100) Critical M000-017 Installed Security Update for Windows XP (M001100) Critical M000-018 Installed Security Update for Windows XP (M001300) Critical M000-012 Installed Security Update for Windows XP (M001300) Critical M000-012 Installed Security Update for Windows XP (M001300) Critical M000-013 Installed Security Update for Windows XP (M001300) Critical M000-013 Installed Security Update for Windows XP (M001300) Critical M000-013 Installed Security Update for Windows XP (M001300) Important M000-013 Installed Security Update for Windows XP (M001300) Important M000-014 Installed Security Update for Windows XP (M001300) Important M000-015 Installed Security Update for Windows XP (M001300) Important M000-016 Installed Security Update for Windows XP (M0001400) Important M000-016 Installed Security Update for Windows XP (M0012000) Important M000-016 Installed Security Update for Windows XP (M0022014) Critical M000-016 Installed Security Update for Windows XP (M0022014) Critical M000-016 Installed Security Update for Windows XP (M0022014) Critical M000-016 Installed Security Update for Windows XP (M0022014) Critical M000-016 Installed Security Update for Windows XP (M0022014) Critical M000-016 Installed</pre>		MS05-049	Installed	Security Update for Windows XP (KB900725) Important
<pre>setup = setup = s</pre>		MS05-053	Installed	Security Update for Windows XP (KB896424) Critical
<pre>critical minimum security Update for Windows XP (RS911327) Important </pre>		MS05-050	Installed	Security Update for Windows XP (KB904/06) Critical
<pre>HSD0-000 Intelled Security Update for Windows Y# (WSD120) Important HSD0-000 Intelled Security Update for Windows Media Player Plug-in (WSD1564) HSD0-006 Intelled Cumulative Security Update for Outlook Express for Windows XP (HSD11567) Important HSD0-016 Intelled Security Update for Windows Y# (HSD1531) Critical HSD0-018 Intelled Security Update for Windows Y# (HSD1531) Critical HSD0-019 Intelled Security Update for Windows Y# (HSD1531) Critical HSD0-010 Intelled Security Update for Windows Y# (HSD1531) Critical HSD0-023 Intelled Security Update for Windows Y# (HSD1531) Critical HSD0-023 Intelled Security Update for Windows Y# (HSD1531) Important HSD0-023 Intelled Security Update for Windows Y# (HSD1531) Important HSD0-023 Intelled Security Update for Windows Y# (HSD1531) Important HSD0-023 Intelled Security Update for Windows Y# (HSD1531) Important HSD0-024 Intelled Security Update for Windows Y# (HSD1531) Important HSD0-024 Intelled Security Update for Windows Y# (HSD1531) Important HSD0-024 Intelled Security Update for Windows Y# (HSD1531) Important HSD0-024 Intelled Security Update for Windows Y# (HSD1531) Important HSD0-024 Intelled Security Update for Windows Y# (HSD1531) Important HSD0-025 Intelled Security Update for Windows Y# (HSD1531) Important HSD0-026 Intelled Security Update for Windows Y# (HSD1531) Important HSD0-026 Intelled Security Update for Windows Y# (HSD1531) Important HSD0-026 Intelled Security Update for Windows Y# (HSD1531) Important HSD0-026 Intelled Security Update for Windows Y# (HSD1531) Critical HSD0-026 Intelled Security Update for Windows Y# (HSD1531) Critical HSD0-026 Intelled Security Update for Windows Y# (HSD1531) Critical HSD0-026 Intelled Security Update for Windows Y# (HSD1533) Critical HSD0-026 Intelled Security Update for Windows Y# (HSD1533) Critical HSD0-026 I</pre>		MS06-002	Installed	Security Update for Windows XP (KB900519) Critical
<pre>1 3006-009 Installed Security Update for Windows Xe (KS911562) Important </pre>		MS06-008	Installed	Security Update for Windows XP (KB911927) Important
<pre>NB06-006 Tatalled Security Update for Nindows Media Player Plug-in (NB911564) Tmportant </pre>		MS06-009	Installed	Security Update for Windows XP (KB901190) Important
<pre>Tmportant M006-016 Installed Cumulative Security Update for Outlook Express for Windows XP (R3911567) Important M006-016 Installed Security Update for Windows XP (KM911662) Critical M006-021 Installed Security Update for Windows XP (KM911662) Critical M006-023 Installed Security Update for Windows XP (KM917043) Critical M006-023 Installed Security Update for Windows XP (KM917043) Critical M006-023 Installed Security Update for Windows XP (KM917043) Critical M006-023 Installed Security Update for Windows XP (KM917043) Critical M006-023 Installed Security Update for Windows XP (KM917043) Critical M006-023 Installed Security Update for Windows XP (KM917043) Critical M006-023 Installed Security Update for Windows XP (KM917043) Critical M006-023 Installed Security Update for Windows XP (KM917043) Critical M006-023 Installed Security Update for Windows XP (KM917043) Critical M006-024 Installed Security Update for Windows XP (KM920173) Critical M006-025 Installed Security Update for Windows XP (KM920173) Critical M006-026 Installed Security Update for Windows XP (KM920173) Critical M006-027 Installed Security Update for Windows XP (KM920174) Critical M006-026 Installed Security Update for Windows XP (KM920174) Critical M006-027 Installed Security Update for Windows XP (KM920174) Critical M006-027 Installed Security Update for Windows XP (KM920174) Critical M006-027 Installed Security Update for Windows XP (KM920174) Critical M006-027 Installed Security Update for Windows XP (KM920174) Critical M006-027 Installed Security Update for Windows XP (KM920174) Critical M006-027 Installed Security Update for Windows XP (KM920174) Critical M006-027 Installed Security Update for Windows XP (KM920174) Critical M006-027 Installed</pre>		MS06-006	Installed	Security Update for Windows Media Player Plug-in (KB911564)
<pre>(HS911567) Important HS95-016 Installed Cemulative Security Update for Windows XP (HS911562) Critical HS95-015 Hstalled Security Update for Windows XP (HS91562) Critical HS95-015 HS12164 Security Update for Windows XP (HS91562) Critical HS95-015 HS12164 Security Update for Windows XP (HS91562) Critical HS95-015 HS12164 Security Update for Windows XP (HS91563) Critical HS95-015 HS12164 Security Update for Windows XP (HS91563) Critical HS95-015 HS12164 Security Update for Windows XP (HS91563) HS97-141 HS95-015 HS12164 Security Update for Windows XP (HS91563) LS97 HS97-141 HS95-015 HS12164 Security Update for Windows XP (HS915753) HS97-141 HS95-015 HS12164 Security Update for Windows XP (HS915753) HS97-141 HS95-050 HS12164 Security Update for Windows XP (HS91763) HS97-141 HS95-050 HS12164 Security Update for Windows XP (HS917673) HS97-141 HS95-050 HS12164 Security Update for Windows XP (HS917673) HS97-141 HS95-050 HS12164 Security Update for Windows XP (HS917673) HS97-141 HS95-050 HS12164 Security Update for Windows XP (HS917673) HS97-141 HS95-050 HS12164 Security Update for Windows XP (HS917673) HS97-141 HS95-050 HS12164 Security Update for Windows XP (HS917773) Critical HS95-050 HS12164 Security Update for Windows XP (HS920763) HS97-141 HS95-050 HS12164 Security Update for Windows XP (HS920763) HS97-141 HS95-050 HS12164 Security Update for Windows XP (HS920768) MS67-161 HS97-161 HS97-160 HS97-160 </pre>	Important			
<pre>(KB911567) Important </pre>		MS06-016	Installed	Cumulative Security Update for Outlook Express for Windows XP
<pre> Mode-oid Installed Security Update for Windows XP (KB90833) Critical Mode-oid Installed Security Update for Windows XP (KB90833) Critical Mode-oid Installed Security Update for Windows XP (KB91733) Critical Mode-oid Installed Security Update for Windows XP (KB91733) Critical Mode-oid Installed Security Update for Windows XP (KB91733) Lew Mode-oid Installed Security Update for Windows XP (KB91733) Important Mode-oid Installed Security Update for Windows XP (KB91733) Important Mode-oid Installed Security Update for Windows XP (KB91733) Important Mode-oid Installed Security Update for Windows XP (KB91733) Important Mode-oid Installed Security Update for Windows XP (KB91733) Important Mode-oid Installed Security Update for Windows XP (KB91742) Critical Mode-oid Installed Security Update for Windows XP (KB91742) Critical Mode-oid Installed Security Update for Windows XP (KB92010) Important Mode-oid Installed Security Update for Windows XP (KB92010) Important Mode-oid Installed Security Update for Windows XP (KB92010) Important Mode-oid Installed Security Update for Windows XP (KB92010) Important Mode-oid Installed Security Update for Windows XP (KB92010) Important Mode-oid Installed Security Update for Windows XP (KB92010) Important Mode-oid Installed Security Update for Windows XP (KB92010) Critical Mode-oid Installed Security Update for Windows XP (KB92010) Critical Mode-oid Installed Security Update for Windows XP (KB92010) Critical Mode-oid Installed Security Update for Windows XP (KB92010) Critical Mode-oid Installed Security Update for Windows XP (KB92010) Critical Mode-oid Installed Security Update for Windows XP (KB92010) Critical Mode-oid Installed Security Update for Windows XP (KB92010) Critical Mode-oid Installed Security Update for Windows XP (KB9</pre>	(KB911567) Important			
<pre>NBUB-015 Installed Security Update for Windows Media Player 9 (MB91734) Critical </pre>		MS06-014	Installed	Security Update for Windows XP (KB911562) Critical
<pre>critical </pre>		MS06-015	Installed	Security Update for Windows XP (KB908531) Critical
<pre>critical NS06-003 restalled Security Update for Nindows XP (NS017344) Critical NS06-003 Installed Security Update for Nindows XP (NS017350) Important NS06-005 Installed Security Update for Nindows XP (NS017350) Important NS06-005 Installed Security Update for Nindows XP (NS017350) Important NS06-005 Installed Security Update for Nindows XP (NS017350) Important NS06-005 Installed Security Update for Nindows XP (NS017450) Important NS06-005 Installed Security Update for Nindows XP (NS017450) Important NS06-001 Installed Security Update for Nindows XP (NS027650) Important NS06-001 Installed Security Update for Nindows XP (NS027650) Important NS06-003 Installed Security Update for Nindows XP (NS027650) Important NS06-003 Installed Security Update for Nindows XP (NS027650) Important NS06-003 Installed Security Update for Nindows XP (NS027650) Important NS06-003 Installed Security Update for Nindows XP (NS027650) Important NS06-003 Installed Security Update for Nindows XP (NS027650) Moderate NS06-003 Installed Security Update for Nindows XP (NS027650) Moderate NS06-003 Installed Security Update for Nindows XP (NS027650) Moderate NS06-003 Installed Security Update for Nindows XP (NS027650) Moderate NS06-003 Installed Security Update for Nindows XP (NS027650) Moderate NS06-003 Installed Security Update for Nindows XP (NS027650) Moderate NS06-004 Installed Security Update for Nindows XP (NS027650) Moderate NS06-007 Installed Security Update for Nindows XP (NS027650) Moderate NS06-007 Installed Security Update for Nindows XP (NS027650) Moderate NS06-006 Installed Security Update for Nindows XP (NS027650) Critical NS06-006 Installed Security Update for Nindows XP (NS027650) Critical NS06-006 Installed Security Update for Nindows XP (NS027579) Critical NS06-066 Installed Security Update for Nindows XP (NS027579) C</pre>		MS06-024	Installed	Security Update for Windows Media Player 9 (AB91/734) Critical
<pre>(MS06-022 Installed Security Update for Windows XP (KS918436) Critical </pre>		MS06-023	Installed	Security Undate for Windows XP (KB917344) Critical
<pre>NB00-019 Installed Security Update for Windows XP (KB913500) Low NB00-025 Installed Security Update for Windows XP (KB911280) Important NB00-025 Installed Security Update for Windows XP (KB911280) Critical NB00-025 Installed Security Update for Windows XP (KB91722) Critical NB00-025 Installed Security Update for Windows XP (KB92070) Important NB00-025 Installed Security Update for Windows XP (KB92070) Important NB00-025 Installed Security Update for Windows XP (KB920214) Critical NB00-025 Installed Security Update for Windows XP (KB920214) Critical NB00-025 Installed Security Update for Windows XP (KB920214) Critical NB00-025 Installed Security Update for Windows XP (KB920214) Critical NB00-025 Installed Security Update for Windows XP (KB920466) Critical NB00-025 Installed Security Update for Windows XP (KB920466) Critical NB00-025 Installed Security Update for Windows XP (KB920466) Critical NB00-025 Installed Security Update for Windows XP (KB920466) Critical NB00-026 Installed Security Update for Windows XP (KB92046) Critical NB00-026 Installed Security Update for Windows XP (KB92046) Critical NB00-026 Installed Security Update for Windows XP (KB920470) Low NB00-070 Installed Security Update for Windows XP (KB920470) Low NB00-070 Installed Security Update for Windows XP (KB920470) Low NB00-070 Installed Security Update for Windows XP (KB920470) Low NB00-070 Installed Security Update for Windows XP (KB920470) Low NB00-070 Installed Security Update for Windows XP (KB920470) Low NB00-070 Installed Security Update for Windows XP (KB920470) Low NB00-070 Installed Security Update for Internet Explorer for Windows XP (KB92040) - NB00-066 Installed Security Update for Windows XP (KB920470) Low NB00-070 Installed Security Update for Windows XP (KB920470) Important NB00-066 Installed Security Update for Wi</pre>		MS06-022	Installed	Security Update for Windows XP (KB918439) Critical
<pre>(M900-032 Testalled Security Update for Windows XP (K9917953) Important M900-035 Testalled Security Update for Windows XP (K9914368) Critical M900-051 Testalled Security Update for Windows XP (K991422) Critical M900-051 Testalled Security Update for Windows XP (K9920670) Important M900-051 Testalled Security Update for Windows XP (K9920670) Important M900-051 Testalled Security Update for Windows XP (K9920670) Testalled M900-051 Testalled Security Update for Windows XP (K992061) Critical M900-053 Testalled Security Update for Windows XP (K992065) Moderate M900-053 Testalled Security Update for Windows XP (K992065) Moderate M900-053 Testalled Security Update for Windows XP (K992070) Temportant M900-055 Testalled Security Update for Windows XP (K9920440) Temportant M900-055 Testalled Security Update for Windows XP (K9920440) Moderate M900-057 Testalled Security Update for Windows XP (K9920410) Critical M900-056 Testalled Security Update for Windows XP (K9920710) Critical M900-057 Testalled Security Update for Windows XP (K9920710) Critical M900-056 Testalled Security Update for Windows XP (K9920710) Critical M900-057 Testalled Security Update for Windows XP (K9920710) Critical M900-056 Testalled Security Update for Windows XP (K9920710) Critical M900-057 Testalled Security Update for Windows XP (K992070) Critical M900-056 Testalled Security Update for Windows XP (K992070) Critical M900-056 Testalled Security Update for Windows XP (K992070) Critical M900-056 Testalled Security Update for Windows XP (K992070) Critical M900-056 Testalled Security Update for Windows XP (K992070) Critical M900-056 Testalled Security Update for Windows XP (K992070) Testal M900-056 Testalled Security Update for Windows XP (K992070) Testal </pre>		MS06-018	Installed	Security Update for Windows XP (KB913580) Low
<pre>(MS06-025 Installed Security Update for Windows XP (KB911280) Important </pre>		MS06-032	Installed	Security Update for Windows XP (KB917953) Important
<pre> MS06-036 Installed Security Update for Windows XP (KB914388) Critical MS06-050 Installed Security Update for Windows XP (KB920670) Important MS06-045 Installed Security Update for Windows XP (KB921398) Moderate MS06-046 Installed Security Update for Windows XP (KB921398) Moderate MS06-043 Installed Security Update for Windows XP (KB920670) Important MS06-043 Installed Security Update for Windows XP (KB9202616) Critical MS06-053 Installed Security Update for Windows XP (KB920676) Moderate MS06-053 Installed Security Update for Windows XP (KB920676) Moderate MS06-053 Installed Security Update for Windows XP (KB920676) Moderate MS06-053 Installed Security Update for Windows XP (KB920466) Ortical MS06-057 Installed Security Update for Windows XP (KB92146) Tritical MS06-057 Installed Security Update for Windows XP (KB92146) Moderate MS06-057 Installed Security Update for Windows XP (KB921410) Critical MS06-056 Installed Security Update for Windows XP (KB921410) Critical MS06-057 Installed Security Update for Windows XP (KB921410) Critical MS06-057 Installed Security Update for Windows XP (KB921410) Critical MS06-056 Installed Security Update for Windows XP (KB921410) Low MS06-057 Installed Security Update for Windows XP (KB921470) Low MS06-056 Installed Security Update for Windows XP (KB92170) Low MS06-056 Installed Security Update for Flash Player (KB923780) Critical MS06-056 Installed Security Update for Windows XP (KB923780) Critical MS06-056 Installed Security Update for Windows XF (KB923780) Important MS06-056 Installed Security Update for Windows XF (KB923780) Critical MS06-056 Installed Security Update for Windows XF (KB923780) Important MS06-056 Installed Security Update for Windows XF (KB923780) Important MS06-056 Installed Security Update for Windows</pre>		MS06-025	Installed	Security Update for Windows XP (KB911280) Important
<pre>(MS06-051 Installed Security Update for Windows XP (KB917422) Critical MS06-041 Installed Security Update for Windows XP (KB920670) Important MS06-046 Installed Security Update for Windows XP (KB921398) Moderate MS06-046 Installed Security Update for Windows XP (KB921398) Moderate MS06-043 Installed Security Update for Windows XP (KB92061) Important MS06-052 Installed Security Update for Windows XP (KB92065) Moderate MS06-053 Installed Security Update for Windows XP (KB920466) Critical MS06-053 Installed Security Update for Windows XP (KB920465) Moderate MS06-055 Installed Security Update for Windows XP (KB920465) Moderate MS06-055 Installed Security Update for Windows XP (KB920416) Critical MS06-056 Installed Security Update for Windows XP (KB920419) Critical MS06-057 Installed Security Update for Windows XP (KB920419) Critical MS06-061 Installed Security Update for Windows XP (KB920419) Critical MS06-061 Installed Security Update for Windows XP (KB920419) Critical MS06-061 Installed Security Update for Windows XP (KB920419) Critical MS06-070 Installed Security Update for Windows XP (KB920419) Critical MS06-070 Installed Security Update for Windows XP (KB920470) Low MS06-070 Installed Security Update for Windows XP (KB920470) Low MS06-067 Installed Security Update for Windows XP (KB920470) Low MS06-066 Installed Security Update for Mindows XP (KB92078) Critical MS06-066 Installed Security Update for Windows XP (KB92078) Critical MS06-066 Installed Security Update for Mindows XP (KB92078) Critical MS06-066 Installed Security Update for Mindows XP (KB92078) Critical MS06-066 Installed Security Update for Windows XP (KB92078) Critical MS06-066 Installed Security Update for Windows XP (KB92078) Critical MS06-066 Installed Security Update for Windows XP (KB92078) Critical MS06-066 Installed Security Update</pre>		MS06-036	Installed	Security Update for Windows XP (KB914388) Critical
<pre> MS06-US0 Installed Security Update for Windows XP (KB920683) Critical </pre>		MS06-051	Installed	Security Update for Windows XP (KB917422) Critical
<pre>(Hasde-Ori Installed Security Update for Windows XF (KB921398) Moderate MS06-046 Installed Security Update for Windows XF (KB921398) Moderate MS06-033 Installed Security Update for Windows XF (KB921391) Important MS06-052 Installed Security Update for Windows XF (KB920685) Moderate MS06-055 Installed Security Update for Windows XF (KB920685) Moderate MS06-056 Installed Security Update for Windows XF (KB923968) Critical MS06-056 Installed Security Update for Windows XF (KB924685) Moderate MS06-056 Installed Security Update for Windows XF (KB924968) Moderate MS06-066 Installed Security Update for Windows XF (KB92496) Moderate MS06-066 Installed Security Update for Windows XF (KB92491) Critical MS06-066 Installed Security Update for Windows XF (KB924191) Critical MS06-066 Installed Security Update for Windows XF (KB922191) Critical MS06-066 Installed Security Update for Windows XF (KB922191) Critical MS06-067 Installed Security Update for Windows XF (KB922303) Critical MS06-066 Installed Security Update for Windows XF (KB922378) Critical MS06-066 Installed Cumulative Security Update for Internet Explorer for Windows XF (KB922760) Critical MS06-066 Installed Security Update for Windows XF (KB923789) Critical MS06-066 Installed Security Update for Windows XF (KB923980) Important Operating System Scan Results Administrative Vulnerabilities Issue: Local Account Password Test Score: Check passed Result: Some user accounts (l of 4) have blank or simple passwords, or could not be analyzed. Detail: User Weak Password Locked Out Disabled SubFORT 388945a0 - - Disabled SubFORT 388945a0 - - Disabled SubFORT 388945a0 - - Disabled zadmin - - - Disabled zadmin - - - Disabled zadmin - - - Disabled SubFORT 388945a0 - Disabled SubFORT 388945a0 - - Disabl</pre>		MS06-050	Installed	Security Update for Windows XP (KB920670) Important
<pre>critical </pre>		MS06-041	Installed	Security Update for Windows XP (KB920683) Critical
<pre>Critical </pre>		MS06-046	Installed	Security Undate for Windows XP (KB921556) Moderate
Critical MS06-052 Installed Security Update for Windows XP (KB919007) Important MS06-053 Installed Security Update for Windows XP (KB925466) Critical MS06-065 Installed Security Update for Windows XP (KB923414) Important MS06-065 Installed Security Update for Windows XP (KB923414) Important MS06-065 Installed Security Update for Windows XP (KB923114) Important MS06-066 Installed Security Update for Windows XP (KB924191) Critical MS06-066 Installed Security Update for Windows XP (KB924191) Critical MS06-066 Installed Security Update for Windows XP (KB924191) Critical MS06-066 Installed Security Update for Windows XP (KB92470) Low MS06-070 Installed Security Update for Windows XP (KB92470) Low MS06-070 Installed Security Update for Windows XP (KB92470) Low MS06-070 Installed Security Update for Internet Explorer for Windows XP (KB922760) Critical MS06-066 Installed Cumulative Security Update for Internet Explorer for Windows XP (KB922760) Critical MS06-066 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 (l of 4) have blank or simple passwords, or could not be analyzed. Detail: User Weak Password Locked Out Disabled Guest Weak Password Locked Out Disabled SUPPORT_38945a0 - - Disabled Issue: File System Score: Check passed		MS06-043	Installed	Security Update for Outlook Express for Windows XP (KB920214)
<pre> MS06-053 Installed Security Update for Windows XP (KB919007) Important MS06-053 Installed Security Update for Windows XP (KB925486) Critical MS06-063 Installed Security Update for Windows XP (KB923414) Important MS06-063 Installed Security Update for Windows XP (KB923414) Important MS06-063 Installed Security Update for Windows XP (KB923191) Critical MS06-061 Installed Security Update for Windows XP (KB922191) Critical MS06-0661 Installed Security Update for Windows XP (KB922191) Critical MS06-0661 Installed Security Update for Windows XP (KB92213) Critical MS06-0661 Installed Security Update for Windows XP (KB92213) Critical MS06-0701 Installed MSXU4 4.0 SP2 Security Update (KB927978) Critical MS06-067 Installed MSXU4 4.0 SP2 Security Update for Internet Explorer for Windows XP (KB922760) Critical MS06-066 Installed Security Update for Flash Player (KB923789) Critical MS06-066 Installed Security Update for Windows XP (KB923980) Important MS06-066 Installed Security Update for Windows XP (KB923980) Important MS06-066 Installed Security Update for Vindows XP (KB923980) Important MS06-066 Installed Security Update for Vindows XP (KB923980) Important MS06-066 Installed Security Update for Windows XP (KB923980) Important MS06-066 Installed Security Update for Windows XP (KB923980) Important MS06-066 Installed Security Update for Windows XP (KB923980) Important MS06-066 Installed Security Update for Windows XP (KB923980) Important MS06-067 Installed Security Update for Windows XP (KB923980) Important MS06-068 Installed Security Update for Windows XP (KB923980) Important MS06-066 Installed Security Update for Windows XP (KB923980) Important MS06-067 Installed Security Update for Windows XP (KB923980) Important MS06-068 Installed Security Update for Windows XP (KB923980)</pre>	Critical		•	
<pre> MS06-055 Installed Security Update for Windows XP (KB920655) Moderate MS06-065 Installed Security Update for Windows XP (KB92344) Important MS06-065 Installed Security Update for Windows XP (KB923161) Critical MS06-061 Installed Security Update for Windows XP (KB923191) Critical MS06-061 Installed Security Update for Windows XP (KB922191) Critical MS06-064 Installed Security Update for Windows XP (KB922191) Critical MS06-064 Installed Security Update for Windows XP (KB922191) Critical MS06-070 Installed Security Update for Windows XP (KB92210) Low MS06-070 Installed Security Update for Windows XP (KB92210) Low MS06-071 Installed MSXML 4.0 SP2 Security Update (KB927976) Critical MS06-071 Installed Windows Malicious Software Removal Tool - November 2006 (KB890830) MS06-067 Installed Cumulative Security Update for Internet Explorer for Windows XP (KB922760) Critical MS06-066 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 HelpAssistant - - Disabled JSuperT.38894520 - - Disabled JSuperT.38894520 - - Disabled JSuperT.38894520 - - Disabled Zadmin - - - Disabled Zadmin -</pre>		MS06-052	Installed	Security Update for Windows XP (KB919007) Important
<pre> MS06-055 Installed Security Update for Windows XP (KB925486) Critical MS06-053 Installed Security Update for Windows XP (KB924191) Critical MS06-057 Installed Security Update for Windows XP (KB924191) Critical MS06-057 Installed Security Update for Windows XP (KB92191) Critical MS06-064 Installed Security Update for Windows XP (KB92013) Critical MS06-0701 Installed Security Update for Windows XP (KB920213) Critical MS06-0701 Installed Security Update for Windows XP (KB920213) Critical MS06-0701 Installed Security Update for Windows XP (KB920213) Critical MS06-0701 Installed Security Update for Windows XP (KB920213) Critical MS06-0701 Installed WSXML 4.0 SP2 Security Update (Step22708) Critical MS06-0701 Installed Windows Malicious Software Removal Tool - November 2006 (KB990830) MS06-067 Installed Security Update for Flash Player (KB923789) Critical MS06-066 Installed Security Update for Windows XP (KB923789) Critical MS06-066 Installed Security Update for Windows XP (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 pased Result: Some user accounts (1 of 4) have blank or simple passwords, or could not be analyzed. Detail:</pre>		MS06-053	Installed	Security Update for Windows XP (KB920685) Moderate
<pre>(MS06-063 Installed Security Update for Windows XP (KB924496 Moderate </pre>		MS06-055	Installed	Security Update for Windows XP (KB925486) Critical
<pre>(KB922760) Installed Security Update for Windows XP (KB923191) Critical </pre>		MS06-063	Installed	Security Update for Windows XP (KB923414) Important
<pre>(H000 0.0 Installed Security Update for Windows XP (KB924191) Critical </pre>		MS06-065	Installed	Security Update for Windows XP (KB923191) Moderate
<pre>(HSOG-064 Installed Security Update for Windows XP (KB922013) Low </pre>		MS06-057	Installed	Security Undate for Windows XP (KB923191) Critical
<pre> MS06-068 Installed Security Update for Windows XP (KB920213) Critical MS06-070 Installed Security Update for Windows XP (KB924270) Low MS06-070 Installed MSXML 4.0 SP2 Security Update (KB92778) 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 MS06-066 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</pre>		MS06-064	Installed	Security Update for Windows XP (KB922819) Low
<pre> 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 MS06-066 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 (l 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</pre>		MS06-068	Installed	Security Update for Windows XP (KB920213) Critical
<pre> 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 MS06-066 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 Issue: File System Score: Check passed</pre>		MS06-070	Installed	Security Update for Windows XP (KB924270) Low
<pre> 890830 Installed Windows Malicious Software Removal Tool - November 2006 (KB890830) MS06-067 Installed Cumulative Security Update for Internet Explorer for Windows XP (KB922760) Critical MS06-066 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</pre>		MS06-071	Installed	MSXML 4.0 SP2 Security Update (KB927978) Critical
<pre>MS06-067 Installed Cumulative Security Update for Internet Explorer for Windows XP (KB922760) Critical </pre>		890830 1	Installed	Windows Malicious Software Removal Tool - November 2006 (KB890830)
<pre>(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</pre>	I	MC06 067	Tratallad	L Cumulative Cocumity Undate for Internet Puplemen for Mindays VD
<pre>(MDD1700) + Official +</pre>	(KB922760) Critical	M300-007	Instatted	Cumulative security opdate for internet Explorer for Windows Ar
<pre>/ MSOG-OGG Installed Socially Optice 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:</pre>	(ID)22700) Criticar	MS06-069	Installed	Security Update for Flash Player (KB923789) Critical
<pre>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:</pre>		MS06-066	Installed	Security Update for Windows XP (KB923980) Important
<pre>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:</pre>				
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 zadmin - - - Issue: File System Score: Check passed				
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 Issue: File System Score: Check passed	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				
<pre>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:</pre>	Administrative Vulne	erabilities		
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 Issue: File System Score: Check passed	Issue Local	Account Pa	seword Test	
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	Score: Check	nassed	.55W010 1050	
Detail: User Weak Password Locked Out Disabled Guest Weak - Disabled HelpAssistant - - Disabled SUPPORT_388945a0 - - Disabled zadmin - - - Issue: File System Score: Check passed	Result: Some	user accoun	ts (1 of 4)	have blank or simple passwords, or could not be analyzed.
Detail: User Weak Password Locked Out Disabled Guest Weak - Disabled HelpAsistant - - Disabled SUPPORT_388945a0 - - Disabled zadmin - - - Issue: File System Score: Check passed			/	· · · · · · · · · · · · · · · · · · ·
User Weak Password Locked Out Disabled Guest Weak - Disabled HelpAssistant - - Disabled SUPPORT_388945a0 - - Disabled zadmin - - - Issue: File System Score: Check passed	Detail	:		
Guest Weak - Disabled HelpAssistant - - Disabled SUPPORT_388945a0 - - Disabled zadmin - - - Issue: File System Score: Check passed		User Wea	ak Password	Locked Out Disabled
HelpAssistant - - Disabled SUPPORT_388945a0 - - Disabled zadmin - - - Issue: File System Score: Check passed		Guest We	eak - Di	isabled
zadmin - - - zadmin - - - Issue: File System Score: Check passed		HeipAssist	tant - -	- Disabled
Issue: File System Score: Check passed		SUFFURI_30 zadmin -	- - -	DISANTER
Score: Check passed	Issue: File	System	1 1 1	
	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 <u>http://la-samhna.de/library/scanners.html</u>.

10.4 Open Source Host Based Intrusion Detection System (OSSEC)

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

10.5 Free PC Audits

<u>http://www.belarc.com/free_download.html?/try/ib.CIS.cg</u>iprovides a free program to profile and review the software on a PC.

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.



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

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

13.3 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 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 the add on security products are used and whether the features are appropriate
- Determine whether the features of the add on security product are implemented properly
- Determine whether the features of the add on security product allow other security features to be circumvented

15 System Management

15.1 Chkdsk

Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp.				
C:\Docume Checks a d	ents and Settings\Rodney>chkdsk /? isk 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),			
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			
/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.			
	(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.				
WARNIN	G! 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) Analyze only -a Force defragmentation even if free space is low -f Verbose output -v -? Display this help text 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>

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

16.2 Application Database Security

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	9
www.Microsoft.com	9
http://www.computerhope.com/history/windows.htm	9
http://www.cisecurity.org/	10
http://www.pcisecuritystandards.com/	10
http://www.us-cert.gov/reading room/	10
http://www.nist.gov/	10
Physical Security	13
http://www.openwall.com/john/	
Active Directory and the Global Catalog	15
Domains, Forests, and Trees	
http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default	t.msp
X	
http://En.Wikipedia.com/Active Directory#Trust	20
Security Settings and Group Policy Objects	22

User Profiles, Groups, and Organizational Units	
http://www.beginningtoseethelight.org/ntsecurity/index.php	
Resource Protections	
Services and Privileged Programs	
www.BlackViper.com	
Network Access	
Logging and Monitoring	
http://la-samhna.de/library/scanners.html	
http://www.ossec.net/wiki/index.php/OSSEC	
http://www.belarc.com/free_download.html?/try/ib.CIS.cgi	
Backup and Contingency Planning.	
Patch Management	
Miscellaneous Tools	
Add On Security Products	
System Management	
Application Security	
http://www.owasp.org/index.php/Main Page	
Other Sources of Information	

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