Resultant Set of Policy Provider

You can connect to Windows Server 2003 domain controller and simulate Resultant Set of Policy (RSoP) for Group Policy settings. The simulation is referred to as planning mode

This service is installed by default but configured to start manually

If disabled, RSop planning mode simulation will not be available

Routing and Remote Access

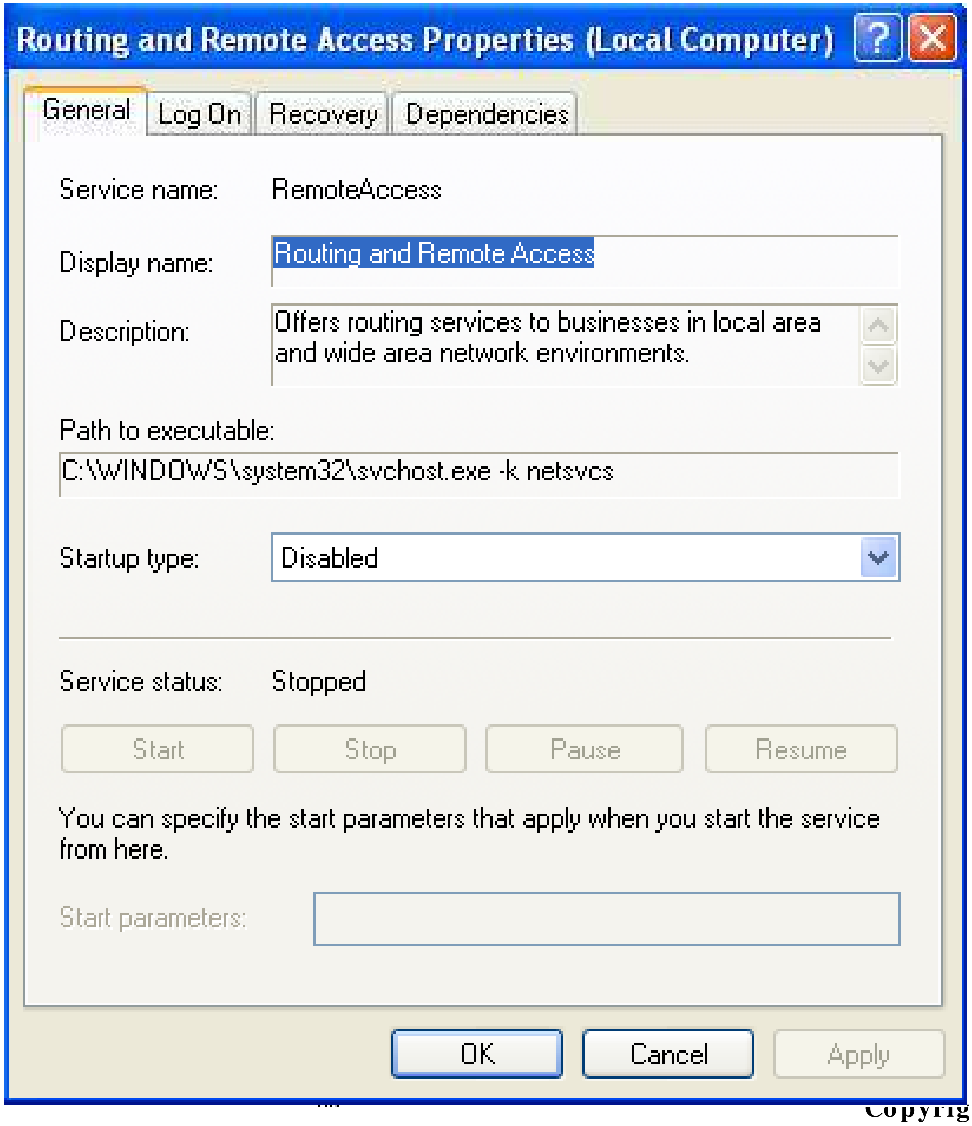
The service provides multi protocol LAN-to-LAN, LAN-to-WAN, VPN and NAT routing services and provides dial-up and VPN remote access services

The service replaces the Routing and Remote Access Service (RRAS) and Remote Access Service (RAS) features in Windows NT 4.0

The service is installed and disabled by default

If disabled the incoming RAS, VPN or dial-on-demand connections, and routing protocols will not be received or transmitted

Routing and Remote Access



Routing and Remote Access Properties (Local Computer)

Service name: RemoteAccess

Display name: Routing and Remote Access

Description: Offers routing services to businesses in local area and wide area network environments.

Path to executable:
C:\WINDOWS\system32\svchost.exe -k netsvcs

Startup type: Disabled

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

SAP Agent

The service advertises network services on an IPX network through the IPX Service Advertising Protocol (SAP).

Features as file and print services depend this service.

It requires NWLINK IPX/SPX Compatible Transport protocol, and not installed by default.

If disabled, the reference features may not work properly.

Secondary Logon

Users can create processes with different security principals with the help of this service

A restricted user can use this service to temporarily run an application

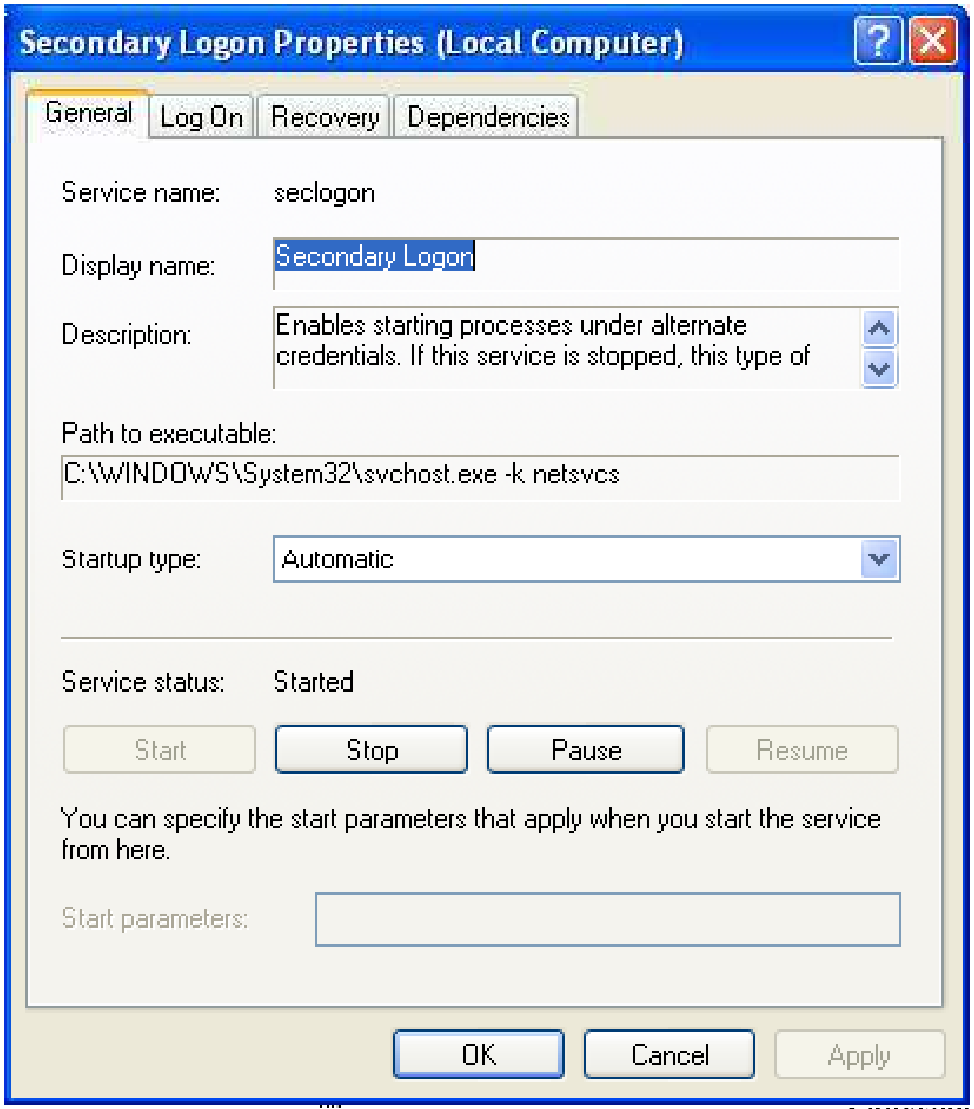
This service contain RunAs.exe allowing to run *.exe file and MMC consoles

This service is also called as **RunAs Service**

Installed and run automatically by default

If disabled, this type of logon will be unavailable

Secondary Logon



Secondary Logon Properties (Local Computer)

Service name: seclogon

Display name: Secondary Logon

Description: Enables starting processes under alternate credentials. If this service is stopped, this type of

Path to executable:
C:\WINDOWS\System32\svchost.exe -k netsvcs

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Security Accounts Manager

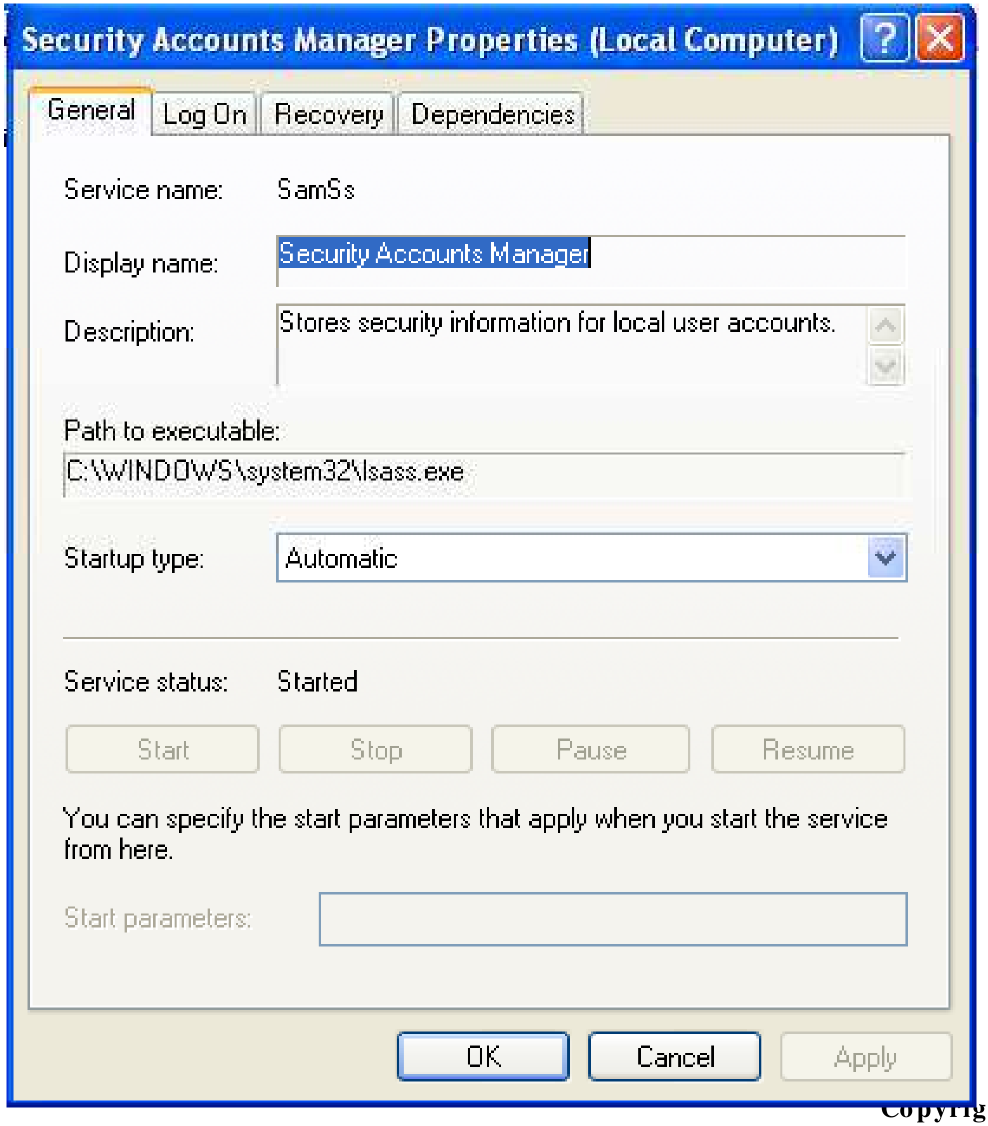
User and group information is protected by this service

The startup of this service signals other services that it is ready to accept requests

If disabled, other processes can not start

Do not disable this service

Security Accounts Manager



Service name: SamSs

Display name: Security Accounts Manager

Description: Stores security information for local user accounts.

Path to executable:
C:\WINDOWS\system32\lsass.exe

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Security Center

The service manages security setting by giving a central location for Windows XP with SP2 computers

This service performs the tasks such as:

- Checks whether the Windows Firewall service is running
- Queries specific third-party WMI providers to see if compatible antivirus software is installed, whether the software is up-to-date, and whether real-time scanning is turned on

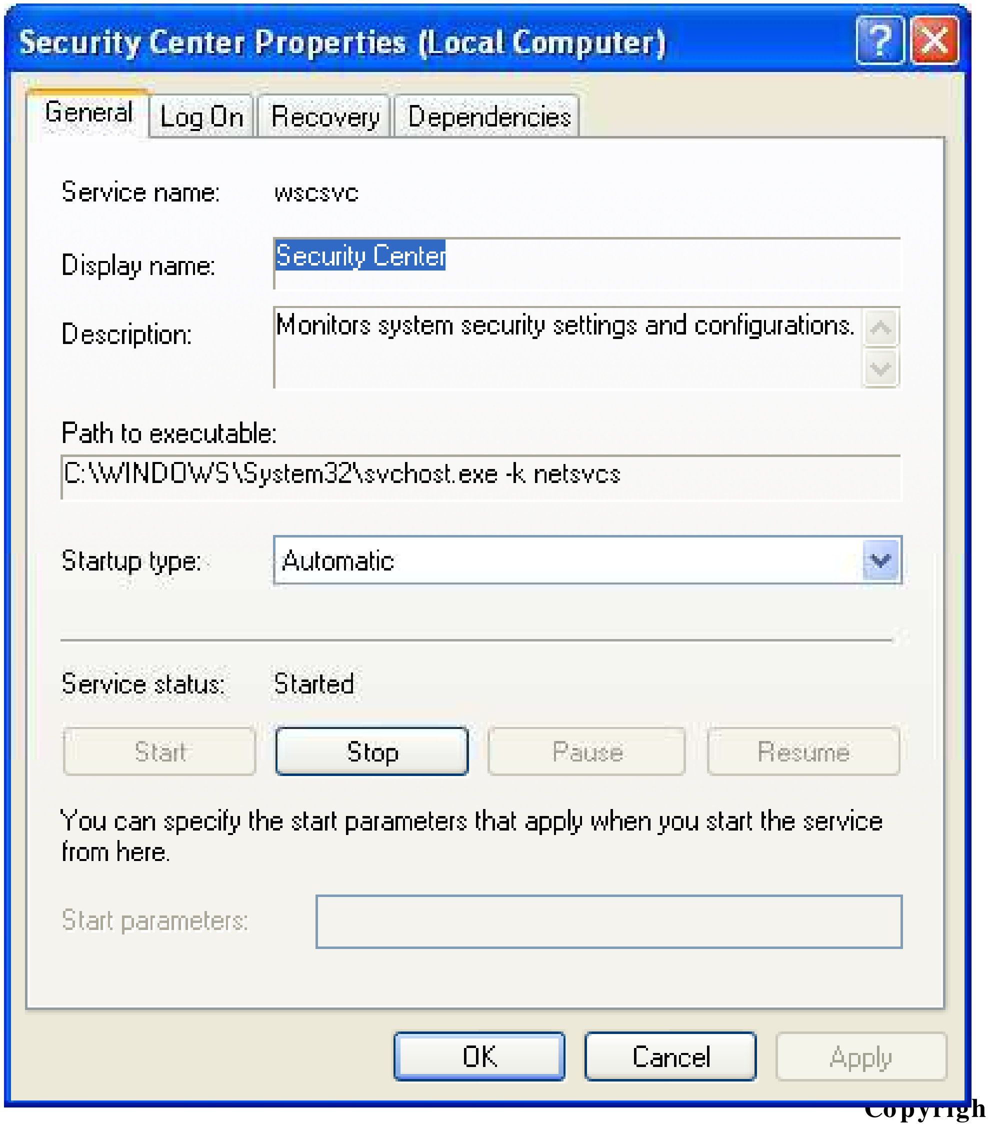
Security Center (Cont’d)

Checks the configuration of the **Automatic Updates** service.

If any service is not up to date a alert message is given to the user.

If disabled, the components will work as per the setting but no centralized service is provided.

Security Center (Cont'd)



Security Center Properties (Local Computer)

Service name: wscsvc

Display name: Security Center

Description: Monitors system security settings and configurations.

Path to executable:
C:\WINDOWS\System32\svchost.exe -k netsvcs

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Server

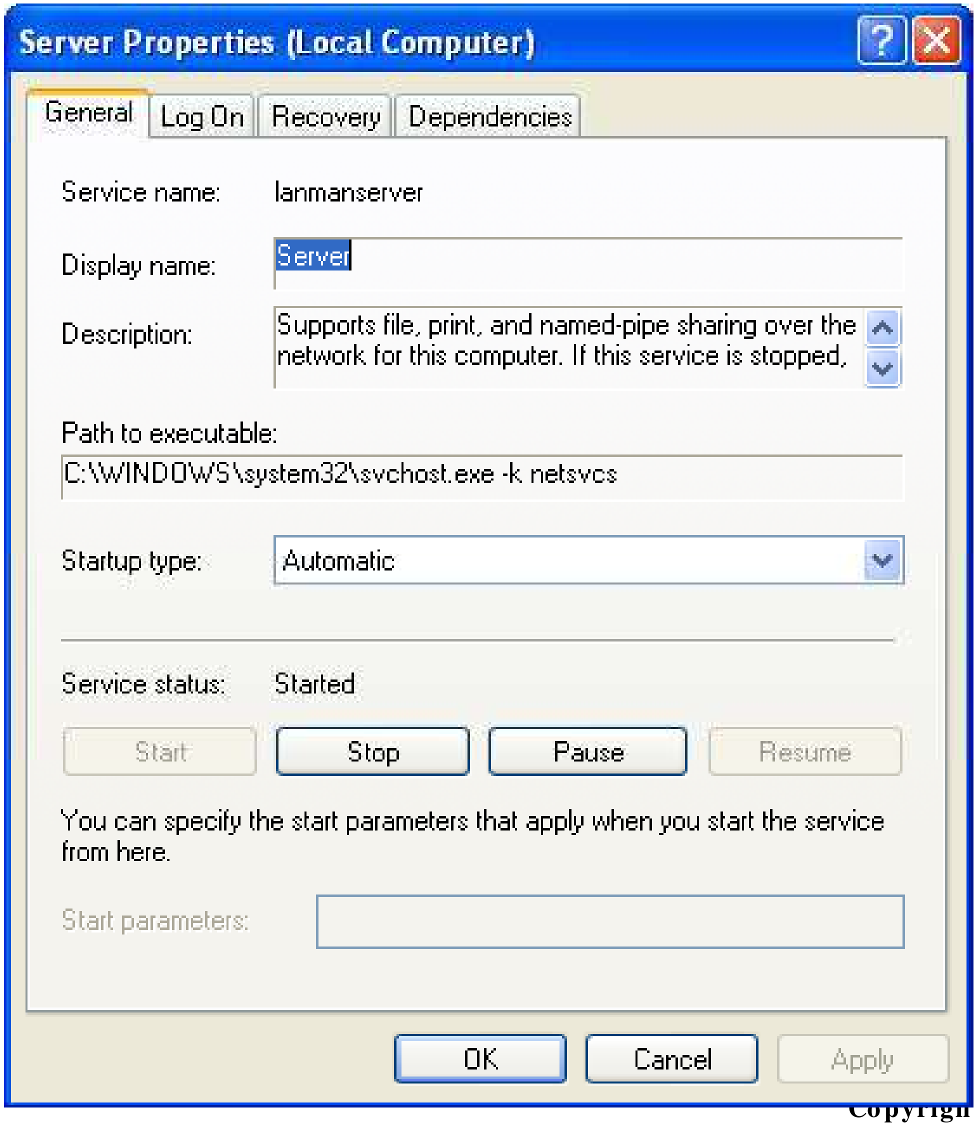
This service provides RPC support, file, print, and named pipe sharing over the network

This service is installed and runs automatically by default on Windows XP and Windows Server 2003

If disabled, local files and printers cannot be shared

It is not able to satisfy remote RPC request

Server



Service name: lanmanserver

Display name: Server

Description: Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped,

Path to executable:
C:\WINDOWS\system32\svchost.exe -k netsvcs

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Shell Hardware Detection

Notification for Auto play hardware events is provided and monitored by this service

Independent hardware vendors (IHVs) and independent software vendors (ISVs) can extend the support to include their hardware devices and applications

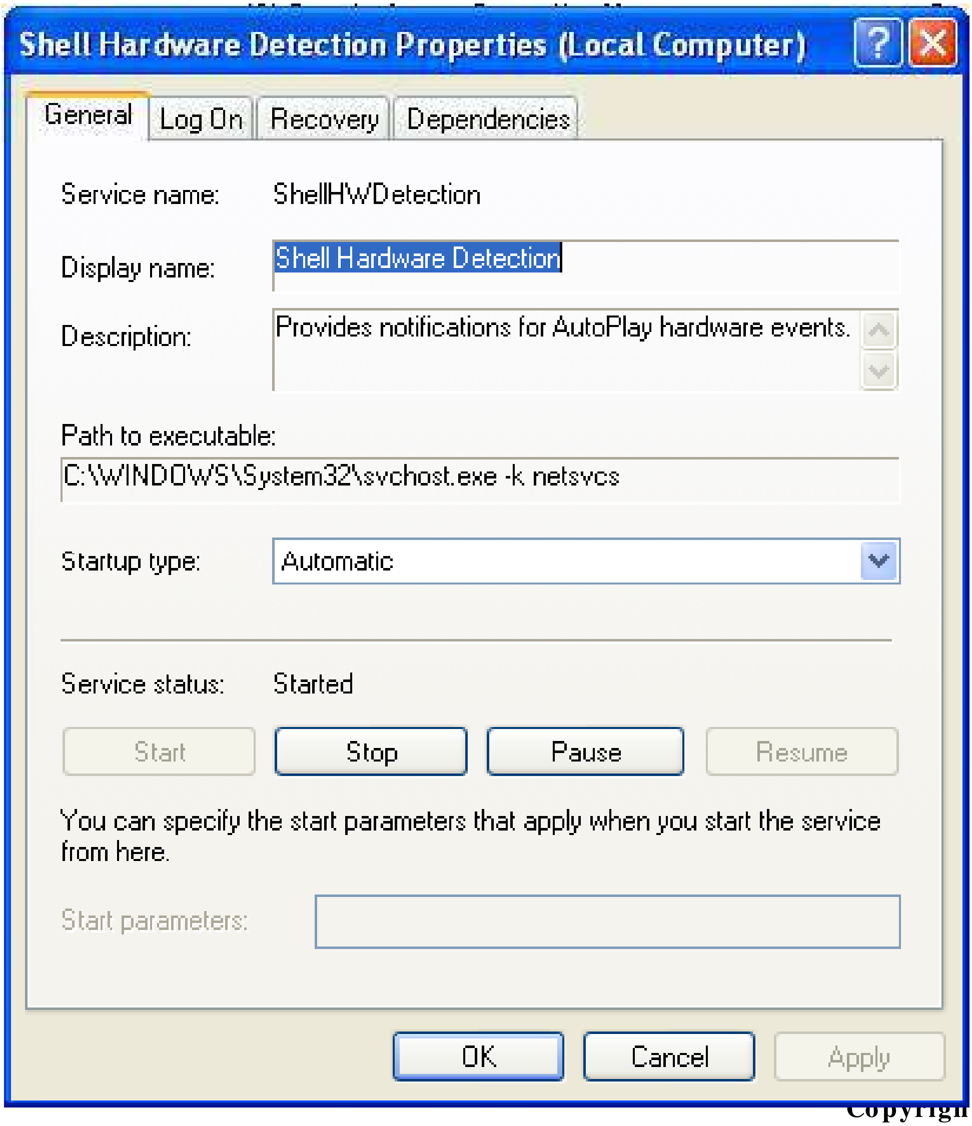
Shell Hardware Detection (Cont'd)

Media and device types that are supported by AutoPlay include:

- Removable storage media
- Flash media
- PC cards
- External hot-plug USB or 1394 fixed drives
- Supported content types, which include:
  - Pictures (.jpg, .bmp, .gif, and .tif files)
  - Music Files (.mp3 and .wma files)
  - Video (.mpg and .asf files)

This service is installed and run automatically by default

Shell Hardware Detection (Cont'd)



Service name: ShellHWDetection

Display name: Shell Hardware Detection

Description: Provides notifications for AutoPlay hardware events.

Path to executable:
C:\WINDOWS\System32\svchost.exe -k netsvcs

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Simple Mail Transport Protocol (SMTP)

This is an e-mail submission and relay agent

This service is used for inter-site email based replication in Windows domain controller

This service is installed and run by default on Windows Server 2003, Web Edition

Simple TCP/IP Services

The service supports the following protocols and ports:

- Echo, port 7, RFC 862
- Discard, port 9, RFC 863
- Character Generator, port 19, RFC 864
- Daytime, port 13, RFC 867
- Quote of the Day, port 17, RFC 865

If enabled, all the above protocols are enabled

If disabled, the operating system is not affected

Simple TCP/IP Services (Cont’d)

This service has to be installed manually

Install the service only if it is necessary to support communication with other computers that use the referenced protocol

Smart Card

The service controls access to a smart card that is inserted into smart card reader

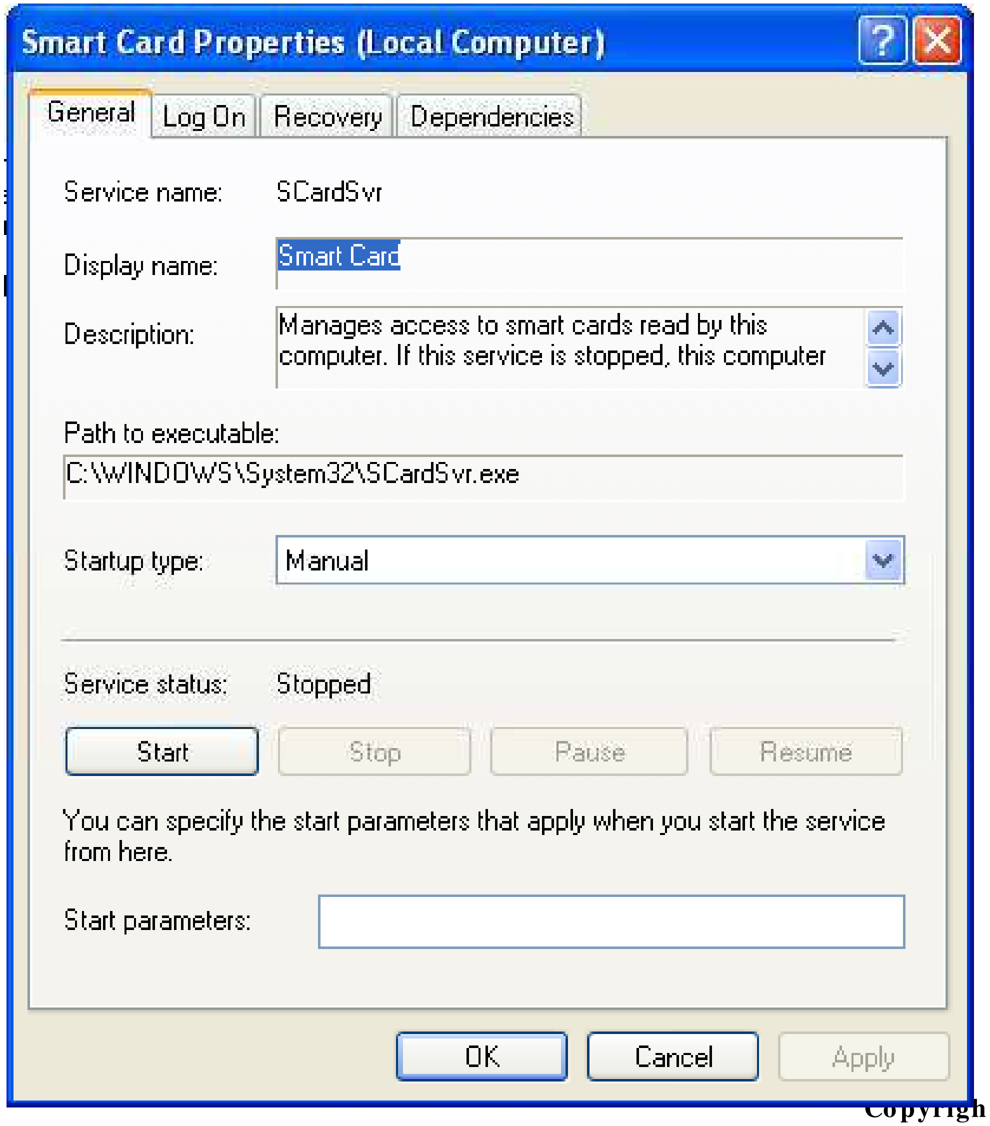
The Resource Manager performs functions:

- Identifies and tracks resources
- Allocates readers and resources across multiple applications
- Supports transaction primitives to access services that are available on a given card

This service is automatically installed on Windows XP and Windows Server 2003 by default, but is configured to start manually

If disabled, smart cards can not be read

Smart Card



Service name: SCardSvr

Display name: Smart Card

Description: Manages access to smart cards read by this computer. If this service is stopped, this computer

Path to executable:
C:\WINDOWS\System32\SCardSvr.exe

Startup type: Manual

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Special Administration Console Helper

This service performs remote management tasks if a function is stopped by an error message

The Windows Emergency Management Services component supports two out-of-band console interfaces:

- The Special Administration Console (SAC)
- !SAC, a subset of SAC commands

Both interfaces support input/output operations

Using command prompt a inbound communication channel by this service

If disabled, SAC service will not be available

System Event Notification

This service monitors events

This service is installed and run automatically by default

If disabled, no event notifications are sent:

- Win32 APIs IsNetworkAlive() and IsDestinationReachable() will not work.
- ISens* interfaces will not work. SENS logon/logoff notifications will fail.
- SyncMgr (Mobsync.exe) will not work properly.
- The COM+ EventSystem will fail when it tries to notify SENS of some events.
- The **Volume Shadow Copy** service will not load properly.

System Restore Service

Windows XP users can take snap shots of there computer and save them as restore point

This service is enabled by default to make point, before any critical modification

If disabled, no restore points will be created

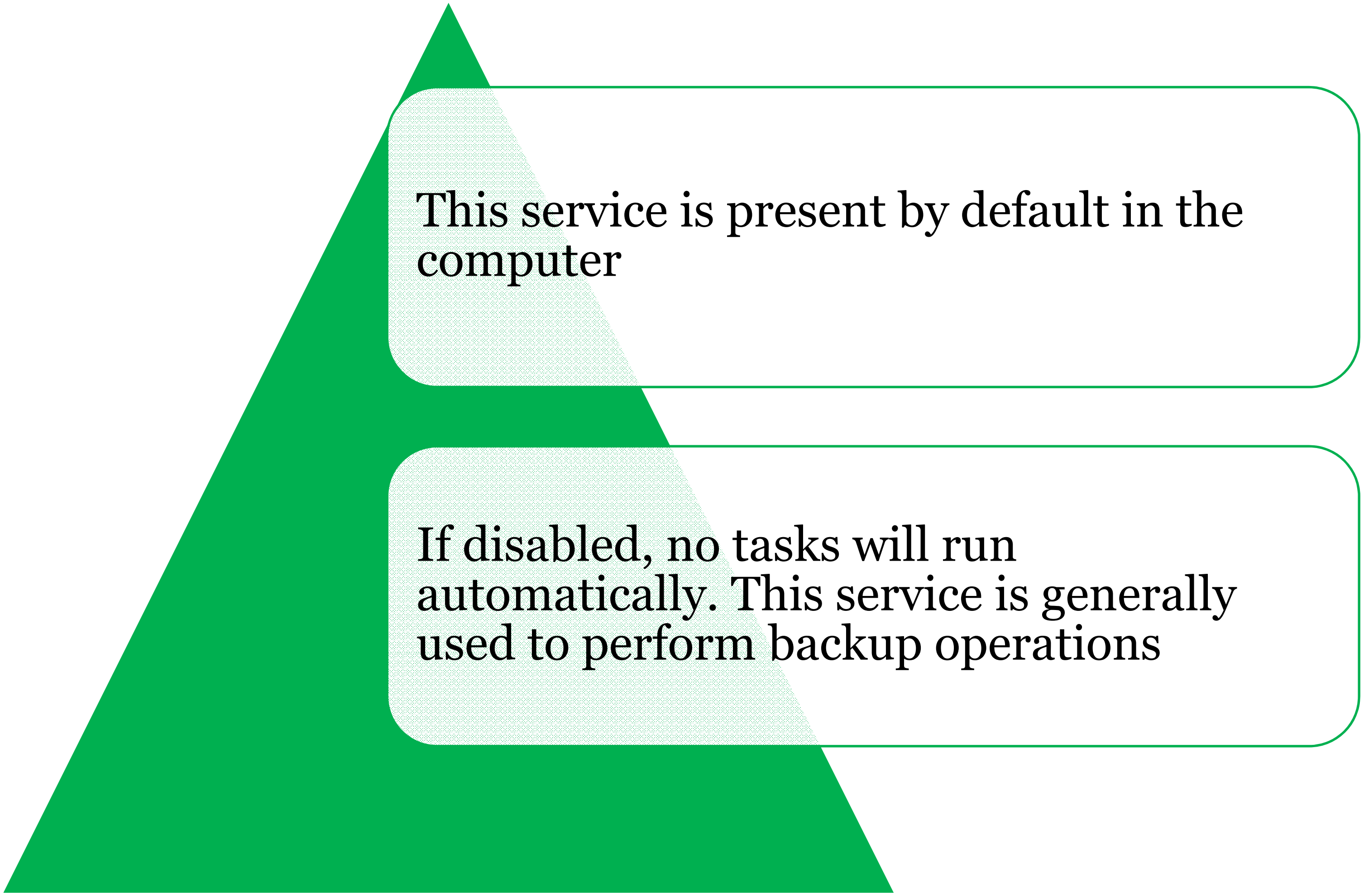
Task Scheduler

The service allows the computer to start a task on the computer

The following tasks can be performed by this service:

- Create work items (currently the only type of work item that is available is tasks)
- Schedule tasks to run at specific times or when a specific event occurs
- Change the schedule for a task
- Customize how tasks are run
- Stop a scheduled task

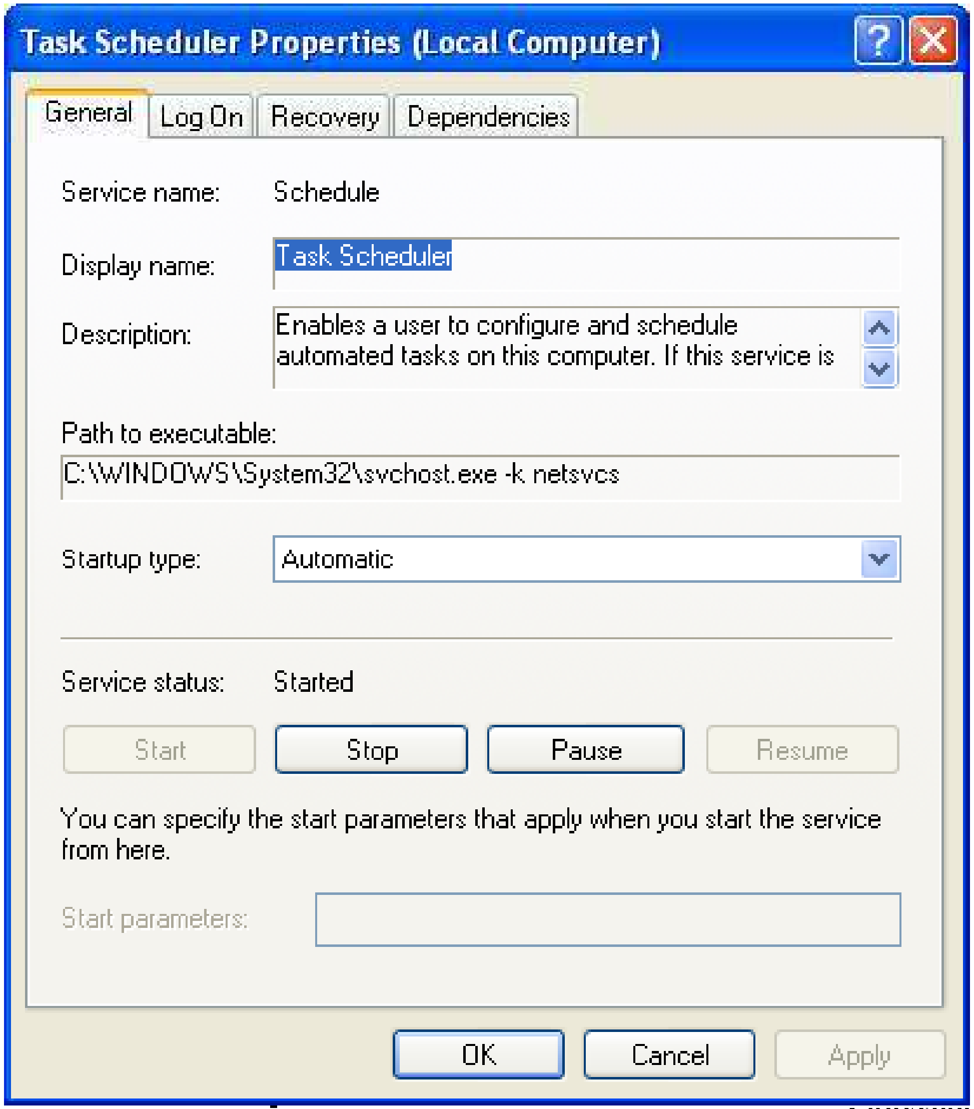
Task Scheduler (Cont'd)



This service is present by default in the computer

If disabled, no tasks will run automatically. This service is generally used to perform backup operations

Task Scheduler (Cont'd)



Task Scheduler Properties (Local Computer)

Service name: Schedule

Display name: Task Scheduler

Description: Enables a user to configure and schedule automated tasks on this computer. If this service is

Path to executable:
C:\WINDOWS\System32\svchost.exe -k netsvcs

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

TCP/IP NetBIOS Helper Service

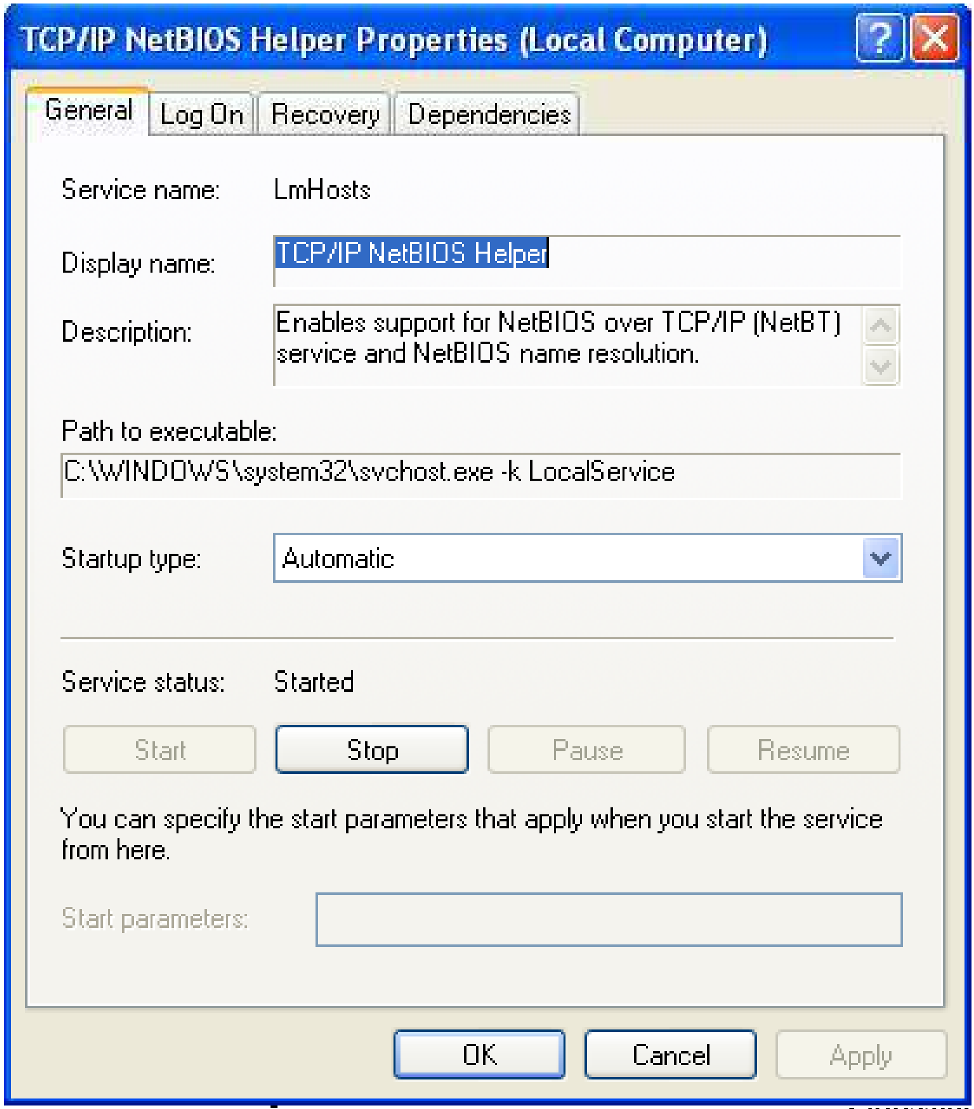
The service provides support for the NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution for clients on your network

It is enabled to share files, print and logon to the network

This is installed and started automatically

If disabled, NetBT, Redirector (RDR), Server (SRV), **Net Logon** and **Messenger** service clients might not be able to share files, printers and log on to computers

TCP/IP NetBIOS Helper Service



TCP/IP NetBIOS Helper Properties (Local Computer)

Service name: LmHosts

Display name: TCP/IP NetBIOS Helper

Description: Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution.

Path to executable:
C:\WINDOWS\system32\svchost.exe -k LocalService

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

TCP/IP Print Server

TCP/IP-based printing through the Line Printer Daemon protocol is enabled by this service

This is an optional component and has to be installed separately

If disabled, TCP/IP-based printing will not be supported

Telnet

This provides ASCII terminals to ASCII telnet clients

It supports four types of terminals:

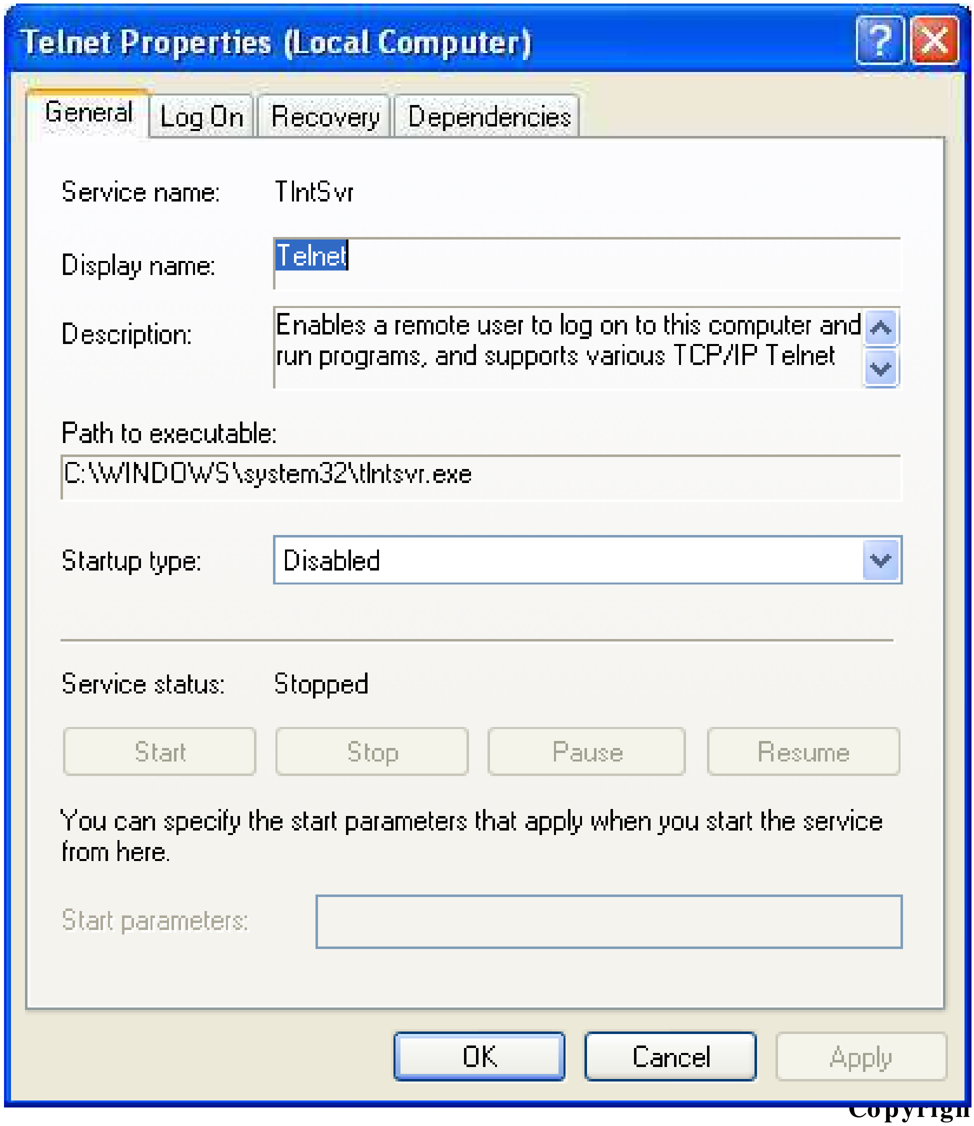
- American National Standards Institute (ANSI)
- VT-100
- VT-52
- VTNT.

This allows logon and running a program from command line

This service is installed by default but disabled

If disabled, remote user access to programs will be unavailable through the Telnet client

Telnet



Telnet Properties (Local Computer)

Service name: TlntSvr

Display name: Telnet

Description: Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet

Path to executable:
C:\WINDOWS\system32\tlntsvr.exe

Startup type: Disabled

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Terminal Services

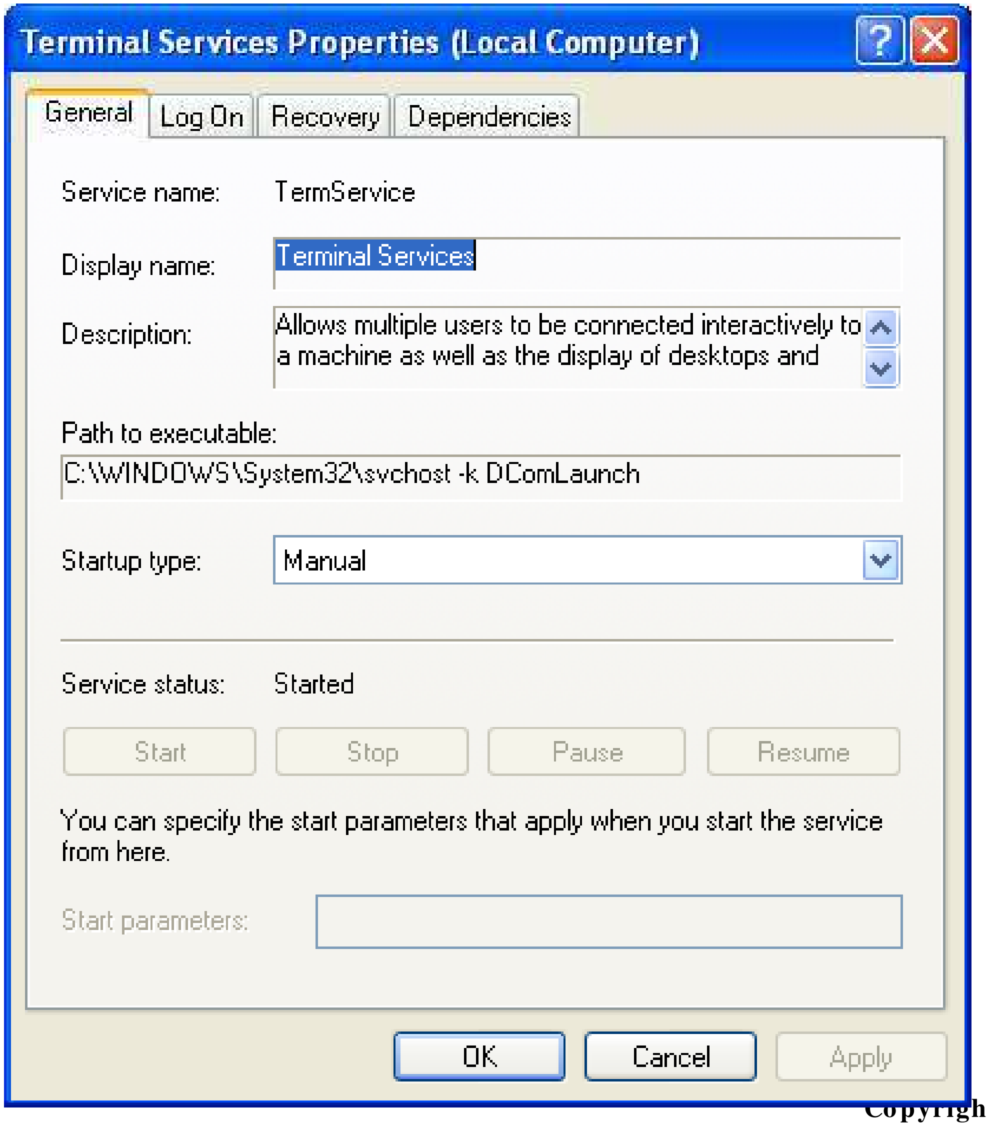
The service provides a multi session environment allowing client devices to interact with virtual Windows desktop session

This is installed by default, Configure the server or Add/Remove Windows Components to change the **Terminal Services** mode, with a startup type to manual

If disabled, Remote Assistance will not work

To prevent remote use clear the **Allow Remote Assistance** and **Allow Remote Desktop** checkboxes on the **Remote** tab of the **System Properties** property sheet

Terminal Services



Terminal Services Properties (Local Computer)

Service name: TermService

Display name: Terminal Services

Description: Allows multiple users to be connected interactively to a machine as well as the display of desktops and

Path to executable:
C:\WINDOWS\System32\svchost -k DComLaunch

Startup type: Manual

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Terminal Services Licensing

When a terminal server is connected this service installs a license server and offer registered client licenses

This service stores the client license and searches for the appropriate terminal

This service is needed by the servers where the service is installed in application mode

If disabled, the licenses are unable to issue

Terminal Services Session Directory

TSSD:

- This service manages a multi session environment to allow a client to access a virtual windows desktop session and windows based programs
- This service uses clusters to route a connection between the user and the server where already a session is active
- This service monitors the disconnected sessions and resets the session
- If disabled, the made request will be sent to one of the active servers

Trivial FTP Daemon

The service is a part of RIS and do not need any authentication for Windows Server 2003

The following RFCs define TFTP protocol:

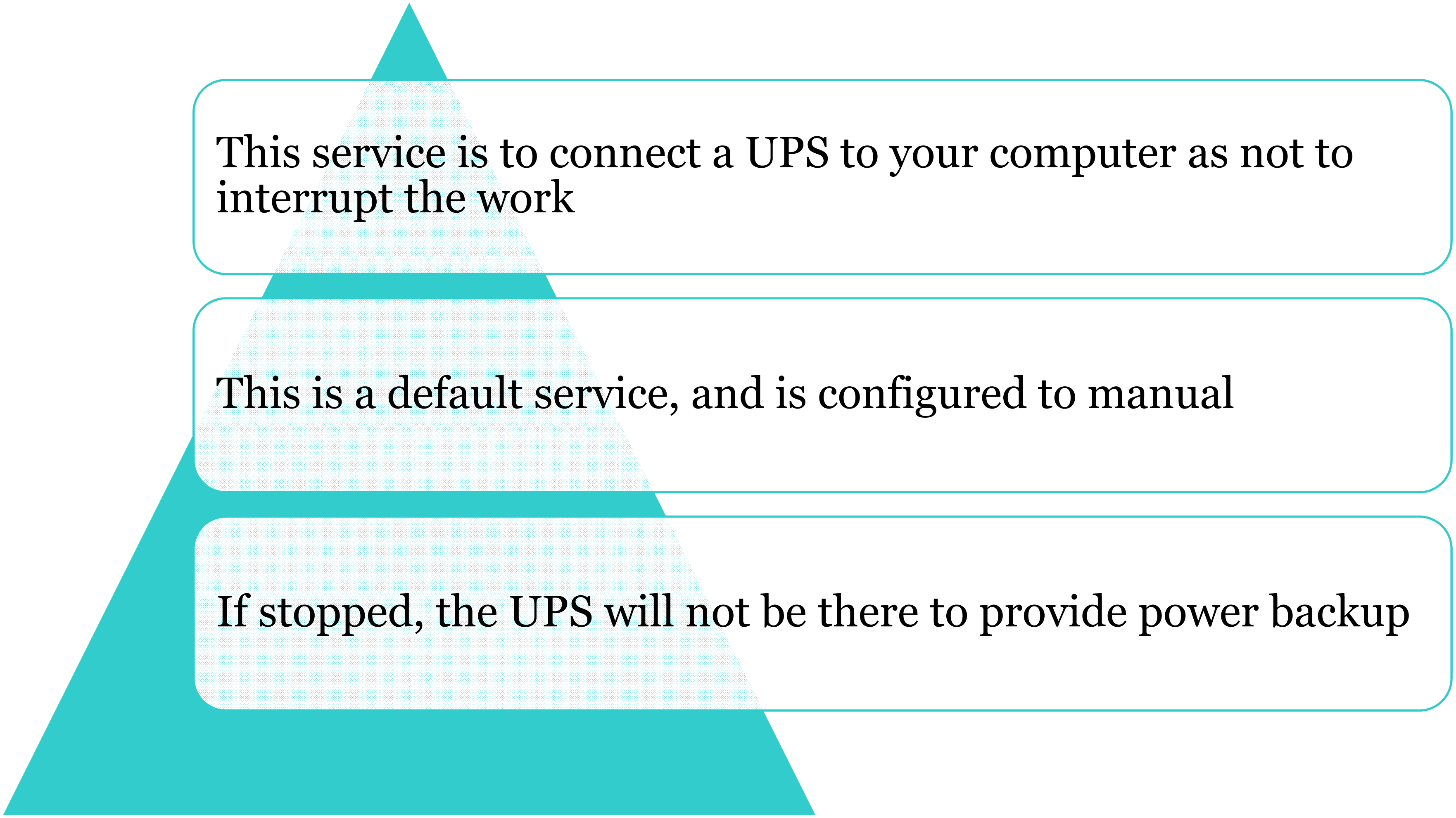
- RFC 1350 – TFTP
- RFC 2347 – Option extension
- RFC 2348 – Block size option
- RFC 2349 – Timeout interval, and transfer size options

By using this service the initial files necessary to begin remote installation process are been downloaded

This service is not installed by default

If disabled, the client computer requiring RIS will fail to install

Uninterruptible Power Supply

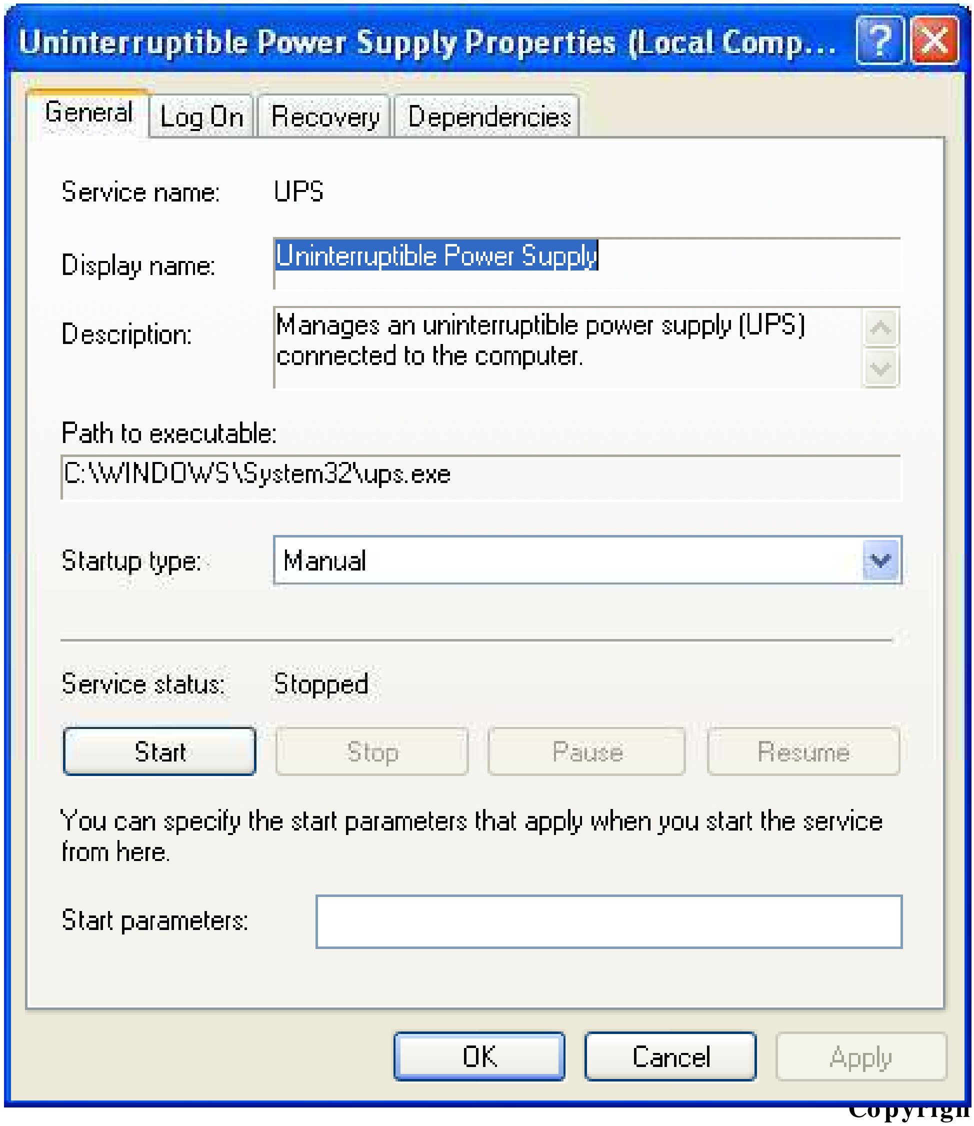


This service is to connect a UPS to your computer as not to interrupt the work

This is a default service, and is configured to manual

If stopped, the UPS will not be there to provide power backup

Uninterruptible Power Supply



Service name: UPS

Display name: Uninterruptible Power Supply

Description: Manages an uninterruptible power supply (UPS) connected to the computer.

Path to executable:
C:\WINDOWS\System32\ups.exe

Startup type: Manual

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Upload Manager

The file transfer (synchronous and asynchronous) between client and server is managed by this service

This service is helped to upload drivers and other needed updates when ever available

The service is installed by default but configured to manual

If disabled, the file transfer will not occur

Virtual Disk Service

The service provides a single interface to manage block storage virtualization

Using this service, you can manage bind operations, performance monitoring, topology discovery and tracking, volume status, and fault tracking

The service is installed and configured to manual

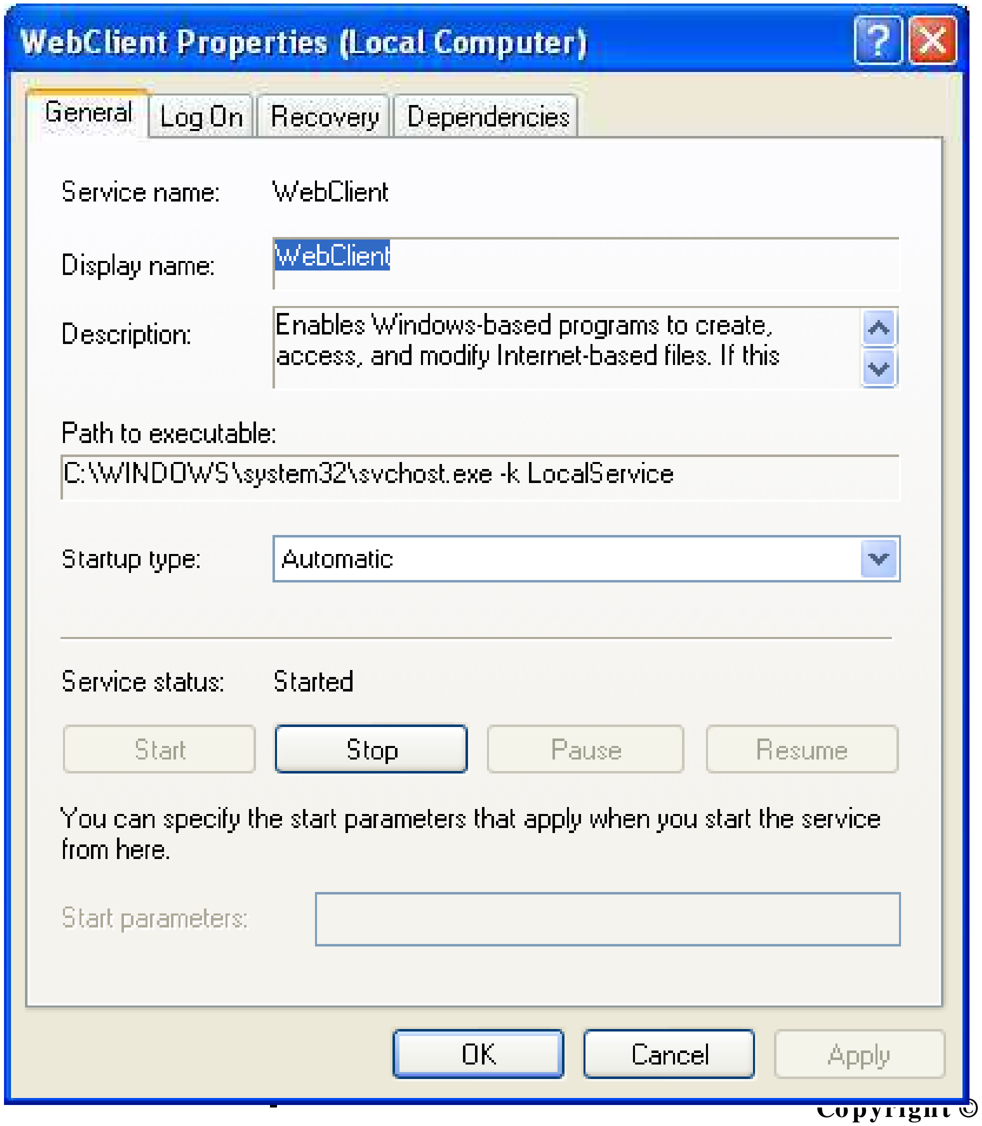
If disabled, this service will no longer be available

WebClient

This service allows Win32 applications to access documents on internet

This service is installed and started automatically on Windows XP, but on Windows Server 2003 this service is disabled

WebClient



Service name: WebClient

Display name: WebClient

Description: Enables Windows-based programs to create, access, and modify Internet-based files. If this

Path to executable:
C:\WINDOWS\system32\svchost.exe -k LocalService

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Web Element Manager

This service is installed on Windows Server 2003, web edition

The administrator can connect to website on port 8098 to get the information on:

- Tabs to display on the Administration Web site
- Remote administration tasks that are available to the Administrator
- Table of contents
- Help topics
- Remote administration alerts that can be displayed

This service will start when ever a request is sent and stops after it operations are performed

If disabled, a service dependent on this service will not start

Windows Firewall /Internet Connection Sharing

This service uses a dial up or broadband connection to provide network address translation (NAT), address and name resolution, and/or intrusion-prevention services

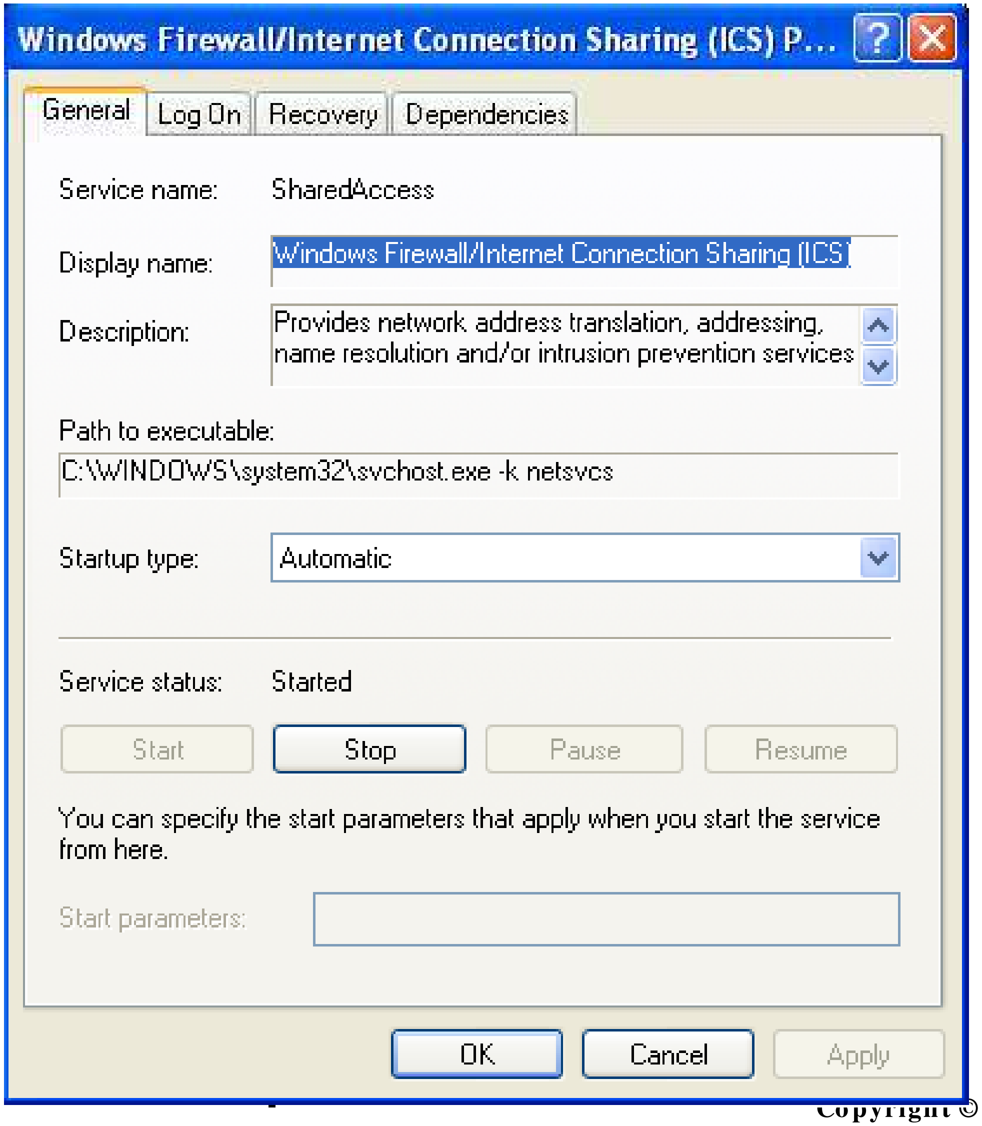
- Enabled - Computer becomes integrated gateway

This service has a location-aware Group Policy

In windows XP and Windows Server 2003 this service is automatically started by default, but disabled in Windows Server 2003

If disabled, network services will be unavailable

Windows Firewall /Internet Connection Sharing



Windows Firewall/Internet Connection Sharing (ICS) P...

Service name: SharedAccess

Display name: Windows Firewall/Internet Connection Sharing (ICS)

Description: Provides network address translation, addressing, name resolution and/or intrusion prevention services

Path to executable:
C:\WINDOWS\system32\svchost.exe -k netsvcs

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Windows Installer

This service manages the process of installing and removing of applications

This service can be used to modify, repair, or remove existing applications

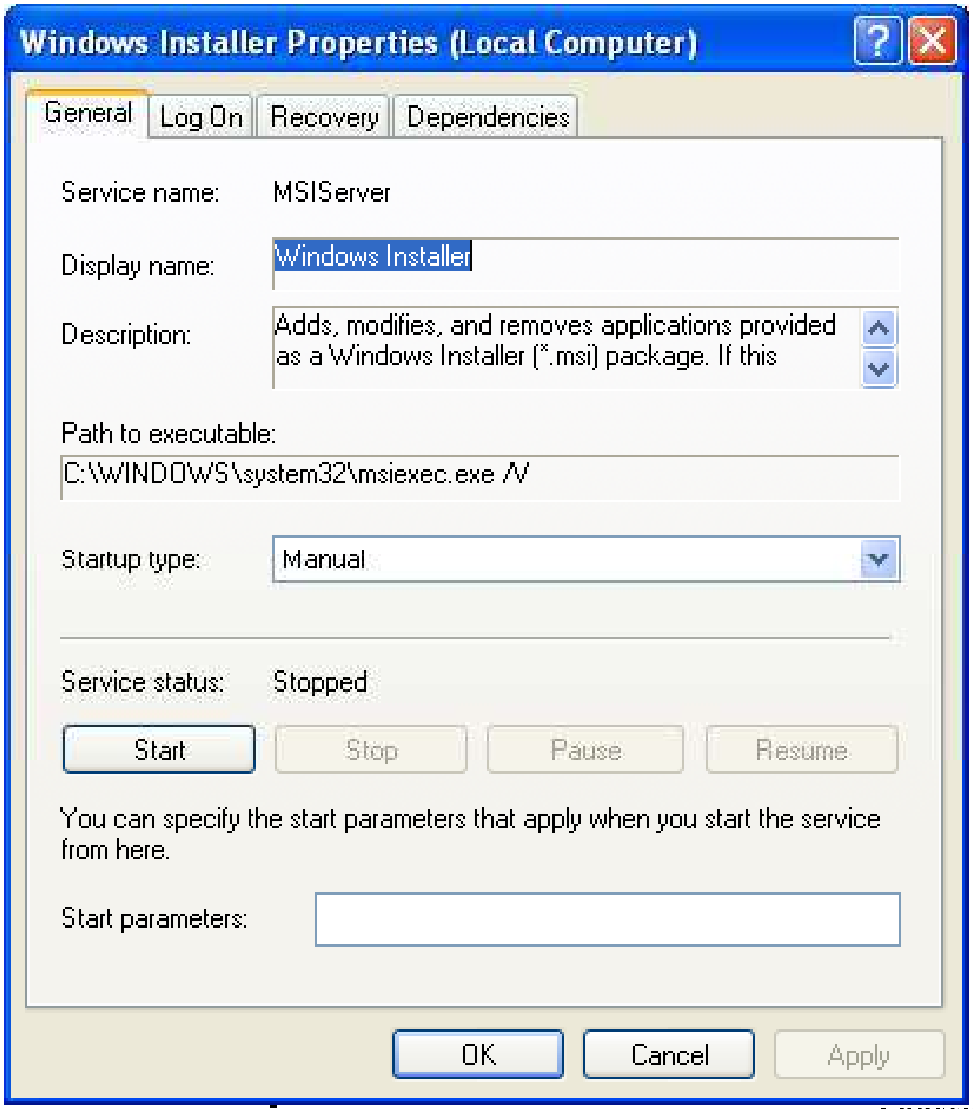
This service has a package of .msi files containing information on application setup and installation

This service also acts as extensible software management system

This is installed by default but configured to manual

If disabled, application can not be installed if they need this service to do so

Windows Installer



Windows Installer Properties (Local Computer)

Service name: MSIServer

Display name: Windows Installer

Description: Adds, modifies, and removes applications provided as a Windows Installer (*.msi) package. If this

Path to executable:
C:\WINDOWS\system32\msiexec.exe /V

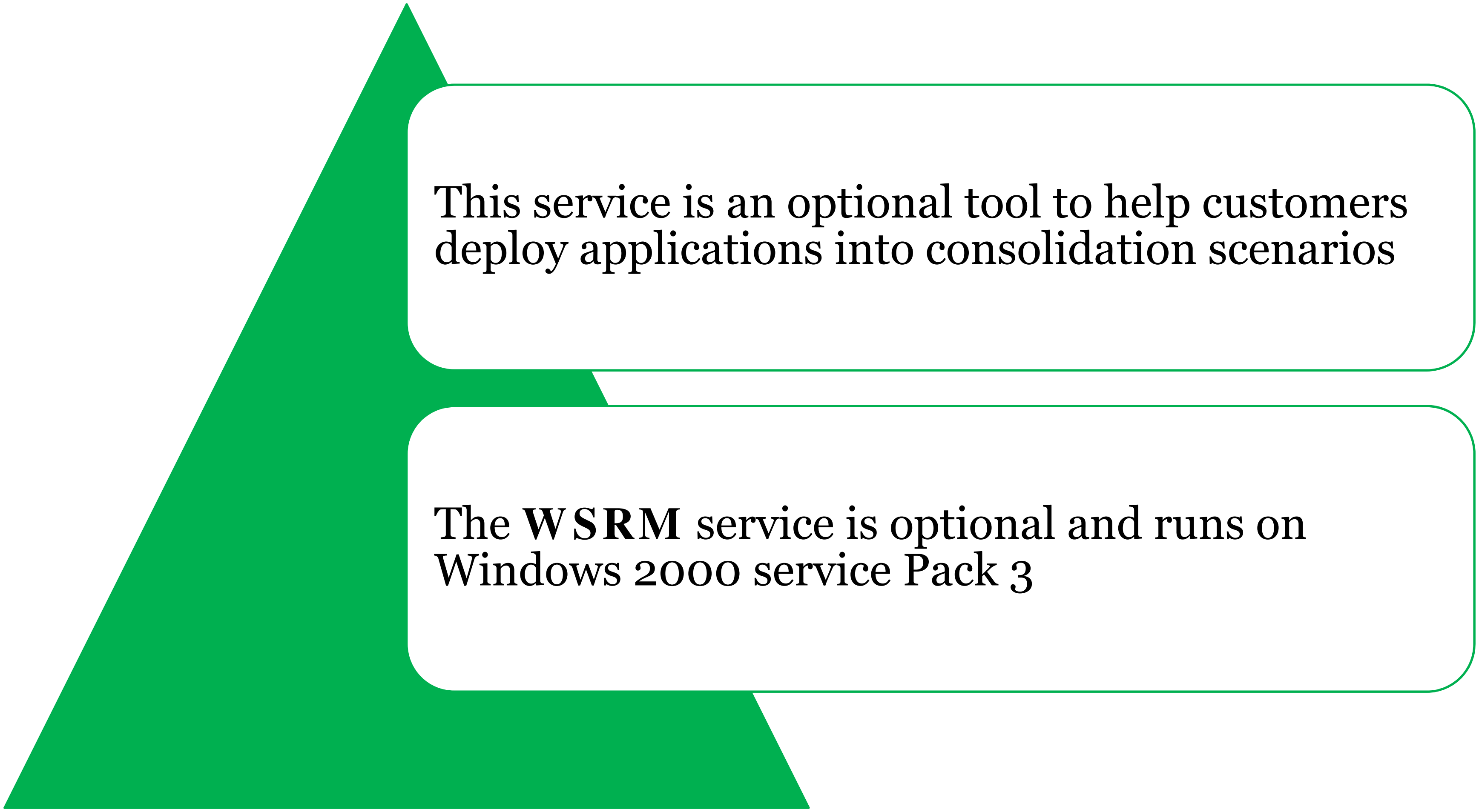
Startup type: Manual

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Windows System Resource Manager



This service is an optional tool to help customers deploy applications into consolidation scenarios

The **WSRM** service is optional and runs on Windows 2000 service Pack 3

Windows Time

This service manages the synchronization of date and time on the whole network

A NTP (Network Time Protocol) is used to synchronize the clock of the client and the server

Using this service the time can be synchronized from an external time server

If disabled, the local computer will not be synchronized with the external network

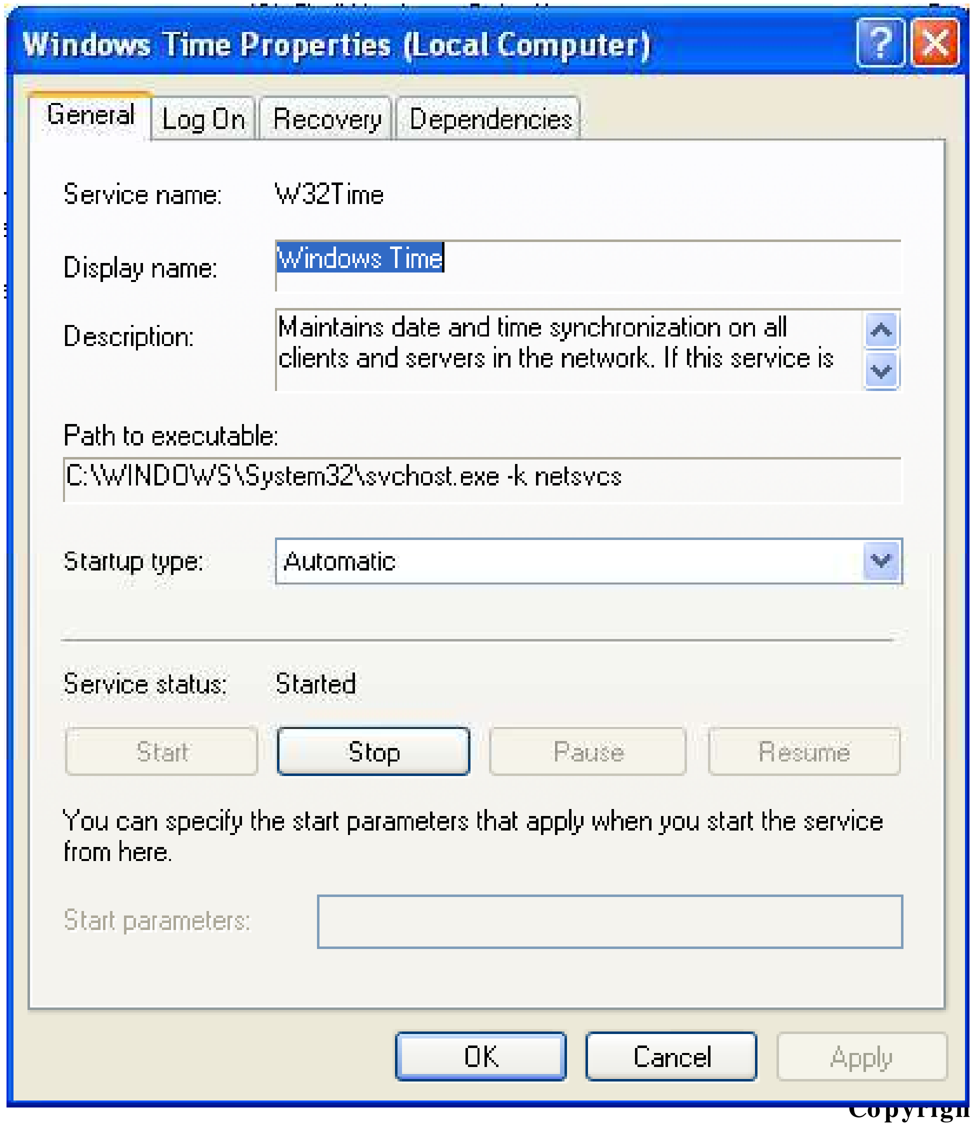
Windows Time (Cont'd)

There are two possible scenarios:

- If you stop the service on a workstation, the workstation will not be able to synchronize its time with another source but no other external server will be affected
- If you stop the service on a domain controller, the same effect as in the previous scenario will apply but domain members will also be unable to synchronize time with it

By default, the service is installed and run automatically on Windows XP and Windows Server 2003 computers

Windows Time (Cont'd)



Windows Time Properties (Local Computer)

Service name: W32Time

Display name: Windows Time

Description: Maintains date and time synchronization on all clients and servers in the network. If this service is

Path to executable:
C:\WINDOWS\System32\svchost.exe -k netsvcs

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

WinHTTP Web Proxy Auto-Discovery Service

This service process the Web Proxy Auto-Discovery (WPAD) protocol for Windows HTTP Services (WinHTTP)

WPAD is a protocol enabling an HTTP client to automatically discover a proxy configuration

If disabled, A WAPD protocol is executed with in the HTTP client, but not in an external service process and there will be no functionality loss

This service is installed by default and configured to manual

Wireless Configuration

The service starts automatic configuration for IEEE 802.11 wireless adapter for wireless communication

This service is installs and starts automatically on Windows Server 2003 and Windows XP

If disabled, automatic wireless configuration will not be provided

Workstation

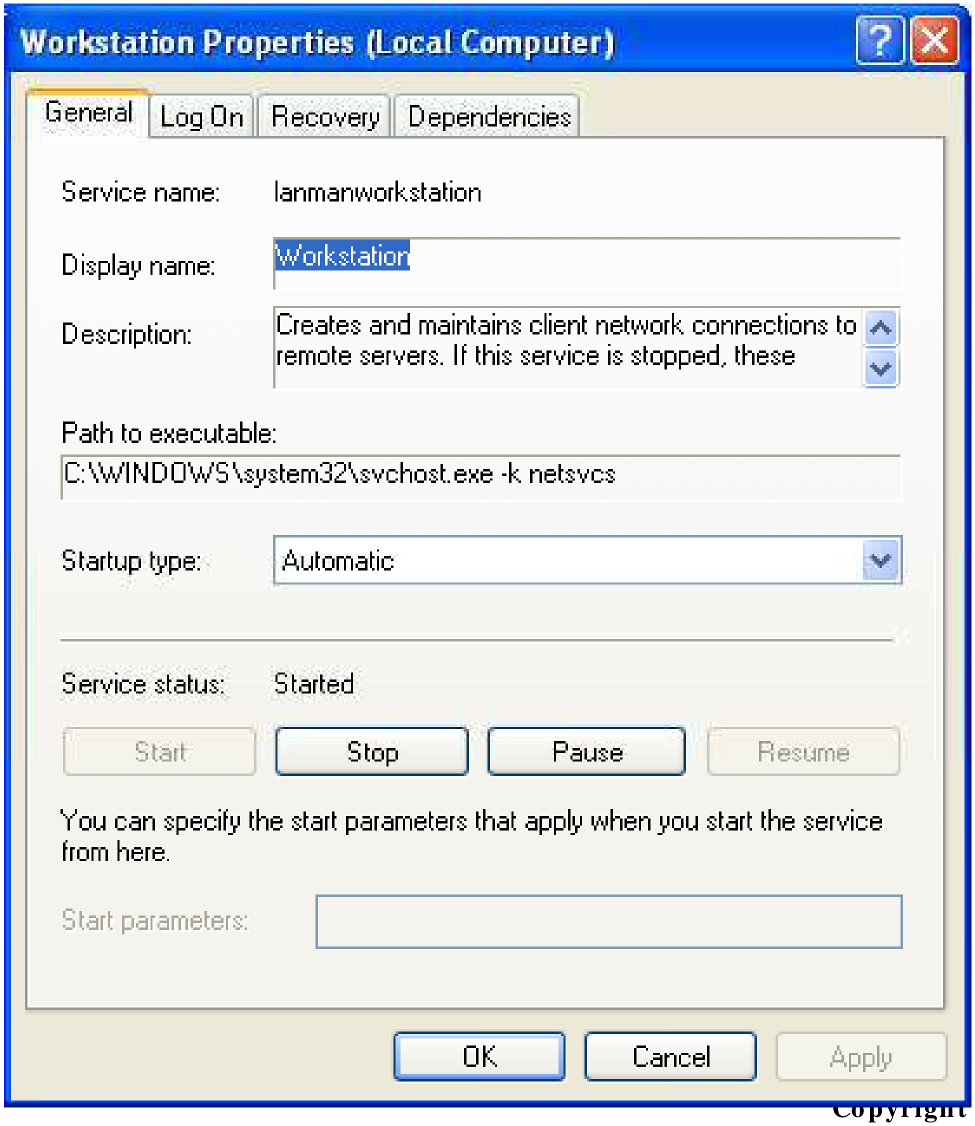
The service creates and maintains network connection and communication

It is installed and run automatically on Windows XP and Windows Server 2003

If disabled, remote servers can not be connected and can not access files through named pipes

Internet browsing and web client will work properly

Workstation



Service name: lanmanworkstation

Display name: Workstation

Description: Creates and maintains client network connections to remote servers. If this service is stopped, these

Path to executable:
C:\WINDOWS\system32\svchost.exe -k netsvcs

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

World Wide Web Publishing Service

The service provides web connectivity and administration of sites through MMC IIS snap-in

This service is an optional component installed on Windows Server 2003 or Windows XP as part of the IIS package

If stopped, the Windows Server 2003 operating system can not serve a Web request

Software Restriction Policies

Software restriction policies provide a policy-driven system to specify which programs are allowed to execute and which are not

The Threat of Malicious Software

The daily increase usage of network in business computing is more likely than an organization's users which encounter malware (malicious software)

These policies can help organizations protect themselves through another layer of defense against viruses, Trojans, and other types of malicious code

The Threat of Malicious Software (Cont'd)

Vulnerability

- Networks are collaborated increasingly in use of communication, instant messaging and peer-to-peer applications, and this may increase risk from viruses, worms and other forms of malware
- E-mail and instant messaging can transport unwanted hostile code which can take many forms from native Windows executable (.exe) files, to macros in word processing (.doc) documents, to script (.vbs) files
- E-mail messages are often transmitted with viruses and worms which include techniques to trick users for activating the malicious code

The Threat of Malicious Software (Cont'd)

Vulnerability

- Various forms of code can be difficult for users to know which is safe and which is not
- Activate malicious code may damage hard disk, flood a network, confidential information or compromise security of computer

Countermeasure

- To test the policies a sound design can be created in organization before deploying them into production environment

The Threat of Malicious Software (Cont'd)

Potential Impact

- A hostile application and other disable applications are allowed through flawed software restriction policy.
- Sufficient resources are given to manage and trouble shoots the implementation of policies.

Windows XP and Windows Server 2003 Administrative Templates

This section of the group policy gives the settings for appearance of the computer in the environment

This section has many settings available to configure and import .adm files to make other settings available

Administrative template settings are shown in this section

CEH™ Certified Ethical Hacker

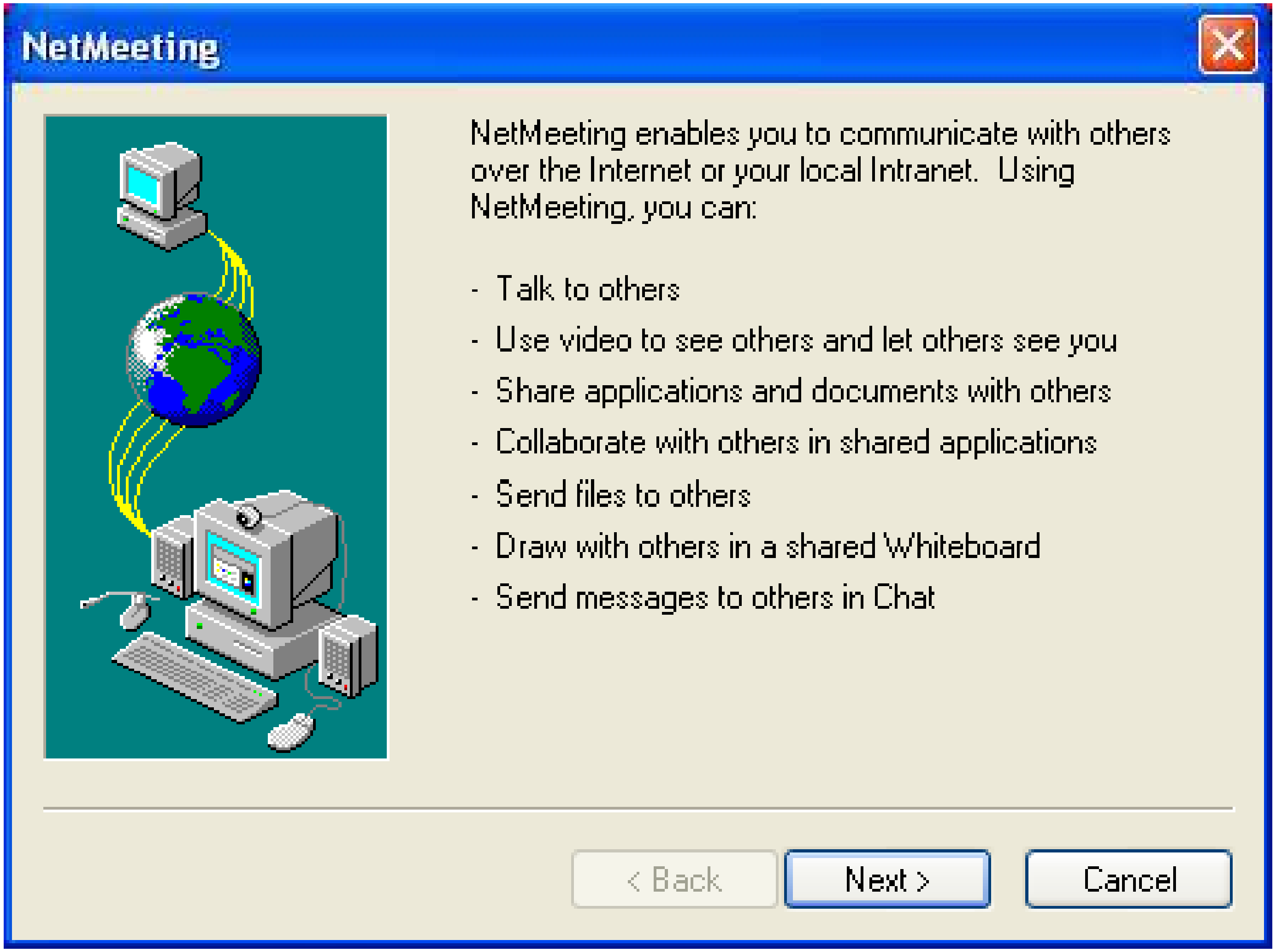
Computer Configuration Settings

This settings made in this section are available only to the members of Active Directory® directory service domain

NetMeeting

- This feature allows user to conduct vital meeting on the network
- They can be configured from the following location:
  - **Computer Configuration\Administrative Templates\Windows Components\NetMeeting**

NetMeeting



NetMeeting enables you to communicate with others over the Internet or your local Intranet. Using NetMeeting, you can:

- Talk to others
- Use video to see others and let others see you
- Share applications and documents with others
- Collaborate with others in shared applications
- Send files to others
- Draw with others in a shared Whiteboard
- Send messages to others in Chat

Disable Remote Desktop Sharing

By using the policy, the remote desktop sharing features can be stopped

Enable – The policy cannot be configured to automatically answer calls and remote control of the local desktop

The values for the Disable remote Desktop Sharing setting are:

- Enabled
- Disabled
- Not Configured

Disable Remote Desktop Sharing (Cont'd)

Vulnerability

- Enabled, the remote desktop sharing feature is not accessible

Countermeasure

- Configure the policy setting to **Enabled**

Potential Impact

- User cannot configure remote desktop sharing but can make use of features like Windows Remote Assistance and Remote Desktop if enabled

Internet Explorer Computer Settings

Internet Explorer (IE) a Web browser in Windows XP and Windows Server 2003 can be managed through group policies

Configure this policy setting at:

- **Computer Configuration\Administrative Templates\Windows Components\Internet Explorer**

EC-Council

Disable Automatic Install of Internet Explorer Components

This setting stops the automatic download of components through IE, when ever the user browses a site

If disabled or not configured, the user may be stopped to install the necessary software

By this setting the admin can set conditions on what kind of components can be installed

The values for the **Disable Automatic Install of Internet Explorer components** setting are:

- **Enabled**
- **Disable**
- **Not Configured**

Disable Automatic Install of Internet Explorer Components (Cont'd)

Vulnerability

- Some Web sites may have malicious code in their components and if a user trying to access this component the code can be executed and data may loss

Countermeasure

- Configure the setting to Enabled

Potential Impact

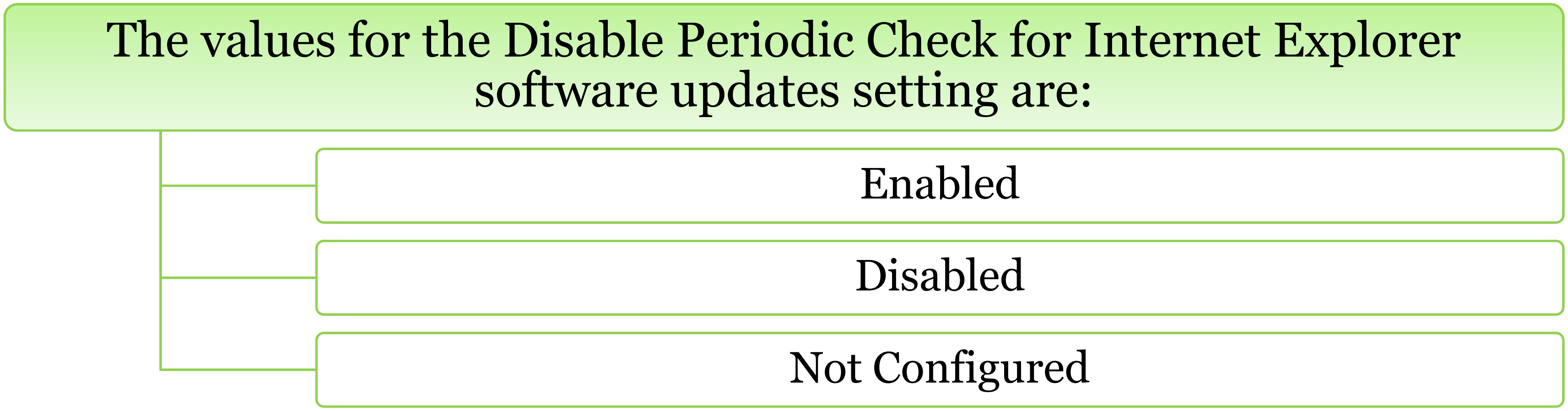
- IE will not allow downloading of components automatically

Disable Periodic Check for Internet Explorer Software Updates

This policy disables the automatic update option on IE, and user will not know what newer versions are updated for the software

If disabled, IE will check on updates every 30 days

By this policy setting admin can keep track on the version control of IE



The values for the Disable Periodic Check for Internet Explorer software updates setting are:

- Enabled
- Disabled
- Not Configured

Disable Periodic Check for Internet Explorer Software Updates (Cont'd)

Vulnerability

- This policy can be enabled to stop automatic periodic checks for updates

Countermeasure

- Configure the policy setting to **Enabled**

Potential Impact

- This will not allow IE to automatically download and install and component
- But the admin should have any other program that can run updates for necessary software

Disable Software Update Shell Notifications on Program Launch

This policy will not display a message to the user if any Microsoft Software Distribution Channel installs a new component

If disabled, a message is sent to inform the users about the new installation

The values for the **Disable software update shell notifications on program launch** setting are:

- Enabled
- Disabled
- Not Configured

Disable Software Update Shell Notifications on Program Launch (Cont'd)

Vulnerability

- By enabling this policy, the administrator may not want the users to have any kind of intimation on the installation of components and service packs

Countermeasure

- Configure the setting to Enabled

Potential Impact

- Users will not receive any message to notify the about any installation

Make Proxy Settings Per-Machine (Rather than Per-User)

If enabled, the user cannot change user defined proxy settings

The values for the Make proxy settings per-machine (rather than per-user) setting are:

- Enabled
- Disabled
- Not Configured

Make Proxy Settings Per-Machine (Rather than Per-User) (Cont'd)

Vulnerability

- If disabled, users can set there own proxy settings

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- The users have to use the settings defined for the computer

Security Zones: Do Not Allow Users to Add/Delete Sites

The policy disables site management settings for security zones

If disabled, users can Add/Remove site zones

The values for the Security Zones: Do not allow users to add/delete sites setting are:

- Enabled
- Disabled
- Not Configured

Security Zones: Do Not Allow Users to Add/Delete Sites (Cont'd)

Vulnerability

- If the policy is not configured, the users can add/remove sites which may contain malicious data

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- An administrator has to configure to add any remote site

Security Zones: Do Not Allow Users to Change Policies

This policy setting permit you to effectively disable the Custom Level button and Security level for the zone slider on the Security tab in the Internet Options dialog box

If disabled, users may modify the security zone settings. The values for the Security Zones: Do not allow users to change policies settings are:

- Enabled
- Disabled
- Not Configured

Security Zones: Do Not Allow Users to Change Policies (Cont'd)

Vulnerability

- If users can change the security setting malicious data codes can be available

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- For IE zone, users are not able to configure security setting

Turn off Crash Detection

The crash detection feature in IE is managed by this policy

If enable, A crash in IE will start Windows Error Reporting

If disabled, crash detection feature will be functional

The values for the **Turn off Crash Detection** setting are:

- Enabled
- Disabled
- Not Configured

Certified Ethical Hacker

Turn off Crash Detection (Cont’d)

Vulnerability

- This report may contain important information from the computer memory

Countermeasure

- Configure the policy setting to **Enabled**

Potential Impact

- The information gathered by the crashes on the add-ons is not reported to Microsoft
- Disabling this option will allow to report the problem

EC-Council

Do Not Allow Users to Enable or Disable Add-ons

By configuring this policy, user cannot operate through Manage Add-ons

If enabled, it is not possible to Manage Add-ons

If disabled, the user will be able to Manage Add-ons

The values for the **Do not allow users to enable or disable add-ons** setting are:

- Enabled
- Disabled
- Not Configured

Do Not Allow Users to Enable or Disable Add-ons (Cont'd)

Vulnerability

- The add-ons not allowed by the organization security policy will relatively cause some problem

Countermeasure

- Configure the value of the setting to **Enabled**

Potential Impact

- If enabled, Add-ons cannot be managed

Internet Explorer\Internet Control Panel\Security Page

Configure Internet Explorer Security Page Group Policy settings within the Group Policy Object Editor at the location:

- **Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page**

Follow the general security guidelines

Internet Explorer\Internet Control Panel\Security Page (Cont'd)

Vulnerability

- If users are allowed to any security setting in IE, they may install applications with malicious code

Countermeasure

- Use the settings in the **Internet Explorer\Internet Control Panel\Security Page** node to configure values for security zone-related behavior

Potential Impact

- The default values for these policy settings provide enhanced security over earlier versions of Windows

Internet Explorer\Internet Control Panel\Advanced Page

Allow Software to Run or Install Even if the Signature is Invalid

This policy settings concludes on the usage of a software with an invalid signature

Enable – Install and run software with invalid file signature

Disable – Cannot install software with invalid file signature

The values for the **Allow software to run or install even if the signature is invalid** setting are:

- Enabled
- Disabled
- Not Configured

Allow Software to Run or Install Even if the Signature is Invalid (Cont'd)

Vulnerability

- All software download have digital signatures attached to it, to recognize its validity
- The validity of unsigned code cannot be ascertained

Countermeasure

- Configure the setting to **Disabled**

Potential Impact

- The software signatures may have invalid signatures. A proper check has to be performed before using the software

Allow Active Content from CDs to Run on User Machines

This policy concludes whether active contents on CDs can run on user computers.

The values for the **Allow active content from CDs to run on user machines** setting are:

- Enabled
- Disabled
- Not Configured

Allow Active Content from CDs to Run on User Machines (Cont'd)

Vulnerability

- The installing software from a CD rather than the network can crack an organization security policy

Countermeasure

- Configure the setting to **Disabled**

Potential Impact

- When enabled, applications to be installed form the CD might not work properly

Allow Third-party Browser Extensions

(This policy setting is only available in Windows Server 2003.)

A third-party browser extension known as Browser Helper Objects (BHOs) can be used

The values for the **Allow third-party browser extensions** setting are:

- Enabled
- Disabled
- Not Configured

Allow Third-party Browser Extensions (Cont'd)

Vulnerability

- The Third-party browser extensions may not be safe, and may violate security policy

Countermeasure

- Configure the setting to **Disabled**

Potential Impact

- If disabled, user can install third-party browser extensions

Check for Server Certificate Revocation

(This policy setting is only available in Windows Server 2003.)

A Secure Socket Layer connection between browser and remote server gives a certificate to be used for initial negotiation

If enabled, it determines that the certificate is on the issuing authority's certificate revocation list

The values for the Check for server certificate revocation setting are:

- Enabled
- Disabled
- Not Configured

Check for Server Certificate Revocation (Cont'd)

Vulnerability

- User may communicate with server with an invalid certificate. This may lead to information disclosure or even active attacks

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- If enabled, warning messages can be given

Check for Signatures On Downloaded Programs

(This policy setting is only available in Windows Server 2003.)

This policy will check for a digital signature on the downloaded software

If enabled, this policy will check for the signature and can display information before downloading

The values for the **Check for signatures on downloaded programs** setting are:

- Enabled
- Disabled
- Not Configured

Check for Signatures on Downloaded Programs (Cont'd)

Vulnerability

- Any virus can be downloaded unknowingly

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- When enabled, user can view the information about software

Do Not Save Encrypted Pages to Disk

(This policy setting is only available in Windows Server 2003.)

When IE accesses any pages from the remote server, the pages are stored in a temporary folder as IE can access the pages easily next time with out a reconnection

The values for the Do not save encrypted pages to disk setting are:

- Enabled
- Disabled
- Not Configured

Do Not Save Encrypted Pages to Disk (Cont'd)

Vulnerability

- These pages may contain sensitive information like password and credit card numbers

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- If disabled, the pages will not be saved to the disk

Empty Temporary Internet Files Folder when Browser is Closed

(This policy setting is only available in Windows Server 2003.)

When files are downloaded from the Internet the temporary files are cached in a temporary folder

These temporary folders have to be cleaned by IE

The values for the **Empty Temporary Internet Files folder when browser is closed** setting are:

- Enabled
- Disabled
- Not Configured

Empty Temporary Internet Files Folder when Browser is Closed (Cont'd)

Vulnerability

- The file in the temporary folder may contain sensitive information, which may be accessed by any other user

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- IE uses the temp folders to increase browser performance
- If disabled, the time and bandwidth may increase

Internet Explorer\Security Features

The **Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Security Features**

- portion of the Windows Administrative Templates has many settings

Each of these policy settings has their subordinate settings:

Internet Explorer Processes.

- Possible values:
  - **Enable** – the behavior is stopped for IE and Windows Explorer process
  - **Disable** – Default settings are considered
  - **Not Configured** – Default settings are considered

EC-Council

Internet Explorer\Security Features (Cont'd)

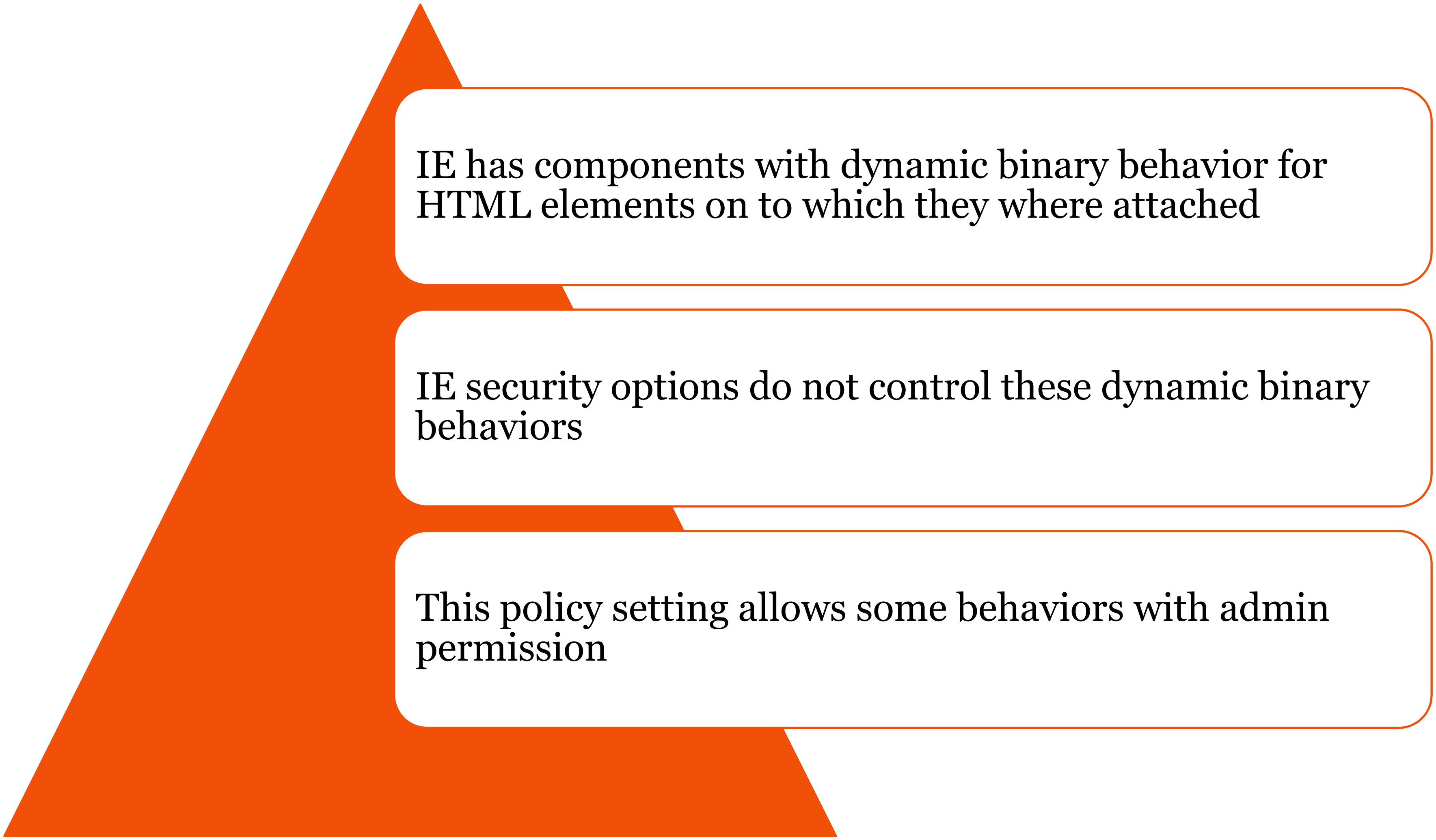
Process List

- This gives individual processes with security features to be enabled or disabled
- A list known, as process list will contain the process applied by the feature
- The value 1 disabled the feature and 0 enables it

All Processes

- Possible values:
  - Enable – the behavior is stopped for IE and Windows Explorer process
  - Disable – Default settings are considered
  - Not Configured – Default settings are considered

Binary Behavior Security Restriction



IE has components with dynamic binary behavior for HTML elements on to which they where attached

IE security options do not control these dynamic binary behaviors

This policy setting allows some behaviors with admin permission

Binary Behavior Security Restriction (Cont'd)

Vulnerability

- Some behaviors that are written bad and malicious behaviors can be accessed and compromised

Countermeasure

- Disable binary behaviors and allow only a set of admin-approved behaviors

Potential Impact

- Some applications dependent on binary behavior may not work properly

EC-Council

MK Protocol Security Restriction

This policy blocks MK protocol to reduce attack possibility

The MK protocols have been used to extract data from compressed files

Vulnerability

- Vulnerabilities may be in the MK protocol handler, or in applications calling it

Countermeasure

- The MK protocol must be blocked when it is not necessary

Potential Impact

- The applications needing MK protocol will fail

Local Machine Zone Lockdown Security

A web browser when access a web page in IE, it places some restrictions as per the security zone

Each zone will be having a set of restrictions

The security zone is decided on basis of the location of access. (Example: An open network may have more restrictions than an intranet work in an organization)

Local Machine Zone Lockdown Security (Cont'd)

Vulnerability

- Generally attackers try to get privileges to access a computer in a local machine zone

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- If this settings are enabled, IE application which use local HTML may not work properly

EC-Council

Consistent MIME Handling

The MIME (Multipurpose Internet Mail Extensions) data is used to handle files downloaded from web server

This setting concludes that Internet Explorer requires that all file-type information that is provided by Web servers be consistent

Enable – IE checks all received files and enforces consistent MIME data

Disable – IE do not need consistent MIME data

Consistent MIME Handling (Cont'd)

Vulnerability

- An attacker can send executable content by using a non-executable MIME type

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- Applications dependent on MIME download objects will be failed

MIME Sniffing Safety Features

The process of inspecting the MIME file (Data file, Executable file) is known as MIME sniffing

If enabled, MIME sniffing will not send a file of one type to another

If disabled, MIME sniff that promotes a file

MIME Sniffing Safety Features (Cont’d)

Vulnerability

- A malicious web site sends one MIME type with a false indication

Countermeasure

- Configure the setting for **All Processes** to **Enabled**

Potential Impact

- MIME files with wrong functionality will not work

Scripted Window Security Restrictions

IE allows scripting for opening, resizing and repositioning the windows programmatically like, restricting pop-up windows

If enabled, these restrictions are applied to IE or Windows Explorer

Scripted Window Security Restrictions (Cont'd)

Vulnerability	• Some websites will resize windows to make the user to use a window with some malicious code
Countermeasure	• Configure the setting for **Internet Explorer Processes** to **Enabled**
Potential Impact	• The malicious website may not work properly

Restrict ActiveX Install

This policy is used to block ActiveX control installation

If enabled, users will not be prompted ActiveX control installation, which has to be done manually

If disabled, ActiveX control installation prompts will not be blocked

Restrict ActiveX Install (Cont'd)

Vulnerability

- User may choose some ActiveX controls which are not permitted to use

Countermeasure

- Configure the setting for **Internet Explorer Processes** to **Enabled**

Potential Impact

- If enable, users cannot be able to install authorized legitimate ActiveX controls

Restrict File Download

If the policy is enabled, file download prompts that are not user-initiated are blocked

Vulnerability	- Some website start a file download with out users idea
Countermeasure	- Configure the policy value for **Internet Explorer Processes** to **Enabled**
Potential Impact	- None

Network Protocol Lockdown

Administrators can specify individual protocols (including HTTP and HTTPS) in this policy setting to control which protocols may be used to obtain active content

Vulnerability

- Users may download the malicious data to be executed

Countermeasure

- Configure the policy setting for Internet Explorer Processes to Enabled

Potential Impact

- If zone controls are set, users cannot run pages with active controls

Internet Information Services

Microsoft Internet Information Service (IIS) 6.0 the built-in web server, allows to share the file easily

Configure the IIS setting:

- **Computer Configuration\Administrative Templates\Windows Components\Internet Information Services**

Prevent IIS Installation

IIS 6.0 is not installed on the computer by default. So, by setting this option to enable you can restrict the installation in future

The values for the **Prevent IIS installation** setting are:

- Enabled
- Disabled
- Not Configured

Prevent IIS Installation (Cont'd)

Vulnerability

- The older versions of IIS have serious security problem related with it
- IIS 6.0 is secure than its previous versions
- IIS 6.0 should be installed only on web servers

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- Applications that need IIS may not be installed
- This policy setting will have no effect if it is enabled on a computer on which IIS is already installed

Terminal Services

This component is builds on a solid foundation by the application server mode; it is extended with new capabilities in Windows XP

This policy allows Windows based applications to any computing device

When an application runs on TS, the execution is carried on the server, and only display information is transmitted on the network

Configure the Policy settings at the location:

- **Computer Configuration\Administrative Templates\Windows Components\Terminal Services**

Deny Log Off of an Administrator Logged in to the Console Session

This policy determines whether an administrator can log off an admin form a remote server where he is logged on

The console session is also known as Session 0

The values for the **Deny log off of an administrator logged in to the console session** setting are:

- Enabled
- Disabled
- Not Configured

Deny Log Off of an Administrator Logged in to the Console Session (Cont’d)

If enable, Logging off an admin connected to the computer is not possible

If disabled, an admin can logoff another admin from a computer

If the current administrator is logged off, unsaved data will be lost

Deny Log Off of an Administrator Logged in to the Console Session (Cont’d)

Vulnerability

- An attacker can make a Terminal Server session and get access to the console
- The attacker will have a complete control on the computer

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- An administrator cannot log off another admin from a session o console

Do Not Allow Local Administrators to Customize Permissions

This policy controls the admin rights for permissions in Terminal Services Configuration (TSCC) tool

If enabled, the admin will not be able to change the security description. The security descriptions are Read Only

If disabled, the server admin will have full right for read and write to the security descriptions in TSCC permission tab

The values for the **Do not allow local administrators to customize permissions** setting are:

- Enabled
- Disabled
- Not Configured

Do Not Allow Local Administrators to Customize Permissions (Cont'd)

Vulnerability

- An attacker who gained permission on a server can change them using TSCC tool to stop other user connections to server and generate a DoS connection

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- The TSCC **Permissions** tab cannot customize per-connection security descriptors or change the default security descriptors

Sets Rules for Remote Control of Terminal Services User Sessions

This policy gives the control level in a Terminal Server session

There are two types of remote control permissions:

- **View Session** – Permits the remote control user to watch a session
- **Full Control** – Permits the remote control user to interact with the session

If enabled, the admin can interact with the Terminal server session

Sets Rules for Remote Control of Terminal Services User Sessions (Cont'd)

To disable, set the option to No remote control allowed

If disabled, the admin cannot get the level of permission using TSCC tool

The values for the **Sets rules for remote control of Terminal Services user sessions** setting are:

- Enabled with options for:
  - No remote control allowed
  - Full Control with user's permission
  - Full Control without user's permission
  - View Session with user's permission
  - View Session without user's permission
- Disabled
- Not Configured

Sets Rules for Remote Control of Terminal Services User Sessions (Cont'd)

Vulnerability

- At attacker can gain access as an admin and view the actions of other users

Countermeasure

- Configure the setting to **Enabled** and select the **No remote control allowed** option

Potential Impact

- Administrators will not be able to use the remote control feature to assist other Terminal Services users

Client/Server Data Redirection

Terminal Services allows data and resources from the client and server to be redirected

This section allows you to customize the redirection type

Configure the Terminal service setting at:

- **Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Client\Server data redirection**

Allow Time Zone Redirection

This policy decides on redirecting the time zone to Terminal server session

If enabled, clients can send their time zone information to the server

The computer's time and time zone can be changed by connecting to, Session 0

If disabled, time zone cannot be sent to the server

Allow Time Zone Redirection (Cont'd)

The values for the Allow Time Zone Redirection setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability	• The time zone can be transmitted between server and the local machine
Countermeasure	• Configure the policy setting to **Disabled**
Potential Impact	• Time zone redirection will not be possible

EC-Council

Do Not Allow COM Port Redirection

By using this policy redirecting the data to the client port from the remote computer can be stopped

If enabled, data cannot be redirected to COM port computers. And server data cannot be sent to the local computer

If disabled, redirection of Terminal Service COM port is possible

An admin can stop the redirection using TSCC tool

Do Not Allow COM Port Redirection (Cont'd)

The values for the **Do not allow COM port redirection** setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

- No direct user interaction is needed to forward data from Terminal server session to local computer

Countermeasure

- Configure the policy setting to **Enabled**

Potential Impact

- COM port redirection will not be possible

Do Not Allow Client Printer Redirection

This policy decides on using the client printers on the Terminal server session

Bt default client printer is mapped to Terminal server session

If enabled, the print job cannot be redirected in the Terminal server session

The redirection is possible when this policy is disabled

Do Not Allow Client Printer Redirection (Cont'd)

The values for the **Do not allow client printer redirection** setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

- No user interaction is necessary to forward data

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- Printer redirection will not be possible

Do Not Allow LPT Port Redirection

This policy tells to stop the redirection of data to client parallel port or not during a Terminal Server session

If enabled, users cannot redirect server data to their local LPT port

If disabled, LPT port redirection is allowed

The values for the **Do not allow LPT port redirection** setting are:

- Enabled
- Disabled
- Not Configured

Do Not Allow LPT Port Redirection (Cont'd)

Vulnerability	- No user interaction is necessary to forward data
Countermeasure	- Configure the setting to Enabled
Potential Impact	- LPT port redirection will not be possible

Do Not Allow Drive Redirection

Using this policy, mapping client drives upon connection to the Terminal service automatically; this behavior can be over ridden

If enabled, client drive redirection is prevented

If disabled, client drive redirection is always allowed

The values for the **Do not allow drive redirection** setting are:

- Enabled
- Disabled
- Not Configured

Do Not Allow Drive Redirection (Cont'd)

Vulnerability	- No user interaction is necessary to forward data
Countermeasure	- Configure the setting to **Enabled**
Potential Impact	- Drive redirection will not be possible

Encryption and Security

Configure the Terminal Server Encryption and Security settings in the following location:

- **Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security**

Set Client Connection Encryption Level

This policy decides on enforcing an encryption level for the data sent between client and remote computer during the terminal server session

If enabled, a level of encryption can be given for connections on the server. By default the level is high

If disabled, no encryption level is given

Set Client Connection Encryption Level (Cont'd)

The values for the **Set Client Connection Encryption Level** setting are:

Enabled with encryption options:

- **Client Compatible**. The level encrypts data to maximum key strength. This is used for remote computers running in mixed or legacy client environment.
- **High Level**. This level encrypts the data to 128-bit. Clients that do not support this level of encryption cannot connect.
- **Low Level**. The level encrypts the data to 56-bit. In this data between server and client is not encrypted.

Disabled

Not Configured

Set Client Connection Encryption Level (Cont'd)

Vulnerability

- If Terminal Server client will use low level encryption, an attacker can decrypt after capturing the traffic

Countermeasure

- Configure the setting to High Level

Potential Impact

- Clients that do not support 128-bit encryption will be unable to establish Terminal Server sessions

Always Prompt Client For A Password On Connection

This policy decides on prompting the client for password ever time he is connected

This policy will ask for password to the client at Terminal service even after connecting to Remote Desktop connection

If enabled, automatic logon is not accepted

If disabled, user can logon automatically

An administrator can still enforce password prompting by using the TSCC tool

Always Prompt Client For A Password On Connection (Cont'd)

The values for the **Always prompt client for a password on connection** setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

- Users are generally allowed to store their username and password while creating Remote Desktop connection.
- If an attacker accesses a Remote computer and gains access then by using the stored password he can gain access to the Terminal Server.

Always Prompt Client For A Password On Connection (Cont'd)

Countermeasure

- Configure the setting to **Enabled**.

Potential Impact

- Users will always have to enter their password when they establish new Terminal Server sessions

RPC Security Policy

Configure the Terminal Server RPC Security setting in the following location:

- **Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security\RPC Security Policy**

Secure Server (Require Security)

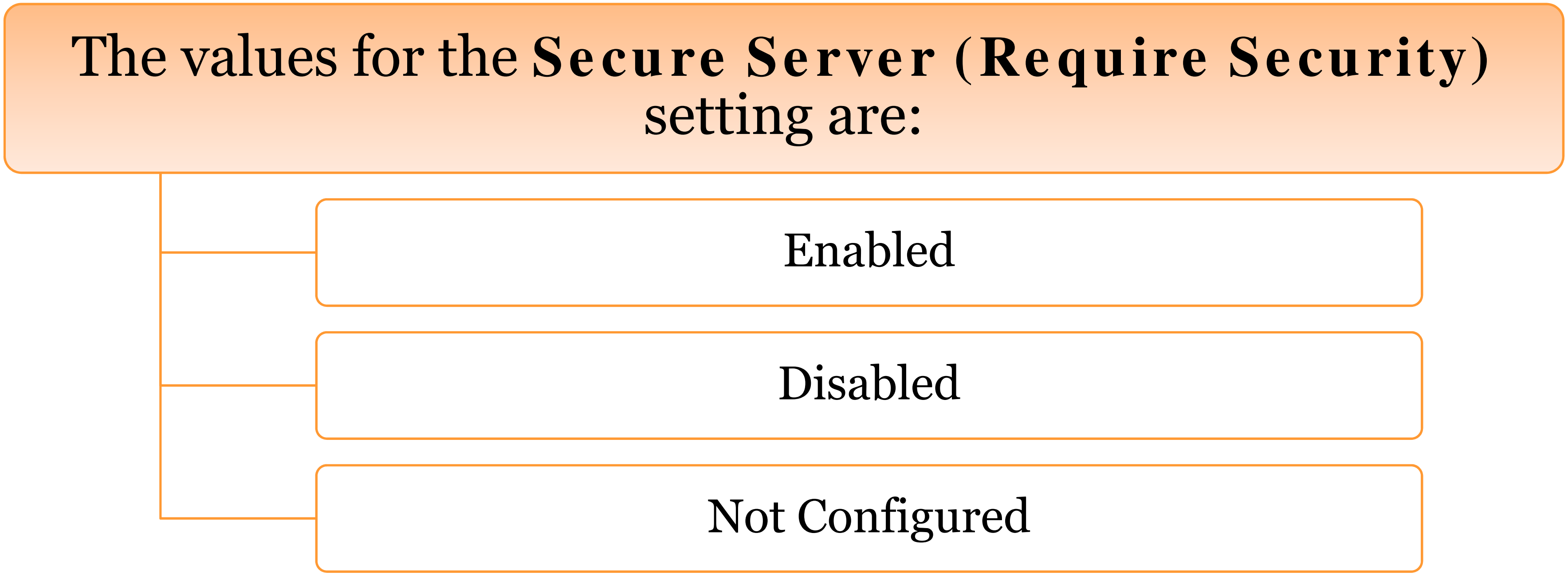
This setting decide that a Terminal Server needs secure remote procedure call (RPC) communication with all clients or allows unsecured communication

Using RPC the communication can be made more secure

If enabled, the request from a RPC clients are only accepted which has a secure request

If disabled, the requests are accepted at any level of security for all RPC traffic

Secure Server (Require Security) (Cont'd)



The values for the **Secure Server (Require Security)** setting are:

- Enabled
- Disabled
- Not Configured

Secure Server (Require Security) (Cont'd)

Vulnerability

- By the un-secure RPC communication the server is exposed to the man-in-the-middle attack and data disclosure attack

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- Clients that do not support secure RPC will be unable to remotely manage the server

Sessions

Configure additional Terminal Server RPC Security settings in the following location:

- **Computer Configuration\Administrative Templates\Windows Components\Terminal Services Encryption and Security\Sessions**

Set Time Limit For Disconnected Sessions

A time limit can be set to the Terminal Server session, which is decided by this policy

The specified time is the maximum time that a disconnected session will remain active

If enabled, the session will be deleted after the specified time limit

If disabled, no time limit is specified for disconnected sessions.

The values for the **Set time limit for disconnected sessions** setting are:

EC-Council

Set Time Limit For Disconnected Sessions (Cont'd)

The values for the **Set time limit for disconnected sessions setting** are:

Enabled with time specification options for:

- Never
- 1 minute
- 5 minutes
- 10 minutes
- 15 minutes
- 30 minutes
- 1 hour
- 2 hours
- 3 hours
- 1 day
- 2 days

Disabled

Not Configured

Set Time Limit For Disconnected Sessions (Cont'd)

Vulnerability

- Every Terminal Server session will use system resources.

Countermeasure

- Configure the setting to **Enabled** and select **1 day** as the option in the **End a disconnected session** list box.

Potential Impact

- The unclosed sessions will be forcibly disconnected after 24 hours of in-activity.

Allow Reconnection From Original Client Only

This policy decides whether the Terminal service will allow a user to connect to his session (disconnected) from a different computer rather than the one used for creating the session

The setting allows the user to do so

If enabled, user can only reconnect form the original client computer. If a user tries from another computer a new session is created

If disabled, user can connect from any computer

Allow Reconnection From Original Client Only (Cont'd)

The values for the **Allow reconnection from original client only** setting are:

- Enabled
- Disabled
- Not Configured

Allow Reconnection From Original Client Only (Cont'd)

Vulnerability

- By default, user can connect from any computer
- If enabled, user has to connect from the same computer used before

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- Users will connect to re-establish disconnected sessions with the computer that they used to establish the session

Windows Explorer

Configure the following Windows Explorer setting in the following location:

- **Computer Configuration\Administrative Templates\Windows Components\Windows Explorer**

Turn Off Shell Protocol Protected Mode

This configures the amount of functionality for the shell protocol to open folders and launch files

In protected mode the functionality will not allow to open large set of files

If enabled, any application can open any folder or file

If disabled, it is set to protected mode and only some files and folders are opened

Turn Off Shell Protocol Protected Mode (Cont'd)

The values for the **Turn off shell protocol protected mode** setting are:

- Enabled
- Disabled
- Not Configured

Vulnerability

- This protocol allows application to open files and folders. This can access and file with malicious code, and may create a DoS condition

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- If enabled, Web pages that depend on use of the shell protocol will not function properly

Windows Messenger

Instant message can be sent to users on the network using Windows Messenger

The messages may include files and any attachments:

Configure the prescribed Windows Messenger setting in the following location:

- **Computer Configuration\Administrative Templates\Windows Components\Windows Messenger**

Do not allow Windows Messenger to be run

- The policy setting allows the user to disable Windows Messenger
- Configure this setting to **Enabled** to stop Windows Messenger

Windows Update

This is used to download new software update, drivers etc

Configure the Windows Update settings in the following location:

- Computer Configuration\Administrative Templates\Windows Components\

EC-Council

Configure Automatic Updates

This policy determines whether new updates are downloaded from Windows automatic update service or not

If enabled, the operating system will check when the computer is online and check for new updates

If disabled, updates will not take place automatically

Administrator can configure Automatic Updates through the Control Panel

The values for the **Configure Automatic Updates** setting are:

Configure Automatic Updates (Cont'd)

Enabled, with options in the **Configure automatic updating** list box for:

- **2. Notify before downloading any updates and notify again before installing them.** In this option the windows will alert the user by giving a message in the status bar about the updates availability. When user clicks it will start auto-download and again prompts the user after completion, to install the updates
- **3. Download the updates automatically and notify when they are ready to be installed.** This option will download the updates automatically without any interruption to the user and then asks for installation
- **4. Automatically download updates and install them on the schedule specified below.** The download and installation will be done as per a specific schedule. The computer will start downloading and installing and if necessary it will restart the computer all by itself

Configure Automatic Updates (Cont'd)

Disabled

Not Configured

If enabled, select one of the options (2, 3 or 4).

Configure Automatic Updates (Cont'd)

Vulnerability

- The setting help you ensure that the computers have most recent critical operating system updates and service packs installed

Countermeasure

- Configure the policy setting to **Enabled** and select **4**

Potential Impact

- Operating system will download and install at 03:00 A.M. daily

Reschedule Automatic Updates Scheduled Installations

This policy decides the time period to wait by the automatic updates before starting installation which was previously missed

IF enabled, any missed installation as per schedule will start as soon as the computer is started again

If disabled, the missed scheduled installation will take place with the next schedule installation

The values for the **Reschedule Automatic Updates scheduled installations** setting are:

- Enabled, with the option to specify a time between 1 to 60 minutes
- Disabled
- Not Configured

Reschedule Automatic Updates Scheduled Installations (Cont'd)

Vulnerability

- The automatic installations start after a time period when the computer restarts

Countermeasure

- Configure the setting to **Enabled** and specify 10 minutes

Potential Impact

- Automatic Updates will not start until 10 minutes after the computer restarts

System

Configure the prescribed System computer setting in the following location:

- **Computer Configuration\Administrative Templates\System**

Turn off Autoplay

Autoplay will start reading a drive as soon as a disk is inserted and will start the setup file or start a media player if the disk is audio disk

If enabled, it prevents the Autoplay functionality. Autoplay is disabled by default

Vulnerability

- At attacker can use this feature to execute a malicious program and hurt the computer

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- The setup files should be initialized and launched manually

Do Not Process The Run Once List

This policy ignores the run once list of programs which runs when Windows starts

If enabled, the run once list cannot be executed as it is the common way to attack

The values for the Do not process the run once list setting are:

- Enabled
- Disabled
- Not Configured

Do Not Process The Run Once List (Cont'd)

Vulnerability

- The programs in run once list can compromise the security of Windows XP client

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- If enabled, the users may loose some functionality
- This configuration may prevent some setup and installation programs

Logon

Configure the prescribed Logon computer settings in the following location:

Computer Configuration\Administrative Templates\System\Logon

Don't Display The Getting Started Welcome Screen At Logon

This policy is used to hide the welcome screen that is displayed when the user logs on

This policy is applicable to Windows 2000 Professional and Windows XP Professional

The operating systems Windows 2000 Server or Windows Server 2003 do not support this policy

The values for the **Don't display the Getting Started welcome screen at logon** setting are:

- Enabled
- Disabled
- Not Configured

EC-Council

Don't Display The Getting Started Welcome Screen At Logon (Cont'd)

Vulnerability

- The welcome screen helps in exploring the system features

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- Users will not see the welcome screen when logged on to the computers

Do Not Process The Legacy Run List

Lists of programs are executed when Windows XP starts

This list is stored in registry at the location:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

The values for the Do not process the legacy run list setting are:

- Enabled
- Disabled
- Not Configured

Do Not Process The Legacy Run List (Cont'd)

Vulnerability	• An unauthorized user can run a program each time Windows start and can cause harm to the computer
Countermeasure	• Configure the setting to **Enabled**
Potential Impact	• If enabled, programs like antivirus software and software distribution and monitoring software are prevented from execution

Group Policy

Configure settings in the following location to modify how group policy is processed:

- **Computer Configuration\Administrative Templates\System\Group Policy**

Internet Explorer Maintenance Policy Processing

This policy tells when IE maintenance policies are updated

This setting overrides the present settings followed while installing updates

To enabled, use the check box and change the options

Internet Explorer Maintenance Policy Processing (Cont'd)

The values for the **Internet Explorer Maintenance policy processing** setting are:

- **Enabled**
  - Allow processing across a slow network connection.
  - Do no apply during periodic background processing.
  - Process even if the Group Policy objects have not changed.
- **Disabled**
- **Not Configured**

Vulnerability

- Enable this policy and select **Process even if the Group Policy objects have not changed** option to make sure policies will be reprocessed even if they have not changed.

Internet Explorer Maintenance Policy Processing (Cont'd)

Countermeasure

- Configure the setting to **Enabled**
- Clear both of the check boxes for **Allow processing across a slow network** and **Do not apply during periodic background processing**
- Select the check box for **Process even if the Group Policy objects have not changed**

Potential Impact

- These policies are reapplied every time they are refreshed

IP Security Policy Processing

This policy decides when IP security policies are updated

If enabled, the provided check boxes are used to change the options

The values for the **IP security policy processing** setting are:

IP Security Policy Processing (Cont'd)

Enabled

- Allow processing across a slow network connection – Even the updates are being transmitted over a slow network. The updates process is carried
- Do not apply during periodic background processing – The updates to the effected policies are stopped in the background
- Process even if the Group Policy objects have not changed – Even if the policies have not been changed the updates and reapplies are processed

Disabled

Not Configured

IP Security Policy Processing (Cont'd)

Vulnerability

- Enable and set **Process even if the Group Policy objects have not changed** option to reprocess the policies even if there is not much change

Countermeasure

- Configure the **IP security policy processing** setting to **Enabled**
- Clear the **Do not apply during periodic background processing** check box
- Select the **Process even if the Group Policy objects have not changed** check box

Potential Impact

- The IP security policies are reapplied for every refresh

Registry Policy Processing

This policy decides when registry policies are updated

Enabled and use the checkbox to set the option

The values for the **Registry policy processing** setting are:

- Enabled with options for:
  - Do not apply during periodic background processing
  - Process even if the Group Policy objects have not changed
- Disabled
- Not Configured

Registry Policy Processing (Cont'd)

Vulnerability

- Enable and select the **Process even if the Group Policy objects have not changed** option for assurance that the policies will be reprocessed even if nothing is changed

Countermeasure

- Configure the setting to **Enabled.**
- Clear the **Do not apply during periodic background processing** check box
- Select the **Process even if the Group Policy objects have not changed** check box

Potential Impact

- For every refresh group policies are re applied

Security Policy Processing

This policy setting decides when security policies are updated

If enabled, use the checkbox to change the option

The values for the **Security policy processing** setting are:

- Enabled with options for:
  - Do not apply during periodic background processing
  - Process even if the Group Policy objects have not changed
- Disabled
- Not Configured

Security Policy Processing (Cont'd)

Vulnerability

- Enable the policy and select **Process even if the Group Policy objects have not changed** option to make sure that the policies will be reprocessed even if there is no change

Countermeasure

- Configure the setting to **Enabled**
- Clear the **Do not apply during periodic background processing** check box
- Select the **Process even if the Group Policy objects have not changed** check box

Potential Impact

- For every refresh group policies are re applied

Error Reporting

This policy lets administrators to manage the cabinet files created by DW.exe and redirect stop error reports to a local file server

This policy helps admin to figure the common errors faced by the users

You can configure the Error Reporting settings in the following location:

- **Computer Configuration\Administrative Templates\System\Error Reporting**

Display Error Notification

This policy setting is user to specify whether a user can send an error report or not.

By enabling the policy the user will get a message if an error occurs.

If **Report Errors** setting is enabled, the user can set to report the error or not.

If disabled, user will not get any option the report the error.

The values for the **Display Error Notification** setting are:

- Enabled
- Disabled
- Not Configured

Display Error Notification (Cont'd)

Vulnerability	- If disabled, the user will not see the error message
Countermeasure	- Configure the setting to **Disabled**
Potential Impact	- Users will not see error report messages when they are generated

Report Errors

This policy decides on reporting the errors

If enabled, the user can report the error when occurred

The values for the **Report Errors** setting are:

- Enabled
  - Do not display links to any Microsoft provided "more information" Web sites
  - Do not collect additional files
  - Do not collect additional machine data
  - Force queue mode for application error
  - Corporate upload file path
  - Replace instances of the word "Microsoft”

Report Errors (Cont'd)

The other values for the **Report Errors** setting are:

- Disabled
- Not Configured

The default configuration is Enable in Windows XP and Disable id Windows Server 2003.

EC-Council

Report Errors (Cont'd)

Vulnerability

- In default configuration, when an error occurs the office will send the error to Microsoft
- If disabled, it is difficult to Microsoft to identify and diagnose the bugs in the application
- In an organization an Corporate Error Reporting (CER) server will be maintained as when an error occur it is pointed to the server. The server will generate a report and will send the information to Microsoft

Countermeasure

- Configure the setting to **Enabled**
- Select the **Corporate upload file path** option to point to the UNC path for your organization's CER server

Potential Impact

- Error reporting will be enabled, the reports are sent to CER server

Internet Communications Management

The products in Windows family include many technologies that communicate with the internet and maximize ease-of-use

These technologies give many benefits, but this involves a risk as these communicate with site which admin needs to control

Distributed COM

COM gives computer wide access control list (ACLs)

This check is in addition to any access that is run against the server specific ACLs

If access failed, the call, activation, or launch request is denied

Manage the new DCOM security features in Windows XP SP2 and Windows Server 2003 SP1 in the following:

- **Computer Configuration\Administrative Templates\Windows Components\System\Distributed COM\Application Compatibility Settings**

Common Issues

In this section the two settings share common vulnerability, countermeasure, and potential impact information

Distributed COM (Cont'd)

Vulnerability

- The COM components written improperly can be attacked across the network, by which information can be reveled, DoS or privilege escalation attacks can rise

Countermeasure

- Use the **Allow local activation security check exemptions** and **Define Activation Security Check exemptions** settings in conjunction with the DCOM access control mechanisms to impose access and execution controls on DCOM components.

Potential Impact

- If DCOM access controls are added to existing applications, those applications may not work properly

Browser Menus

Through these settings individual features in IE can be Enabled or Disabled

Configured the policy settings in the following location:

- User Configuration\Administrative Templates\Windows Components\Internet Explorer\Browser menus

Disable Save This Program To Disk Option

Enable this settings user can click **Save This Program to Disk** button to download program files

If disabled, user will be informed the command is not available

The values for the **Browser menus: Disable Save this program to disk option** setting are:

- Enabled
- Disabled
- Not Configured

Disable Save this program to disk option (Cont'd)

Vulnerability

- Hostile code can be downloaded from Web sites

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- Users can not click **Save This Program to Disk** button to download program files

Attachment Manager

The Attachment Manager gives the behavior for file attachments in emails and web pages

This service categorizes files that are received and downloaded depending upon the file extension

This service defines files as High risk, Medium risk and Low risk

Attachment Manager (Cont'd)

The Attachment Manager service divides files into three classes:

- **High Risk**. Windows blocks user access to the file
- **Moderate Risk**. Windows prompts the user before it allows access to the file
- **Low Risk**. Windows will not prompt the user before it allows access to the file, regardless of the file's zone information

These policy settings can be configured in the following location:

- **User Configuration\Administrative Templates\Windows Components\Attachment Manager**

Inclusion List For High Risk File Types

This setting allows you to set the high risk file types

If the file is in high risk list, Windows blocks user access to the file

If the file is from Internet, Windows prompts the user before it allows access to the file

If enabled, you can create your own high risk list

If disabled, Windows uses its built-in list of high risk file types

The values for the **Inclusion list for high risk file types** setting are:

- Enabled (allows you to specify a comma-separated list of file extensions)
- Disabled
- Not Configured

Inclusion List For High Risk File Types (Cont'd)

Vulnerability

- If a user accidentally opens high risks file, these files could defect the computer and possibly the network

Countermeasure

- Configure the setting to **Enabled**
- Specify the additional file types that you want to control

Potential Impact

- If the file type is in more than one list then most restricted list will applied as a countermeasure

Inclusion List For Moderate Risk File Types

This setting allows you to set the moderate risk file types

If the file is in moderate risk list or Internet, Windows prompts the user before it allows access to the file

If enabled, you can create your own moderate risk list

If disabled, Windows uses its default list

The values for the **Inclusion list for moderate risk file types** setting are:

- Enabled (allows you to specify a comma-separated list of file extensions)
- Disabled
- Not Configured

Inclusion List For Moderate Risk File Types (Cont'd)

Vulnerability

- If a user accidentally opens high risks file, these files could defect the computer and possibly the network

Countermeasure

- Configure the setting to **Enabled**
- Specify the additional file types that you want to control

Potential Impact

- If the file type is in more than one list then most restricted list will applied as a countermeasure
- Use caution for moving high risk file types to the moderate risk list, as it will be easier for users to execute potentially risky files

Inclusion List For Low File Types

This setting allows you to set the low risk file types

If the file is in low risk list or Internet, Windows prompts the user before it allows access to the file

If enabled, you can create your own low risk list

If disabled, Windows uses its default list

The possible values for the **Inclusion list for low file types** setting are:

- Enabled (allows you to specify a comma-separated list of file extensions)
- Disabled
- Not Configured

Inclusion List For Low File Types (Cont'd)

Vulnerability

- If a user accidentally opens high risks file, these files could defect the computer and possibly the network

Countermeasure

- Configure the setting to **Enabled**
- Specify the additional file types that you want to control

Potential Impact

- If the file type is in more than one list then most restricted list will applied as a countermeasure
- Use caution for moving high risk file types to the low risk list, as it will be easier for users to execute potentially risky files

Trust Logic For File Attachments

The logic that windows use to find the risk in file attachment is given by this setting.

If enabled, the order in which Windows processes risk assessment data can be chosen.

If disabled, Windows uses its default trust logic.

The values for the **Trust logic for file attachments** setting are:

- Enabled
  - Looking at the file handler and type.
  - Preferring the file handler.
  - Preferring the file type.
- Disabled
- Not Configured

Trust Logic For File Attachments (Cont'd)

Vulnerability

- Attacker may mould a file to exploit vulnerability in a specific file handler

Countermeasure

- Configure the setting to **Enabled: Looking at the file handler and type**

Potential Impact

- Configure the **Trust logic for file attachments** setting to use both the file handler and type

Hide Mechanisms To Remove Zone Information

This setting allows the user to manually remove the zone information from a saved file attachment

If the zone information can be removed, users could open potentially dangerous file attachments that Windows had previously blocked

If enabled, windows hide the checkbox and unblock button

If disabled, Windows displays the checkbox and **Unblock** button

The values for the **Hide mechanisms to remove zone information** setting are:

- Enabled
- Disabled
- Not Configured

Hide Mechanisms To Remove Zone Information (Cont'd)

Vulnerability

- User can remove the location information which could be from an un-trusted location

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- Users can not remove the zone information from the file

Notify Antivirus Programs When Opening Attachments

This policy manages how registry antivirus programs are notified when attachments are opened

If enabled, Windows calls the registered antivirus programs to scan an opened file

If the antivirus program fails, the attachment is blocked from being opened

If disable, Windows does not call the registered antivirus programs when file attachments are opened

The values for the **Notify antivirus programs when opening attachments** setting are:

- Enabled
- Disabled
- Not Configured

Notify Antivirus Programs When Opening Attachments (Cont'd)

Vulnerability	• Antivirus programs which may not perform on-access check will not be able to scan download files
Countermeasure	• Configure the setting to **Enabled**
Potential Impact	• If enabled, all files and emails are scanned

Windows Explorer

This is used to navigate the file system on clients that run Windows XP Professional

Configure the prescribed Windows Explorer user settings in the following location:

- **User Configuration\Administrative Templates\Windows Components\Windows Explorer**

Remove Security Tab

The security tab on files and folders are disabled on properties dialog boxes in Windows Explorer

If enabled, users cannot access the **Security** tab

Users will not be able to change settings on the **Security** tab or view the list of users

Remove Security Tab (Cont'd)

Vulnerability

- Security tabs can be determined the account permission for any file system object
- Attackers can target those accounts to gain greater access

Countermeasure

- Configure the setting to **Enabled**

Potential Impact

- When the tab is enabled, users cannot view the security tab for file system objects or review permissions

System\Power Management

Configure the prescribed **System\Power Management** user setting in the following location:

- **User Configuration\Administrative Templates\System\Power Management**

Prompt for password on resume from hibernate / suspend

- This policy controls that the client computer is locked when they are resumed from hibernate or suspend state.
- If enabled, the client computers are locked and users must provide passwords to unlock.
- If disabled, a potential for a serious security breach, because the client computers may be accessed by anyone after they resume operation.

Additional Registry Entries

It provides additional information about registry entries for the base line security template file

Customized Security Configuration Editor

- When MMC (Microsoft Management Console) security templates snap-in the entries in the security template cannot be represented
- The entries are added to .inf file using Security Configuration Editor (SCE)
- To automate any changes the entries are embedded in the security templates
- By removing this policy the changes have to be made manually by using the tool such as Regedt32.exe

How to Modify the Security Configuration Editor User Interface

This is used to define security templates for any number of computers

These templates can contain:

- Password policies
- Lockout policies
  - Kerberos protocol policies
- Audit policies
- Event log settings
- Registry values
- Service startup modes
- Service permissions
- User rights

How to Modify the Security Configuration Editor User Interface (Cont'd)

These templates also can contain:

- Group membership restrictions
- Registry permissions
- File system permissions

SCE appears in MMC snap-ins and administrator tools, used by the Security Templates snap-in and the Security Configuration and Analysis snap-in

Additional entries are added to SCE using Seregvi.inf

How to Modify the Security Configuration Editor User Interface (Cont'd)

The original security settings are in Policies\Security in the snap-ins and tools

The file sceregvi.inf should be updated and re-register the file Scecli.dll

Once the file Sceregvl.inf has been modified and registered, the custom registry values are uncovered in the SCE user interfaces on that computer

How to Modify the Security Configuration Editor User Interface (Cont'd)

To manually update sceregvl.inf

- Use a text editor (Notepad) to open the Values-sceregvl.txt file from the SCE Update folder of the download for this guide
- Open another window in the text editor and then open the %systemroot%\inf\sceregvl.inf file
- Navigate to the bottom of the "[Register Registry Values]" section in the sceregvl.inf file. Copy and paste the text from the Values-sceregvl.txt file, without any page breaks, into this section of the sceregvl.inf file
- Close the Values-sceregvl.txt file and open the Strings-sceregvl.txt file from the SCE Update folder of the download

How to Modify the Security Configuration Editor User Interface (Cont'd)

To manually update sceregvl.inf

- Navigate to the bottom of the "[Strings]" section in the **sceregvl.inf** file. Copy and paste the text from the Strings-sceregvl.txt file, without any page breaks, into this section of the **sceregvl.inf** file.
- Save the **sceregvl.inf** file and close the text editor.
- Open a command prompt and execute the command **regsvr32 scecli.dll** to re-register the DLL file.

The custom registry values are displayed by the subsequent launch of SCE.

How to Modify the Security Configuration Editor User Interface (Cont'd)

To automatically update sceregvl.inf

The **Values-sceregvl.txt, Strings-sceregvl.txt,** and **Update_SCE_with_MSS_Regkeys.vbs** files that are located in the **SCE Update** folder of the download for this guide must all be in the same location for the script to function.

Execute the **Update_SCE_with_MSS_Regkeys.vbs** script on the computer you wish to update.

Follow the onscreen prompts

How to Modify the Security Configuration Editor User Interface (Cont'd)

The below process will remove custom entries, using this the changes made by automatic update script cab be modified:

To reverse the changes made by the Update_SCE_with_MSS_Regkeys.vbs script

- Execute the **Rollback_SCE_for_MSS_Regkeys.vbs** script on the computer you wish to update.
- Follow the onscreen prompts

How to Modify the Security Configuration Editor User Interface (Cont'd)

The below process will remove custom entries added to SCE user interface.

To restore the SCE to its default state for Windows XP with SP2 Windows Server 2003 with SP1

- The **sceregvl_W2K3_SP1.inf.txt, sceregvl_XPSP2.inf.txt,** and **Restore_SCE_to_Default.vbs** files that are located in the **SCE Update** folder of the download for this guide must all be in the same location for the script to function.
- Execute the **Restore_SCE_to_Default.vbs** script on the computer you wish to update.
- Follow the onscreen prompts

How to Modify the Security Configuration Editor User Interface (Cont'd)

To manually restore the SCE user interface to its default appearance

- Click **Start**, **Run**, type **regedit.exe** and press ENTER to open the Registry Editor tool
- Navigate to **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\SecEdit\Reg Values**
- Each subkey in this location represents one item in the Security Options section of the SCE. Carefully delete all of the subkeys. **Do not delete the parent key** (Reg Values), but only the subkeys that are contained within it
- Open a command prompt and execute the command **regsvr32 scecli.dll** to re-register the SCE DLL
- Subsequent launches of the SCE will only display the original registry values that were included with your version of Windows

TCP/IP-Related Registry Entries

The computer has to be up to date with latest security fixes, to prevent DoS (Denial of Service) attack

The default TCP/IP stack configuration is tuned to handle standard intranet traffic

The DoS attacks directed at TCP/IP stack are of two classes:

Attack that spend many system resources

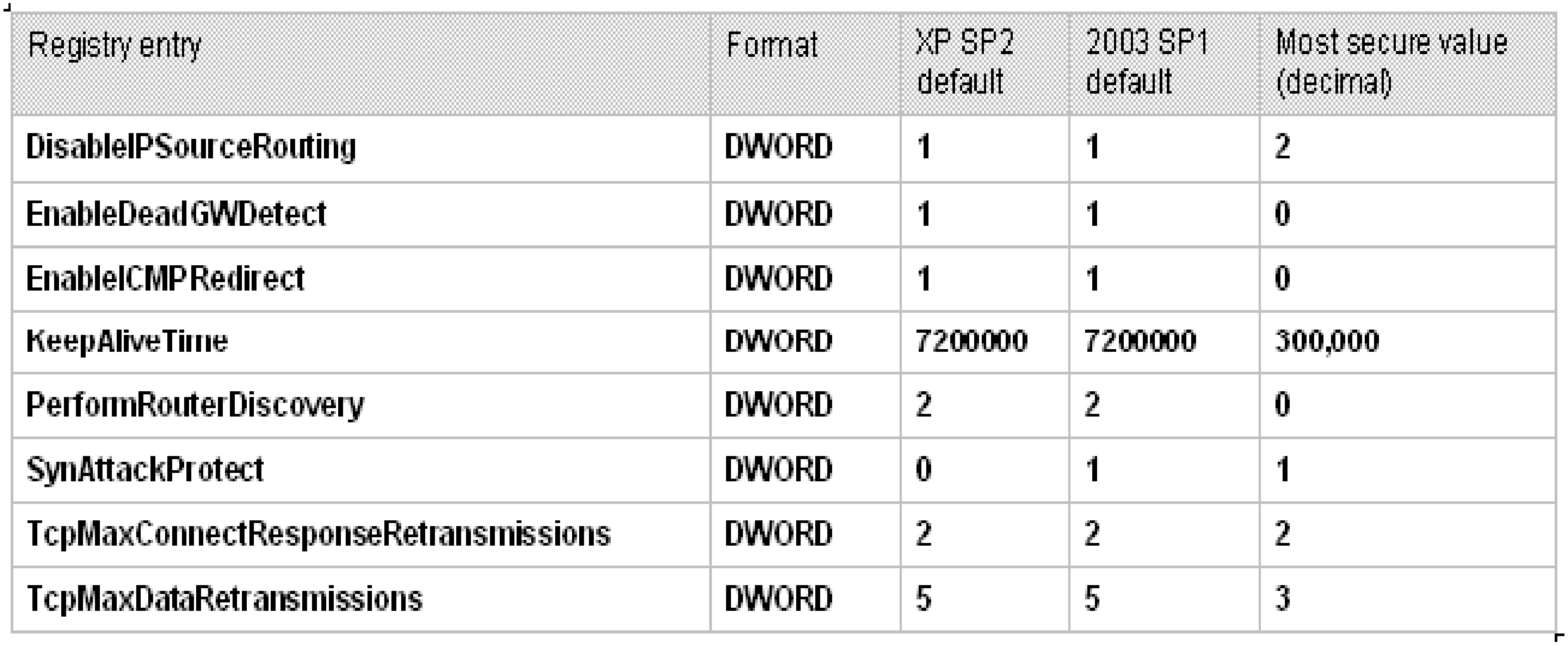
Attacks that send specially crafted packets causing the network stack or the entire operating system to fail

TCP/IP-Related Registry Entries (Cont'd)

The following registry settings help to protect against the attacks that are directed at the TCP/IP stack

The registry settings in the following table were added to the template file in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\ subkey

TCP/IP-Related Registry Entries (Cont’d)



Registry entry	Format	XP SP2 default	2003 SP1 default	Most secure value (decimal)
DisableIPSourceRouting	DWORD	1	1	2
EnableDeadGWDetect	DWORD	1	1	0
EnableICMPRedirect	DWORD	1	1	0
KeepAliveTime	DWORD	7200000	7200000	300,000
PerformRouterDiscovery	DWORD	2	2	0
SynAttackProtect	DWORD	0	1	1
TcpMaxConnectResponseRetransmissions	DWORD	2	2	2
TcpMaxDataRetransmissions	DWORD	5	5	3

Disableipsourcerouting: IP Source Routing Protection Level (Protects Against Packet Spoofing)

This entry appears as MSS: (DisableIPSourceRouting) IP source routing protection level **in the SCE**

It is a process which allows the sender to find the IP route followed by a datagram through a network

Vulnerability

- The source routing packets can be used by an attacker to identify the location

EC-Council

Disableipsourcerouting: IP Source Routing Protection Level (Protects Against Packet Spoofing) (Cont'd)

Countermeasure

- **Configure the** MSS: (DisableIPSourceRouting) IP source routing protection level entry to a value of Highest protection, source routing is completely disabled
- **The possible values for the registry entry are:**
  - 0, 1, or 2. The default configuration is 1 (source routed packets are not forwarded)
- **In the SCE UI,** this list of options appears:
  - No additional protection, source routed packets are allowed
  - Medium, source routed packets ignored when IP forwarding is enabled
  - Highest protection, source routing is completely disabled
  - Not Defined

Potential Impact

- If this value is configured to 2, incoming source routed packets will be dropped

Enabledeadgwdetect: Allow Automatic Detection Of Dead Network Gateways (Could Lead To Dos)

It allows automatic detection of dead network gateways in SCE.

If enabled, and the number of connections experience difficulty the IP will change to a backup gateway.

Vulnerability

- An attack makes the server to switch gateways, probable to an unintended one.

Enabledeadgwdetect: Allow Automatic Detection Of Dead Network Gateways (Could Lead To Dos)

Countermeasure

- This setting allows automatic detection of dead network gateways entry to a value of disabled
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration is 1 (enabled) on Windows Server 2003
- **In the SCE UI, these options appear as:**
  - Enabled
  - Disabled
  - Not Defined

Potential Impact

- If configured to 0, Windows cannot detect dead gateways and switches to alternates

Enableicmpredirect: Allow ICMP Redirects To Override OSPF Generated Routes

This entry allows ICMP redirects to override OSPF generated routes in the SCE

The host routes are pumped by redirecting ICMP (Internet Control Message Protocol)

These routes re-write Open Shortest Path First (OSPF)-generated routes

Vulnerability

- This is an expected behavior that a 10 minute time-out period for the ICMP redirect-plumbed routes temporarily creates a network situation through which traffic is no longer routed properly for host

Enableicmpredirect: Allow ICMP Redirects To Override OSPF Generated Routes

Countermeasure

- Configure this entry to Disabled
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration is 1 (enabled)
- **In the SCE UI, these options appear as:**
  - Enabled
  - Disabled
  - Not Defined

Potential Impact

- The connected interface subnet routes are not imported accurately as RRAS (Routing and Remote Access) is configured as an ASBR (autonomous system boundary router)

Keepalivetime: How Often Keep-alive Packets Are Sent In Milliseconds (300,000 Is Recommended)

This decides how often keep-alive packets are sent in milliseconds in the SCE

A keep-alive packet is sent by TCP to check that an idle connection is still intact

Vulnerability

- An attacker can start many connections to start a DoS condition

Countermeasure

- Configure this value to 300000 or 5 minutes
- **The possible values for this registry entry are:**
- 1 through 0xFFFFFFFF. The default configuration is 7,200,000 (two hours)

Keepalivetime: How Often Keep-alive Packets Are Sent In Milliseconds (300,000 Is Recommended)

In the SCE UI, the following list of options appears:

- 150000 or 2.5 minutes
- 300000 or 5 minutes (**recommended**)
- 600000 or 10 minutes
- 1200000 or 20 minutes
- 2400000 or 40 minutes
- 3600000 or 1 hour
- 7200000 or 2 hours (**default value**)
- Not Defined

Potential Impact

Some applications may need keep-active packets by default and that configures TCP stack flag

For this process the value can be changed from 5 minutes to two hours

Synattackprotect: Syn Attack Protection Level (Protects Against Dos)

This entry protects system again DoS. It adjusts TCP for retransmission of SYN-ACKs

The overhead of incomplete transmission in a connect request attack is minimized by setting this request

By this setting Windows send messages as broadcast rather than multicast

Vulnerability

- In SYN flood attack the attacker sends SYN packets to a server which leaves an half open connection until load increases and will not be able to respond a genuine request

Synattackprotect: Syn Attack Protection Level (Protects Against Dos) (Cont'd)

Countermeasure

- **Configure this entry** to Connections time out
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration is 1 (enabled) for Windows Server 2003 SP1 and 0 (disabled) for Windows XP SP2
- **In the SCE UI, these options appear as:**
  - Connections time out more quickly if a SYN attack is detected
  - No additional protection, use default settings
  - Not Defined

Potential Impact

- This value increases connection delay and TCP connection request quickly time out when an SYN attack is in progress

Tcpmaxconnectresponseretransmissions: SYN-ACK Retransmissions When A Connection Request Is Not Acknowledged

This entry retransmits when a connection request is not acknowledged in the SCE

The number of times the TCP retransmits a SYN before stopping the attempt

Vulnerability

- In SYN flood attack the attacker sends SYN packets to a server which leaves an half open connection until load increases and will not be able to respond a genuine request

Tcpmaxconnectresponseretransmissions: SYN-ACK Retransmissions When A Connection Request Is Not Acknowledged (Cont'd)

Countermeasure

- Configure this to a value of 3 seconds, half-open connections dropped after nine seconds
- The possible values for this registry entry are:
  - 0-0xFFFFFFFF. The default configuration is 2
- In the SCE UI, the following options appear and correspond to a value of 0, 1, 2, and 3, respectively:
  - No retransmission, half-open connections dropped after 3 seconds
  - 3 seconds, half-open connections dropped after 9 seconds
  - 3 & 6 seconds, half-open connections dropped after 21 seconds
  - 3, 6, & 9 seconds, half-open connections dropped after 45 seconds
- Not Defined

Potential Impact

- If the value is more than 2, a SYN attack will be employed internally
- If the value is less than 2, the registry values cannot be read
- If the value is 0, Syn-ATKs will not be retransmitted, and will be out by 3 seconds

Tcpmaxdataretransmissions: How Many Times Unacknowledged Data Is Retransmitted (3 Recommended, 5 Is Default)

This entry decides how many times the unacknowledged data is retransmitted in the SCE. It controls the count of the retransmitting data connection before aborting.

The retransmission time is doubled every time a retransmission is issued.

Vulnerability

- A user can weaken the sender by not replying with an acknowledgement message for the transmitted data.

Tcpmaxdataretransmissions: How Many Times Unacknowledged Data Is Retransmitted (3 Recommended, 5 Is Default)

Countermeasure

- **Configure this entry to a value of 3. The possible values for this registry entry are:**
  - 0 to 0xFFFFFFFF. The default configuration is 5
- **In the SCE UI, this setting can be adjusted using a text entry box:**
  - A user-defined number
- Not Defined

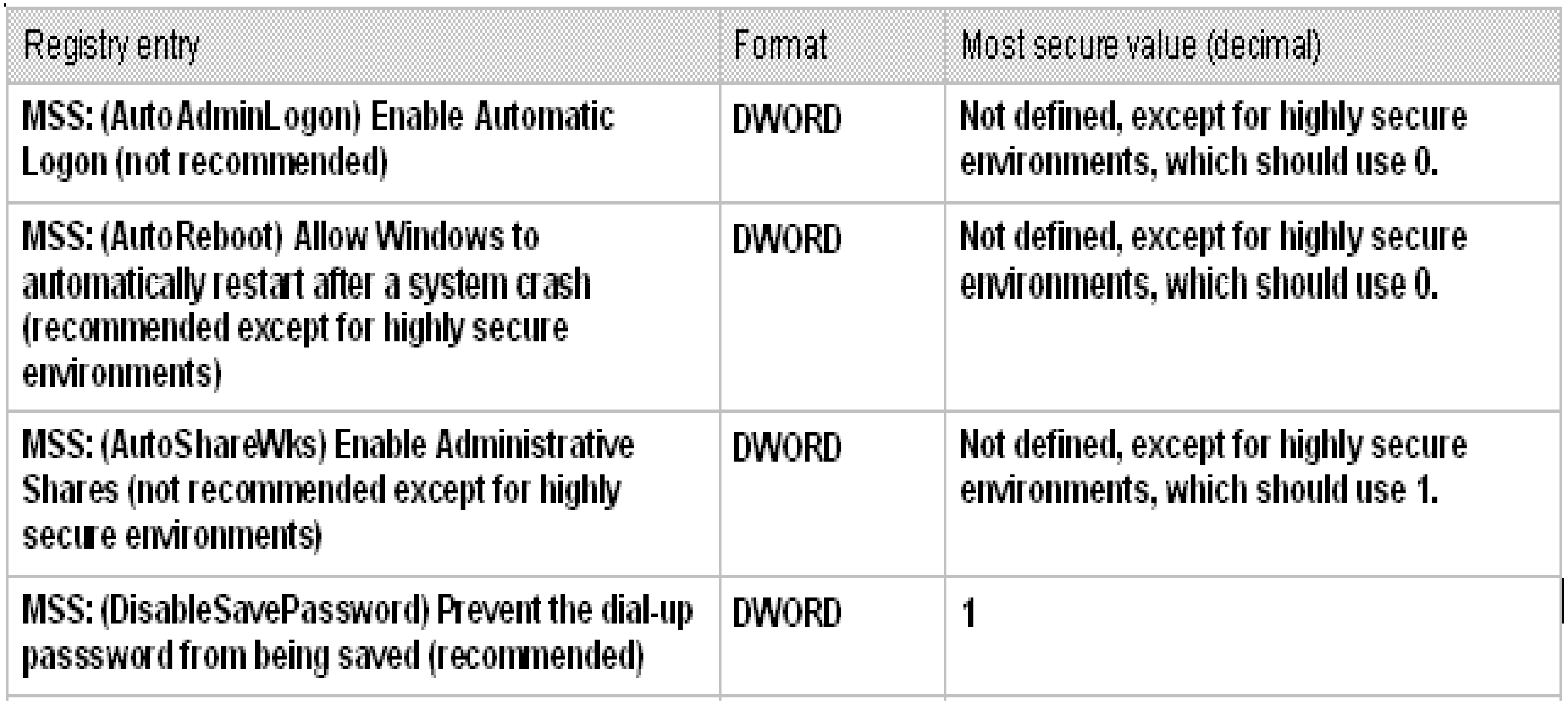
Potential Impact

- TCP start a timer when a transmission starts and if no acknowledgement is sent back, retransmission is issued for 3 times

EC-Council

Miscellaneous Registry Entries

The registry entries in the table are recommended:



Registry entry	Format	Most secure value (decimal)
MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	DWORD	Not defined, except for highly secure environments, which should use 0.
MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)	DWORD	Not defined, except for highly secure environments, which should use 0.
MSS: (AutoShareWks) Enable Administrative Shares (not recommended except for highly secure environments)	DWORD	Not defined, except for highly secure environments, which should use 1.
MSS: (DisableSavePassword) Prevent the dial-up passsword from being saved (recommended)	DWORD	1

Miscellaneous Registry Entries (Cont'd)

MSS: (Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments)	DWORD	Not defined, except for highly secure environments, which should use 1.
MSS: (NoDefaultExempt) Enable NoDefaultExempt for IPSec Filtering (recommended)	DWORD	1 for computers that run Windows XP, 3 for computers that run Windows Server 2003.
MSS: (NoDriveTypeAutoRun) Disable Autorun for all drives (recommended)	DWORD	0xFF
MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers (Only recommended for servers)	DWORD	1
MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames (recommended)	DWORD	1
MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)	DWORD	1
MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)	String	0
MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning	DWORD	0

Configure Automatic Reboot from System Crashes

This entry allows windows to automatically restart after a system crash in the SCE

This finds whether the system restarts automatically or not

You can add this registry value to the template file in the

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl\ **subkey**

Vulnerability

- In some situations computer could struck in an end less loop of failures and reboots. The measure to this is just to stop running the computer

Configure Automatic Reboot from System Crashes (Cont'd)

Countermeasure

- Configure this to Disabled.
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration is 1 (enabled).
- **In the SCE UI, the following options are available:**
  - Enabled
  - Disabled
  - Not Defined

Potential Impact

- The computer will no longer reboot automatically after a failure.

Enable Administrative Shares

This entry enables administrative Shares in the SCE.

By default, Windows XP Professional creates admin shares automatically.

You can add this registry value to the template file in the

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\ **subkey.**

Vulnerability

- These shares are available in all computers; a user can access them to find out password by a brute force attack.

Enable Administrative Shares (Cont’d)

Countermeasure

- Do not configure this entry to Enabled
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration is 1 (enabled).
- **In the SCE UI, these options appear as:**
  - Enabled
  - Disabled
  - Not Defined

Potential Impact

- If these shares are deleted, problem can be created for administrators and the files using the shares

Disable Saving of Dial-Up Passwords

This entry prevents from the dial-up password to be saved in the SCE

You can add this registry value to the template in the

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters\ **subkey**

Vulnerability

- If this entry is enabled, an attacker can connect to the network by steeling a mobile user computer

EC-Council

Disable Saving of Dial-Up Passwords (Cont'd)

Countermeasure

- Configure this entry to Disabled
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration is 0 (disabled)
- **In the SCE UI, the following options are available:**
  - Enabled
  - Disabled
  - Not Defined

Potential Impact

- The logon credentials (dial-up and VPN) of the users can not be stored automatically

Hide the Computer from Network Neighborhood Browse Lists: Hide Computer From the Browse List

This entry hides computers from the browser list in the SCE

Configure a computer not to send announcements to browser as if it is done the computer will be hidden from the browser list

You can add this registry value to the template file in the

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Lanmanserver\Parameters\ **subkey**

Vulnerability

- If enabled, this will help in reducing traffic and removes the a method that an attacker can use

Hide the Computer from Network Neighborhood Browse Lists: Hide Computer From the Browse List (Cont'd)

Countermeasure

- Do not configure this entry to Enabled.
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration is 0 (disabled).
- **In the SCE UI, these options appear as:**
  - Enabled
  - Disabled
  - Not Defined

Potential Impact

- The computer will not appear on any other computer or network.

Configure Netbios Name Release Security: Allow the Computer to Ignore Netbios Name Release Requests Except from WINS Servers

This entry allows the computer to ignore NetBIOS name release request exception from WINS server in SEC

You can add this registry value to the template file in the

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\ **subkey**

Vulnerability

- The NetBT protocol do not use authentication and is vulnerable to spoofing.
- An attacker can send a name conflict datagram, to give up and not to respond the query

Configure Netbios Name Release Security: Allow the Computer to Ignore Netbios Name Release Requests Except from WINS Servers (Cont'd)

Countermeasure

- Configure this entry to Enabled
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration is 1 (enabled).
- **In the SCE UI, these options appear as:**
  - Enabled
  - Disabled
  - Not Defined

Potential Impact

- An attacker sends a request on network to release its NetBIOS name

Enable Safe DLL Search Order: Enable Safe DLL Search Mode (Recommended)

This entry enables safe DLL search mode in the SCE

The order for DLL search order can be configured as:

If SafeDllSearchMode is configured to 1, the search order is as follows:

- The directory from which the application loaded
- The system directory
- The 16-bit system directory. There is no function that obtains the path of this directory, but it is searched

EC-Council

Enable Safe DLL Search Order: Enable Safe DLL Search Mode (Recommended) (Cont'd)

If SafeDllSearchMode is configured to 1:

- The Windows directory
- The current directory
- The directories that are listed in the PATH environment variable

If SafeDllSearchMode is configured to 0, the search order is as follows:

- The directory from which the application loaded
- The current directory
- The system directory
- The 16-bit system directory. There is no function that obtains the path of this directory, but it is searched

Enable Safe DLL Search Order: Enable Safe DLL Search Mode (Recommended) (Cont'd)

If SafeDllSearchMode is configured to 0:

- The Windows directory
- The directories that are listed in the PATH environment variable

You can add this registry value the template file in the

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\ **subkey**

Vulnerability

- If an user accidentally executes some bad code, it could increase the type and degree of damage that can be rendered

Enable Safe DLL Search Order: Enable Safe DLL Search Mode (Recommended) (Cont'd)

Countermeasure

- Configure this entry to Enabled
- **The possible values for this registry entry are:**
  - 1 or 0. The default configuration for Windows XP it is 0 and 1 for Windows Server 2003
- **In the SCE UI, these options appear as:**
  - Enabled
  - Disabled
  - Not Defined

Potential Impact

- Applications are forced to search for DLLs in the system path

Security Log Near Capacity Warning: Percentage Threshold for the Security Event Log at which the System will Generate a Warning

This entry will generate a percentage for the security event log for the generated warnings in the SCE

You can add this registry value to the template file in the

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\ **subkey**

Vulnerability

- If the log capacity reaches to 90 percent and it is configured not to overwrite events the recent events will not be written and if the log capacity is exceeded the system can even shut down if it is configured to do so

Security Log Near Capacity Warning: Percentage Threshold for the Security Event Log at which the System will Generate a Warning (Cont'd)

Countermeasure

- Configure this entry to a value of 90.
- **The possible values for this registry entry are:**
  - 0 to 100. The default configuration is 0 (no warning event is generated).
- **In the SCE UI, the following options are available:**
  - 50%
  - 60%
  - 70%
  - 80%
  - 90%
- Not Defined

Potential Impact

- System generates an audit event when log reaches 90 percent

Registry Entries Available In Windows XP With SP2 And Windows Server 2003 With SP1

The following registry events are for both Windows XP with SP2 and Windows Server 2003 with SP1.n RestrictRemoteClients

The RestrictRemoteClients registry key makes RPC to perform additional security checks

The **RestrictRemoteClients** registry key can have one of three DWORD values:

- **0** . This is a default value and it makes the computer to bypass the RPC interface restriction
- **1**. This is the default value in Windows XP with SP2. It makes all remote un-known calls to be rejected by the RPC runtime
- **2** . All remote un-known calls are rejected by the RPC

Registry Entries Available In Windows XP With SP2 And Windows Server 2003 With SP1 (Cont'd)

The applications passing flags can be modified to the RPC sub system which shows that the default client and server accept un-known RPC requests.

Vulnerability

- Corrupted code can be spread by exploiting buffer remotely

Countermeasure

- The RestrictRemoteClient have a default configuration which can allow backward compatibility
- Configure RestrictRemoteClient to 1 or 2

Potential Impact

- If enabled, un-known user cannot access the RPC Endpoint Mapper Interface

RunInvalidSignatures

This prevents the installation of code which has invalid signatures

Internet Explorer 6.0 blocks the installation of signed code with invalid signatures

The service pack shows this action to all applications

Vulnerability

- A control which has been corrupted may be downloaded and run

RunInvalidSignatures (Cont'd)

Countermeasure	• The default value of RunInvalidSignatures blocks this vulnerability
Potential Impact	• Applications which are legitimately signed will not function if there signature is invalid

Registry Entries Available in Windows XP with SP2

These registry entries are available only in Windows XP with SP2

Security Center Registry Entries for XP

Registry values for security centre determining whether the user receives alerts for the feature

If the key has a value of 0, **the notification icon and alert system for that feature are enabled**

- **These values are in** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center:
  - **AntiVirusDisableNotify**
  - **FirewallDisableNotify**
  - **UpdatesDisableNotify**

Security Center Registry Entries for XP (Cont'd)

Vulnerability

- If the alert feature is disabled for some users they will not receive any warnings

Countermeasure

- **Apply a Group Policy registry entry to implement the warning configuration**

Potential Impact

- If Security Centre functionality is enabled, the values are visible in Security Centre user interface

StorageDevicePolicies\WriteProtect

By default the USB device can be mounted and users can use it without any limit

If necessary this ability can be restricted, To do so add WriteProtect DWORD value to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies and configure it to 1

StorageDevicePolicies\WriteProtect (Cont'd)

Vulnerability

- An attacker could copy data to a removable USB device and steal it

Countermeasure

- When the WriteProtect value is set to 1, Windows XP with SP2 will block writes to USB block storage devices

Potential Impact

- There are other ways that a skilled attacker to steal data with a USB device

Registry Entries Available in Windows Server 2003 with SP1

These registry entries are available only in Windows Server 2003 with SP1

UseBasicAuth

Distributed Authoring and Versioning (DAV) is an HTTP–based protocol which allows remote access to file systems and file servers

The UNC path can be used to access files on DAV server

Windows Server 2003 SP1 introduces the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters\UseBasicAuth subkey

If it is configured to 1, the WebDAV can communicate with web servers which support basic authentication

UseBasicAuth (Cont'd)

Vulnerability

- Attackers can setup Web servers with basic authentication and trick or spoof user attempt to connect it to capture their credentials.

Countermeasure

- By default the WebDAV will not use basic authentication.

Potential Impact

- Applications supporting WebDAV to access web resources will fail if web server only support authentication.

DisableBasicOverClearChannel

The WebDAV redirector is part of remote file system stack

When user opens an URL the credentials may be exposed if the server support only basic authentication

The UseBasicAuth registry entry controls whether basic authentication can be used for WebDAV requests. If you configure the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters\DisableBasicOverClearChannel** value to 1, the use of basic authentication with other Web resources is blocked

DisableBasicOverClearChannel (Cont'd)

Vulnerability

- A Web Server can be setup by the attacker which uses basic authentication
- They make the users to connect it to capture their credentials

Countermeasure

- Configure the DisableBasicOverClearChannel value to 1 on client computers

Potential Impact

- Embedded devices offering HTTP access only supports basic authentication

Additional Countermeasures

This describes the implementation of security accounts for additional countermeasures

Member Server Hardening Procedures

- Most of the counter measures can be applied by Group Policy; some additional measures are difficult or impossible to apply through this

Securing the Accounts

The most known built in account in Windows Server 2003 are Guest and Administrator, these accounts can be renamed but not deleted

Vulnerability

- By default, the guest account is disabled on the computers. The configuration should not be changed
- In the built in administrator account attackers may attempt to comprise a server. To overcome the admin account name should be changed
- This kind of attacks is minimized as the account is not much recognized by its name but by its SID
- This value uniquely identifies each user, group, and computer account and logon session on a network

Securing the Accounts (Cont’d)

Countermeasure

- Change the Administrator account and change the password to a long & complex value on every server.
- To rename the account, configure the Rename administrator account setting in Group Policy at the following location:
- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security\Options
- If the organization uses same account names and passwords on all of the servers, attacker who gains access to one member server will be able to gain access to all others.

Securing the Accounts (Cont'd)

Potential Impact

- The users must keep track on what account name is assigned to each computer as to manage the computer

NTFS

The NTFS partitions support access control list (ACL's) and encryption

The support is not available with the file allocation table (FAT), FAT32, or FAT32x file systems

Vulnerability

- Files which are not protected by ACLs can be accessed, modified and deleted by unauthorized users
- In this the encryption gives more protection and is more viable to files that are accessed by a single user

NTFS (Cont'd)

Countermeasure

- Format all drives on each server to NTFS from FAT, but this gives full control on the ACLs on the converted drives
- Apply following security templates to configure the default file system ACLs:
  - **For workstations.** %windir%\inf\defltwk.inf
  - **For servers.** %windir%\inf\defltsv.inf
  - **For domain controllers.** %windir%\inf\defltdc.inf

Potential Impact

- No negative impact is detected

NTFS (Cont'd)

Microsoft recommends the following additional technologies that can help lessen the impact of these types of attacks:

- Use Syskey with an offline password to prevent startup of the Windows operating system by unauthorized persons.
- Use EFS to encrypt user data. Instruct users to use their domain accounts and either configure no recovery agent or configure it for domain administrator accounts rather than the local administrator account.
- Use BIOS passwords to deny unauthorized users the ability to start computers within your organization.
- Configure the system BIOS to disable the ability of computers to start from CD-ROM drives and floppy disk drives. This configuration will deny the ability of unauthorized users to start computers with their own operating system.

Data and Application Segmentation

Locate the data, application and log files on separate storage device to improve performance

By this you can prevent an attack of Directory Traversal account

Vulnerability

- If application, data and log files are located on the same storage device: Two vulnerabilities are detected
  - The users may accidentally or deliberately fill an application log file or upload files to the server and fill the storage volume with data
  - A directory traversal exploit, in which an attacker takes advantage of a bug in a network service to navigate the directory tree to the root of the system volume to execute a utility remotely

Data and Application Segmentation (Cont'd)

Countermeasure

- If possible relocate web contents, applications log files to a separate partition from the system volume

Potential Impact

- The impact would be less for organizations maintaining the server consistently

Configure SNMP Community Name

SNMP (**Simple Network Management Protocol**) is a network management standard widely used is TCP/IP networks. It provides a way to manage networks

Computers running network management software SNMP management systems or SNMP managers

Vulnerability

- SNMP is week in the view of security, that is all vendors set a default community string name
- When connecting SNMP management device to client the data is in-secured as SNMP traffic is sent in plaintext, without encryption

Configure SNMP Community Name (Cont'd)

Countermeasure

- Configure the SNMP community string for read access on all computers to a random alphanumeric value.
  - At the Services console, double-click **SNMP Service**.
  - Click the **Security** tab on the **SNMP Service Properties** dialog box.
  - Select **public** from the **Accepted community names** list.
  - Click the **Edit** button, and then type the new community name in the **SNMP Service Community Name** dialog box when it appears.
  - Click the **OK** button to close each of the dialog boxes.
- Leave write access through SNMP disabled.

Configure SNMP Community Name (Cont'd)

Countermeasure

- The community name is stored in the registry as a registry value with a DWORD value of 4 The value is stored in: HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities

Potential Impact

- Also configure community string for all management tools using SNMP protocol

Disable NetBIOS and SMB on Public Facing Interfaces

It discusses about servers which are not fully controlled as publicly accessible web servers and email gateways

Vulnerability

- If server message block and NetBIOS on TCP/IP are disabled, a servers attack chances are reduced
- The measures will protect servers from compromise through the SMB and NetBIOS

Disable NetBIOS and SMB on Public Facing Interfaces (Cont'd)

Countermeasure

- The SMB will be in use even if NetBIOS will be disabled as it uses port 445
- So the necessary steps should be taken to disable SMB
- **NetBIOS uses the following ports:**
  - UDP/137 (NetBIOS name service)
  - UDP/138 (NetBIOS datagram service)
  - TCP/139 (NetBIOS session service)
- **SMB uses the following ports:**
  - TCP/139
  - TCP/445
- For accessing servers form internet, remove file and printer sharing for Microsoft Network and Client

Disable NetBIOS and SMB on Public Facing Interfaces (Cont'd)

To disable SMB

- In Control Panel, double-click **Network Connections**
- Right-click any Internet facing connection, and then click **Properties**
- In the **Properties** dialog box, click select **Client for Microsoft Networks**, and then click **Uninstall**
- Follow the uninstall steps
- Select **File and Printer Sharing for Microsoft Networks**, and then click **Uninstall**
- Follow the uninstall steps

Disable NetBIOS and SMB on Public Facing Interfaces (Cont'd)

To disable NetBIOS over TCP/IP

- In Control Panel, double-click **System**, click the **Hardware** tab, and then click the **Device Manager** button
- On the **View** menu, click **Show hidden devices**
- Expand **Non-Plug and Play Drivers**
- Right-click **NetBios over Tcpip**, and then click **Disable**
- This will disable the SMB on TCP/IP and UDP 445

Potential Impact

- Computers cannot connect to the server through SMB and connect to files and folder on the network

Disable Dr. Watson: Disable Automatic Execution of Dr. Watson System Debugger

The debuggers make it easy to trouble shoot the computers and applications

The Dr. Watson tool included with Windows Server 2003 and Windows XP is automated system debugger; to records information about system state and applications which are active

Vulnerability

- An attacker who has already gained administrative privileges has complete control of the computer, so attackers could still pursue other paths if you disable Dr. Watson

Disable Dr. Watson: Disable Automatic Execution of Dr. Watson System Debugger (Cont'd)

Potential Impact

- No debugger will run and no report is created
- The admin will not have much data to solve the system problems

EC-Council

Configure IPsec Policies

IPsec is a tool used by the network security administrators to permit , block, or negotiate security for TCP/IP traffic

IPsec is independent and transparent to applications

An adequate host level protection is gives by Windows firewall component

IPsec should be used to secure host-to-host and host-to-client

Configure IPsec Policies (Cont'd)

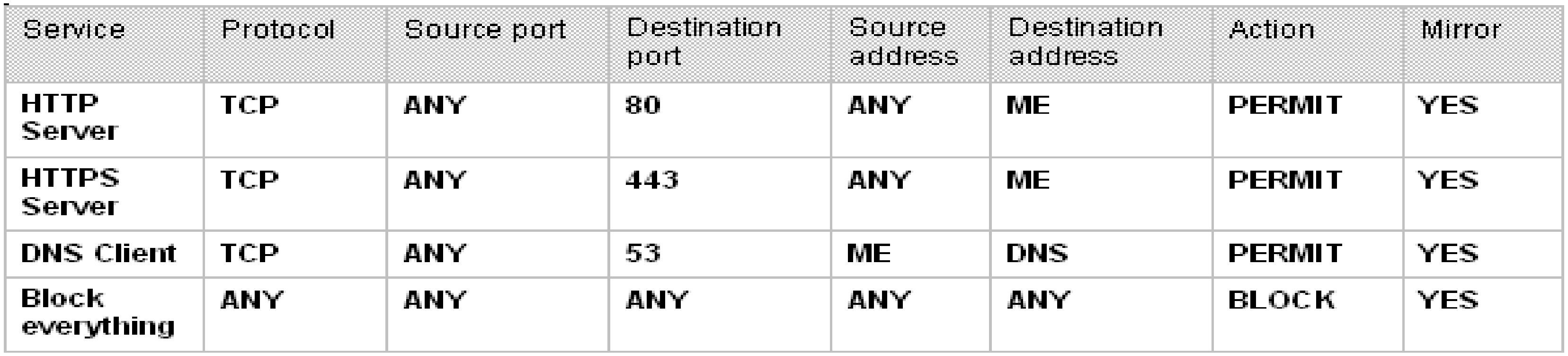
Vulnerability

- The security personnel's mostly concentrate on preventing attacks from outside in a company But the attacks can even occur from inside the company
- Attackers may use NetBT null session to get information
- Firewalls between internal network and internet can not give any security for internal threats
- Authenticated access controls are needed to protect client and server

Configure IPsec Policies (Cont’d)

Countermeasure

- To create a traffic map
- Determine the base network services that are required for the server role
- Identify the protocols and ports that are required by each service. Use tools such as the Netstat.exe command to view open ports and active connections
- Document the IPsec filtering rules that are necessary to allow only the identified traffic



Service	Protocol	Source port	Destination port	Source address	Destination address	Action	Mirror
HTTP Server	TCP	ANY	80	ANY	ME	PERMIT	YES
HTTPS Server	TCP	ANY	443	ANY	ME	PERMIT	YES
DNS Client	TCP	ANY	53	ME	DNS	PERMIT	YES
Block everything	ANY	ANY	ANY	ANY	ANY	BLOCK	YES

Configure IPsec Policies (Cont'd)

Network Traffic Map (Sample)

- IPsec policies that use Windows Server 2003 features such as this one should not be assigned to Windows 2000 or Windows XP computers
- A mirrored block filter will block unicast IP traffic from an IP address from a computer
- Any of the following solutions could be used to block the inbound attack:
  - Use additional IPsec filtering rules to block an attacker from using port 80 to gain inbound access to open ports
  - Use a front-end stateful filtering firewall or router to block inbound traffic from source port 80 unless it corresponds to an outbound connection

Configure IPsec Policies (Cont'd)

Network Traffic Map (Sample)

- In addition to this IPsec policy, configure Windows Firewall on the server's external network adapter to provide stateful filtering for all outbound traffic that is permitted by IPsec filters. Because Windows Firewall is layered above IPsec, Windows Firewall must also be configured to permit TCP ports 80 and 443 inbound.
- You can apply IPsec policies in several ways:
  - Apply them on an individual computer.
  - Attach them to an OU or domain using Group Policy.
  - Write a script for the netsh ipsec command, and then apply the script on select computers.

Configure IPsec Policies (Cont'd)

Potential Impact

- Using IPsec the server can be hardened against network attacks
- IPsec filtering is designed for a simple packet filtering scenario
- Limitations of IPsec filtering include the following:
  - Cannot be applied for a particular application, defined for protocols and ports
  - They are static and do not provide "stateful" outbound traffic filtering. It cannot guard against an attacker using the static inbound permit filter which allows access to any open port
  - Do not differentiate between different types of ICMP messages

Configure IPsec Policies (Cont'd)

Potential Impact

- Do not perform inspection of the contents of IP packets for the purpose of intrusion detection.
  - They can overlap, but cannot be manually ordered. This service internally calculates a weight that provides an automatic filter order.
  - These filters are not interface-specific.
  - These filters cannot be explicitly configured as inbound or outbound.
  - Policy does not support duplicate filters.
  - Windows Server 2003 slowly improves the performance of IPsec filtering.

Configuring Windows Firewall

In Windows XP and Windows Server 2003 a built in Windows firewall can be used to protect organization network fro network attacks with the external firewalls

- Click **Start**, and then click **Control Panel**
- Click **Windows Firewall**
- Click the **On (recommended)** radio button
- If necessary, click the **Exceptions** tab and configure exceptions for protocols that you want to allow through the firewall
- Click **OK** to activate Windows Firewall

Configuring Windows Firewall (Cont'd)

Windows Firewall is only contains a basic intrusion prevention feature

Windows Firewall does not do extensive outbound filtering

Windows Firewall can centrally be managed by the Group Policies