Global Information Assurance Certification Paper

Windows 2000 Server
Resource Kit Security Tools

Kenneth R. Zepernick
GSEC Version 1.2f

Summary

This paper identifies and briefly describes tools and utilities on the Windows 2000 Server Resource Kit CD-ROM that may be useful to security administrators. Each Resource Kit security tool is identified, it's purpose given, and described in a security context.

Overview

I started this project with two purposes in mind. First, I had always wondered what neat security tools were on the Windows 2000 Server Resource Kit CD. There was no single write-up in any of the documentation that told me what might be useful in everyday security tasks. And after checking Microsoft TechNet, the SANS Reading Room, and searching the Web, I could turn up no more than a few write-ups on a handful of tools, or simple lists of all the tools at best. The only way to find out what items might be of interest security administrators was to go through them all, one by one. No administrator really can afford to spend that much time weeding-out the handy utilities. So, I thought it would be a good idea to put together a synopsis of potentially useful security tools.

Second, I figured this project would be a cinch for getting a five-page practical exercise completed. Maybe a couple of days tops, and then I'd be done. Boy, was I wrong! I've been assembling this list of tools for weeks now, and I still don't feel as if it's truly finished. Let me just say this -- it's hard to find something on the Resource Kit CD that *doesn't* have some potential usefulness for security administration.

I've looked into about 300 tools and utilities from the Resource Kit CD, checking to see what kind of practical application each might have to security. I've listed the ones I found that a security administrator might find useful for configuring and maintaining system security.

Notes

(1) The descriptions below are taken from the Microsoft Windows 2000 Server Resource Kit's Tools Help files. I have amplified the descriptions where I could, deleted extraneous caveats for the sake of brevity, and suggested uses for the tools wherever possible. Be sure to consult the Tools Help files for complete descriptions of the tools, installation instructions, syntax and usage, and examples of applications.

(2) Vendor-supplied security products included on the Resource Kit CD are not addressed because the products have become outdated. Always download the latest product evaluation kits directly from the security product vendor site.
(3) There are also many other security tools and utilities on the Windows 2000 Server CD-ROM. They are not covered in this paper. See the Support Tools directory on the Windows 2000 Server CD-ROM.

Contents

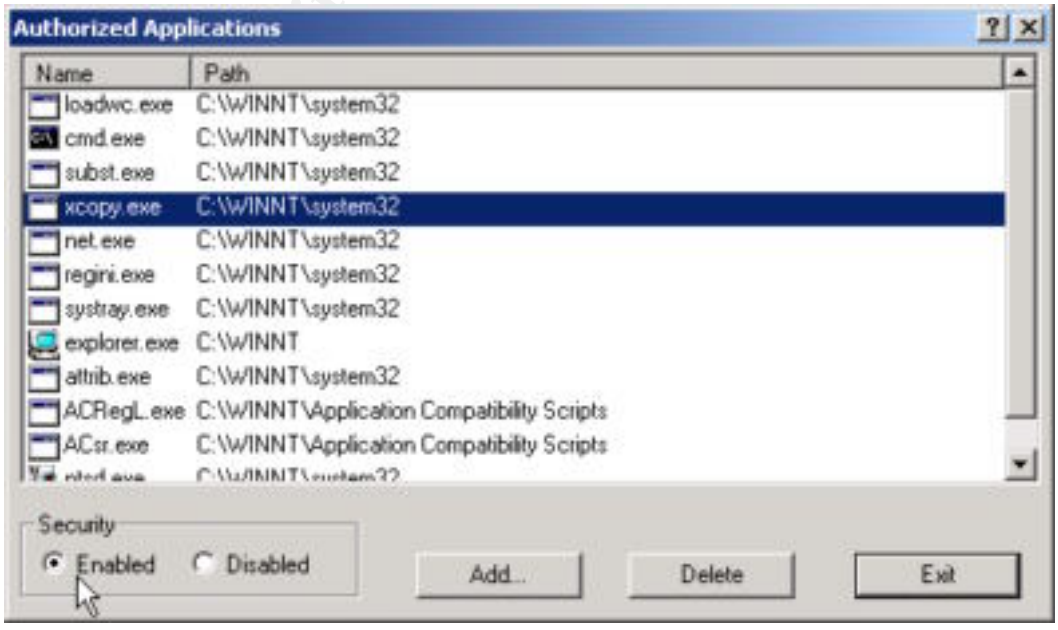
Security Tool Name	Purpose
Application Security	Disable non-administrator users' ability to execute specified application programs.
Audit Policy	View or modify the audit policy of a local or remote computer.
Concurrent Connection Limiter	(1) Tracks/limits the number of concurrent connections by user. (2) Monitors what computers a user is logged on to.
CyberSafe Log Analyst	Analyze collections of security event logs against predefined event signatures (e.g., failed logons, virus activity), and produce easy to interpret graphs and statistics of enterprise-wide security activity.
Console User Manager	Remotely change user account properties.
Directory Services Store	General-purpose utility to manage Windows 2000/Active Directory PKI.
Dump Event Log	Dumps an event log for a local or remote system into a tab-separated text file.
Encrypting File System (EFS) Information	Displays information about files and folders encrypted with EFS.
Event Log Dump	Dumps information from a selected event log.
Enumerate Properties	Display all properties set on any directory service object.
Floppy Lock	Restricts access to the floppy drive.
Group Policy Results	Displays information about the result Group Policy has had on the computer and logged-on user.
Internet Explorer Administration Kit (IEAK)	Customize Internet Explorer (security) settings before you deploy it to your organization.
Internet Protocol Security Policies Tool	Configure IPSec policies in the Directory Service or in a local or remote registry.
Kerberos Tray	Kerberos Tray is a tool that displays ticket information for a computer running the Kerberos protocol.
Kerberos List	Enables you to view and delete Kerberos tickets granted to the current logon session.
Move User	Changes the security of a profile from one user to another.
Service Controller	Remotely start, stop, pause, continue, and query the status of services from the command line.
NTRights	Grants or revokes rights to or from users or groups.
PermCopy	Copies file- and share-level permissions from one share to another.
File Access Permissions per User	Displays a user's access permissions for a file or directory.
Registry Backup	Allows you to backup the registry to a file instead of tape.
Registry Find	Searches and optionally replaces registry data.
Registry Restoration	Restores all or part of the registry from a backup file.
Services List	Shows services and their status on local and remote computers.
Security Configuration Manager Templates for IIS	Defines IIS security policies through IIS Security Templates.

Security Tool Name	Purpose
Show Access Control Lists	Displays access rights for files, folders, and trees.
Show Groups	Shows the groups to which a user belongs.
Show Members	Shows the user names of members of a group.
Show Privileges	Displays the users and groups granted a particular privilege on the local computer.
Remote Shutdown	Shuts down or reboots a local or remote computer.
Server Share Check	Lists shares on a computer and enumerates the ACLs for each one.
Server Information	Displays network, disk drive, and service information about a server.
SubInACL	Migrates security information between users, groups, and domains.
Service ACL Editor	Sets access control lists on services.
Service Monitoring Tool	Monitors services on a computer, and notifies the administrator when changes occur.
User Manager for Domains	Manage Windows NT domains from Windows 2000 workstations.
User Statistics	Displays the user name, full name, and last logon date and time for each user in a given domain.

Name: **Application Security**
Program: **AppSec.exe**
Interface: **GUI**

Purpose: Disable non-administrator users' ability to execute specified application programs.

Description: The Application Security tool allows administrators to enable or disable ordinary users' ability to execute application programs on a local host. Control is applied on a program-by-program basis through a simple GUI. If a non-administrator attempts to execute a protected program, the request will be rejected.



Enabling security on the xCopy program.

Security is applied to the computer, rather than to individual users. Thus, no user account maintenance is necessary. The Application Security tool recognizes only administrators and non-administrators. Consequently, any administrator can execute any programs regardless of its security settings.

Group Policy permits the administrator to restrict access to programs by hiding menu items and desktop icons. The Application Security tool extends security by rejecting user attempts to execute programs via the command line or from within other applications. Group Policy hides programs from users, whereas Application Security explicitly prevents execution.

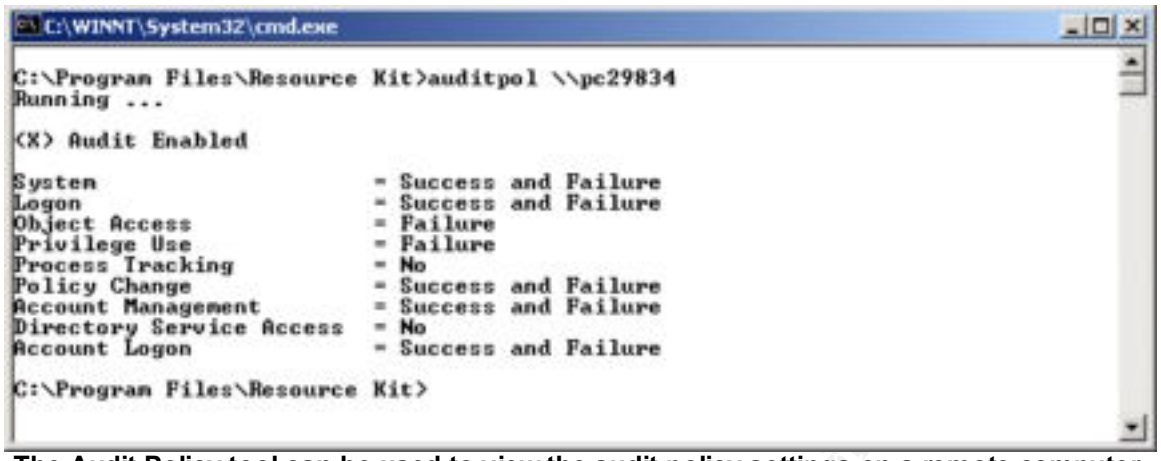
Typical Uses: The Application Security tool is used frequently on Terminal Server. This permits the administrator to place important programs on the server and prevent them from being run by Internet users.

Note: Some early versions of the Windows 2000 Resource Kit CD did not contain the Application Security tool. The latest version of the tool is available from Microsoft. http://www.microsoft.com/windows2000/techinfo/reskit/tools/hotfixes/appsec-o.asp

Name:	**Audit Policy**
Program:	**AuditPol.exe**
Interface:	**Command line.**

Purpose: View or modify the audit policy of a local or remote computer.

Description: The Audit Policy tool is a command line tool the administrator can use to view or set the audit policy on any local or remote computer. The administrator can use it to enable and disable auditing, to specify auditing categories (e.g., system events, logon/logoff events, object access), and to specify the type of event (success, failure, all, or none). The user must have administrator privileges on the target machine for the Audit Policy tool to work.



The Audit Policy tool can be used to view the audit policy settings on a remote computer.

Name:	**Concurrent Connection Limiter**
Program:	**CConnect.exe**
Interface:	**Command line.**

Purpose: (1) Tracks/limits the number of concurrent connections by user. (2) Monitors what computers a user is logged on to.

Description: The Concurrent Connection Limiter allows Windows 2000 and Windows NT network administrators to limit the number of computers a user can be logged on to at the same time. It consists of two parts, a client-side application and an administrative function.
Concurrent Connection Limiter provides the following features:

- It is completely hidden from the end user's view.
- Keeps track of all computers that users are logged onto.
- Tracks last known user of the computer.
- Monitors what logon server users are logging into.
- Allows concurrent connection limitations to be set on a per-user or per-group basis.
- Stores all information in a Microsoft SQL Server database assigned by the Administrator.

Typical Uses: Useful in any situation where account sharing is prohibited by policy, where users are not allowed to be logged on to more than one computer at a time, or where you suspect that an account has been compromised.

References:

See Randy Smith's article in *Windows 2000 Magazine* at
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=15969&pg=1

Name:	**CyberSafe Log Analyst**
Program:	**CLA.msc**
Interface:	**MMC Snap-in**

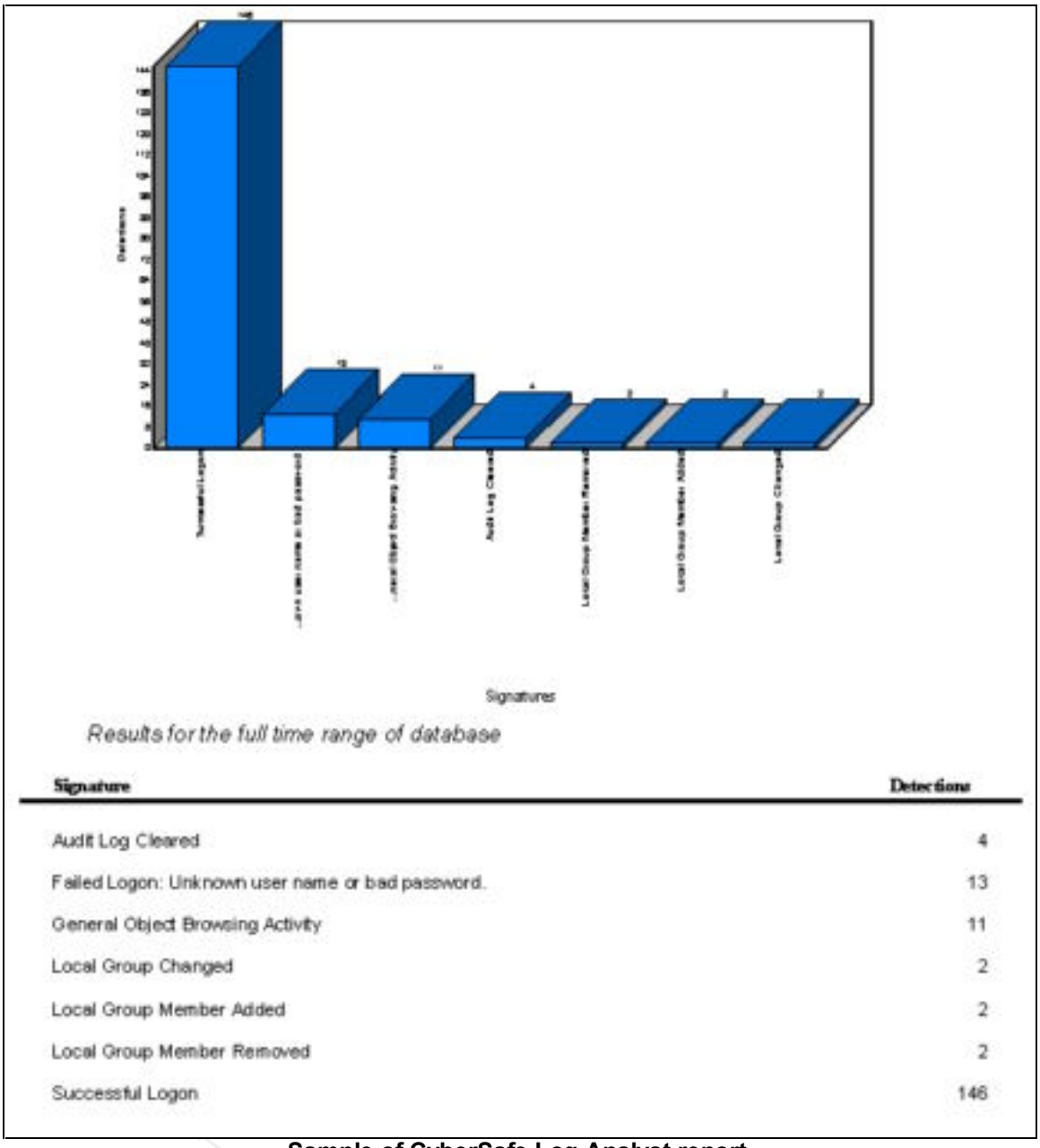
Purpose: Analyze collections of security event logs against predefined event signatures (e.g., failed logons, virus activity), and produce easy to interpret graphs and statistics of enterprise-wide security activity.

Description: CyberSafe Log Analyst processes a user-selected set of security event logs, analyzes them against a predefined set of security event signatures, and displays useful views of your systems' security activity. Security event logs from across the enterprise can be selected for analysis. CLA combines all selected logs into a "super log" prior to analysis, providing you with a single source of security event data. CLA then analyzes the combined security event logs, looking for predefined events or series of events that could indicate security problems. CLA looks for security events that could indicate:

- Trojan horse and virus activity
- Object browsing activity
- Back Orifice 2000 activity
- Failed single logons
- Successful logons and logoffs
- User account and user rights changes
- Password change activity
- Global and local group changes
- Security-relevant system changes

CLA uses predefined security event signatures. While you cannot create new signatures, CLA allows you to edit the built-ins for enhanced filtering. For example, you can modify the Failed Single Logon activity signature to look only for failed logons from a specific user.

CLA provides a set of report templates that allow you to examine the results of the analysis. Results are displayed both graphically and statistically. You can also create your own report templates.



Signature	Detections
Audit Log Cleared	4
Failed Logon: Unknown user name or bad password.	13
General Object Browsing Activity	11
Local Group Changed	2
Local Group Member Added	2
Local Group Member Removed	2
Successful Logon	146

Sample of CyberSafe Log Analyst report.

Typical Uses: Use CLA to get an enterprise view of the security event data scattered across the domain. It provides a perspective on security activity that cannot be gotten from viewing security event logs one system at a time.

References:

See Thomas Shinder's Cool Tools notebook for a review of this product at
http://www.swynk.com/friends/shinder/cybersafe.asp
Also see Smith's article at
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=15969&pg=1

Name:	**Console User Manager**
Program:	**CUsrMgr.exe**
Interface:	**Command line.**

Purpose: Remotely change user account properties from the command line.

Description: You can use Console User Manager to remotely rename or delete users, set passwords, and set or reset other user properties in a Windows NT or Windows 2000 domain. You can also use this tool in a batch file to make user account changes across multiple servers and workstations. You must have administrator privileges on the target computer.

Typical Uses: Adding a master domain administrator account to the local administrators group on workstations, resetting passwords, deleting terminated employee accounts, etc.

Name:	**Directory Services Store**
Program:	**DSStore.exe**
Interface:	**Command line.**

Purpose: General-purpose utility to manage Windows 2000/Active Directory PKI.

Description: The Directory Services Store tool assists in managing Enterprise Public Key Integration. It performs many of the functions available in the MMC Active Directory Users and Computers snap-in and in the Certificate Services snap-in, and includes some additional operations as well. DSStore lets you add, view, and delete enterprise root Certificate Authorities, maintain certificate revocation lists, manage auto-enrollment, check certificate status, and verify the validity of smart cards.

Typical Uses:

- List information about a given computer's certificates.
- List information about a mputer's objects on the domain.
- List information about Certificate Authorities in the Enterprise.
- Add, remove, and display certificates from the directory services Enterprise Root Store.
- Add and remove certificate revocation lists (CRLs) from directory services.
- Validate certificates from directory services public key infrastructure (PKI) locations.
- Pulse "autoenrollment" events to speed up various PKI processes
- Add non-Microsoft Windows 2000 Certificate Authorities or offline Certificate Authorities to the enterprise PKI.
- Manage enterprise roots in directory services.

- Verify Machine Autoenrollment and Domain Controller certificates from Kerberos Key Distribution Center (KDC).
- Check on status and validity of domain controller certificates.
- Check on validity of smart card certificates.

References:

See Don Kiely's article at http://www.itworld.com/nl/nt2k_sec/12042000/pf_index.html
See Randy Smith's article at
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=15969&pg=1

Name:	**Dump Event Log**
Program:	**DumpEL.exe**
Interface:	**Command line.**

Purpose: Dumps an event log for a local or remote computer into a tab-separated text file.

Description: The Dump Event Log tool allows you to retrieve event log data from computers you specify. You must have appropriate privileges on the target computer. You can specify which event log to dump, and the number of days of logging you want to dump. You can also filter the log dump by event source, event ID, and whether to filter in or filter out records.

See Also: Event Log Dump.

References: See the "Exploring Windows NT for Professionals" article, *Extracting event logs with DUMPEL.EXE* for a practical guide to parsing the dump files.
http://www.elementkjournals.com/ewn/9609/ewn9692.htm

Name:	**Encrypting File System (EFS) Information**
Program:	**EFSInfo.exe**
Interface:	**Command line.**

Purpose: Displays information about files and folders encrypted with EFS.

Description: The EFS Information tool lets you view information about EFS files and folders, including information about the EFS account user and the recovery agent accounts. You can use EFS Info to display the user name and e-mail addresses of a file's encryptor and the file's recovery agents. The information displayed is from the EFS certificates associated with each role.

Typical Uses: You can use EFS Info to verify who the file encryptor is, and which recovery accounts are authorized for recovering the file. This is particularly important in instances where files have not been opened for a long time, and thus do not have current user and recovery agent information.

References:

See Don Kiely's article at http://www.itworld.com/nl/nt2k_sec/12042000/pf_index.html
See Randy Smith's article at
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=15969&pg=1

Name:	**Event Log Dump**
Program:	**ELogDmp.exe**
Interface:	**Command line.**

Purpose: Dumps information from a selected event log.

Description: The Event Log Dump tool is a command line tool that dumps information from the System Event log, Security Event log, or Application Event log. You can display any selected log locally or remotely. Any user can use this tool to view the contents of the application log on any remote computer, but only administrators can view the security log and system log on remote computers.

Typical Uses: You can use the Event Log Dump tool in conjunction with the Find String tool (FindStr.exe in %systemroot%\System32) to query for specific event log messages to display.

See Also: Dump Event Log.

Name:	**Enumerate Properties**
Program:	**EnumProp.exe**
Interface:	**Command line.**

Purpose: Display all properties set on any directory service object.

Description: The Enumerate Properties tool dumps all properties on any directory service object.

Typical Uses: You can use Enumerate Properties to display the security descriptors of LDAP objects.

Name:	**Floppy Lock**
Program:	**FlopLock.exe**

Interface: System service.

Purpose: Restricts access to the floppy drive.

Description: Floppy Lock is a service that allows you to control access to the floppy drives of a computer. When the service is started on Windows 2000 Professional, only members of the Administrators and Power Users groups can access the floppy drives. When the service is started on Windows 2000 Server, only members of the Administrators group can access floppy drives.

Floppy Lock works by assigning a Discretionary Access Control List to a floppy drive. When Floppy Lock has the floppy drives on a machine locked, only users in the Adminstrators group can use the floppy drive(s). If the Floppy Lock service is configured to start automatically, the lock stays in place even after the computer is restarted.

Typical Uses: The Floppy Lock service can be used to help prevent unauthorized software installation or the introduction of viruses via floppy disks.

Name: Group Policy Results
Program: GPResult.exe
Interface: Command line.

Purpose: Displays information about the result Group Policy has had on the computer and logged-on user.

Description: GPResult lets you see how Group Policy has been applied to a particular computer or logged-on user. It is sometimes difficult to tell how Group Policy is applied in environments where several Group Policy objects are active (e.g., system, site, domain). With GPResult, you can determine when the latest Group Policy was applied, and which domain controller or directory service supplied the Group Policy object. GPResult provides the following general information:

- Operating System
- Type (Professional, Server, Domain Controller)
- Build number and Service Pack details
- Whether Terminal Services is installed and, if so, the mode it is using
- User Information
- User name and location in Active Directory (if applicable)
- Domain name and type (Windows 2000 or Windows NT)
- Site name
- Whether the user has a local or roaming profile and location of the profile
- Security group membership
- Security privileges
- Computer Information
- Computer name and location in Active Directory (if applicable)

- Domain name and type (Windows 2000 or Windows NT)
- Site name

GPResult also provides the following information about Group Policy:

- The last time policy was applied and the domain controller that applied policy, for the user and computer
- The complete list of applied Group Policy objects and their details, including a summary of the extensions that each Group Policy object contains
- Registry settings that were applied and their details
- Folders that are re-directed and their details
- Software management information detailing assigned and published applications
- Disk quota information
- IP Security settings
- Scripts

Note: Microsoft has supplied an updated GPResult.exe at:
http://www.microsoft.com/WINDOWS2000/techinfo/reskit/tools/existing/gpotool-o.asp

References:

See Randy Smith's Windows 2000 Magazine article at
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=15969&pg=1

Name:	**Internet Explorer Administration Kit (IEAK)**
Program:	**Installer provided in IEAK directory on the Resource Kit CD.**
Interface:	**GUI.**

Purpose: Customize Internet Explorer (security) settings before you deploy it to your organization.

Description: Allows administrators to create, distribute, and update customized installations of Internet Explorer using tools included in the IEAK. You can configure settings before you install, so you don't need to set options on each computer. And you can control which settings your employees can change, so you ensure that security, connection, and other important settings adhere to corporate standards. With IEAK, you can configure and control:

- Security: You can use certification authorities and Authenticode to help manage security.
- Security and Privacy Settings: You can manage security zones, privacy settings, and content ratings for your company. You can customize the settings for each security zone. You can set the level of privacy regarding cookies for all of your browser users. Through content ratings, you can prevent users from viewing

content that may be considered offensive or otherwise inappropriate within your corporate setting.

- Set Policies and Restrictions: You can specify settings across your organization for various aspects of your user's machines, including their desktop, Internet components, operating system, and security.
- Outlook Express Accounts: You can specify the mail and news servers for Outlook Express and require users to log on using Secure Password Authentication (SPA) to access a server.

Much of the information regarding security options in the IEAK is available by clicking Help in the Internet Explorer 6 Customization Wizard.

References:

See Randy Smith's article at
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=15969&pg=1

Name:	**Internet Protocol Security Policies Tool**
Program:	**IPSecPol.exe**
Interface:	**Command line.**

Purpose: Configure IPSec policies in the Directory Service or in a local or remote registry.

Description: This command-line tool configures Internet Protocol Security (IPSec) policies in the directory service, or in a local or remote registry. It does everything that the IPSec Microsoft Management Console (MMC) snap-in does, and is even modeled after the snap-in.

IPSecPol has two mutually exclusive modes: static and dynamic (see Tools Help in the Resource Kit for distinction). The default mode is dynamic. You must have specific privileges for both dynamic and static mode. For static mode, you must have read/write access to the storage that you write. For dynamic mode, you must have Administrator privileges on the computer to which you are plumbing the dynamic policy.

Typical Uses: If you have a large and/or complex IPSec policy that you want to configure, IPSecPol can help you by providing a scriptable way to create that policy. Just put your IPSecPol commands into a batch file. (This also provides a backup in case you lose the directory service or registry that the policy is stored in. Just re-run the batch file.) IPSecPol facilitates just-in-time policy with its batch ability. If someone wants a secured channel with your server, simply send them the tool binaries and the command line or batch file to run.

If your computer is using directory service policy and you want to add rules that will allow you to speak IPSec to computers not covered in the directory service policy, use IPSecPol dynamic mode.

Name:	**Kerberos Tray**
Program:	**KerbTray.exe**
Interface:	**GUI.**

Purpose: Kerberos Tray is a tool that displays ticket information for a computer running the Kerberos protocol.

Description: KerbTray runs in the system tray when launched. The KerbTray icon can be used to view and purge the ticket cache. Positioning your mouse cursor over the KerbTray icon will display the time left on your initial ticket-granting ticket (TGT) before it expires. The icon will also change in the last hour of life before the Local Security Authority (LSA) renews the ticket.

Typical Uses: Double-clicking the KerbTray icon will bring up a list of tickets you have obtained since logon. Right clicking the icon gives you options:

- List Tickets lists all tickets you have obtained since logon.
- Purge Tickets will destroy all tickets that you have cached. Use this option with caution. It may stop you from being able to authenticate to resources. If this happens, logoff then logon again. New tickets are acquired the next time Kerberos services are used.

Name:	**Kerberos List**
Program:	**Klist.exe**
Interface:	**Command line.**

Purpose: Enables you to view and delete Kerberos tickets granted to the current logon session.

Description: Running Kerberos List from a client lets you:

- Display Tickets: Lists the currently-cached tickets of services that you have authenticated to since logon.
- Display Ticket Granting Ticket: Lists the initial Kerberos ticket-granting-ticket (TGT).
- Purge Cached Tickets: Allows you to delete a specific ticket. Purge tickets will destroy all tickets that you have cached, so use this with caution. It might stop you from being able to authenticate to resources. If this happens you will have to logoff and logon again.

Note: To use this tool, and see any tickets, your Windows 2000 computer must be joined to a Windows 2000 domain.

Name:	**Move User**
Program:	**MoveUser.exe**
Interface:	**Command line.**

Purpose: Changes the security of a profile from one user to another.

Description: MoveUser enables you to change the account domain and/or the user name of a profile. You can use the MoveUser tool to move users between Windows 2000 network, or to reassign a specific profile to another user.

Name:	**Service Controller**
Program:	**NetSvc.exe**
Interface:	**Command line.**

Purpose: Remotely start, stop, pause, continue, and query the status of services from the command line.

Description: Service Controller is a command line utility that allows you to administer and query services on a Windows 2000 or NT workstation or server.

In order to use this utility, you must first have adequate permissions on the target computer. In most cases, Local Administrator equivalencies are required.

Available command options:

/query	Queries the status of the service
/start	Starts the service
/stop	Stops the service
/pause	Pauses the service
/continue	Starts the paused service
/list	Lists installed services and drivers

Typical Uses: Use the /list command to check for unauthorized services running on a workstation or server.

See Also: ScList.exe

Name:	**NTRights**
Program:	**NTRights.exe**
Interface:	**Command line.**

Purpose: Grants or revokes rights to or from users or groups.

Description: You can grant or revoke any Windows 2000 right for a user or group of users on a local or remote computer. For example, you can use the NTRights utility to selectively revoke the logon locally right on the local computer so that only members of the local Administrators group can log on locally.

Typical Uses: NTRights is useful in unattended or automated installations of Windows 2000 during which you may want to change the Windows 2000 default rights. You can also use it in situations where you need to change a right in an existing installation, but you can't access and logon to all computers.

Note: The Windows 2000 Resource Kit documentation and the tool's help feature do not list all the rights that can be changed with NTRights. Logon rights that can be changed but are not documented are:

User Right	Friendly Name
SeNetworkLogonRight	Access this computer from the network
SeInteractiveLogonRight	Log on locally
SeBatchLogonRight	Log on as a batch job
SeServiceLogonRight	Log on as a service
SeDenyNetworkLogonRight	Deny access to this computer from the network
SeDenyInteractiveLogonRight	Deny log on locally
SeDenyBatchLogonRight	Deny log on as a batch job
SeDenyServiceLogonRight	Deny log on as a service

Name: **PermCopy**
Program: **PermCopy.exe**
Interface: **Command line.**

Purpose: Copies file- and share-level permissions from one share to another.

Description: PermCopy copies share (Full Control, Read, Change) and file (Full Control, Modify, Read & Execute, Read, Write, Traverse Directory) level permissions from one share to another.

Typical Uses: When you use PermCopy in conjunction with the Windows Xcopy utility, you can copy NTFS files or directory structures between partitions, hard drives, or computers, while maintaining NTFS permissions and share-level permissions. Xcopy is a command-line utility used to copy files and folders from NTFS partitions with their security intact. However, it does not copy share-level permissions. After using Xcopy to copy your files and directory structures, you can setup your shares and restore permissions using PermCopy.

Name:	**File Access Permissions per User**
Program:	**Perms.exe**
Interface:	**Command line.**

Purpose: Displays a user's access permissions for a file or directory.

Description: Perms displays a user's access permissions for a specified file or set of files. Perms queries the permissions associated with a specific access control entry (ACE), displaying only those permissions granted by that particular ACE.

Typical Uses: There are no graphical or command line utilities that produce comprehensive reports on groups, users and permissions included with the Windows Operating System or the Resource Kit. The NET commands and the Windows Resource Kit AddUsers and Perms utilities can be used to create limited administrative reports by piping the output to a text file.

Note: If a user is a member of local or global groups with varying sets of permissions, Perms output does not reflect cases in which this user has been given or denied rights through the ACEs for these local or global groups.

Name:	**Registry Backup**
Program:	**RegBack.exe**
Interface:	**Command line.**

Purpose: Allows you to backup the registry to a file instead of tape.

Description: Registry Backup is a tool for backing up the registry to files without use of a tape drive. RegBack allows you to back up registry hives while the system is running and has the hive files open. It will back up your registry so that, in case of problems with configuration, you can restore it and try again.

Typical Uses: Could be useful as a forensics tool on a computer you believe has had it's registry altered. You can use a file comparison program such as WinDiff to compare a known good backup with a current backup.

See Also: Registry Restore.

Name:	**Registry Find**
Program:	**RegFind.exe**
Interface:	**Command line.**

Purpose: Searches and optionally replaces registry data.

Description: RegFind is a command-line tool that you can use to search the registry of a local or remote computer for arbitrary data, key names, or value names. The tool allows you to replace any of these with new values.

Typical Uses: You can use RegFind to see if your registry has been altered in some specific way, as by a worm, virus, or Trojan that has a distinct registry signature.

Name:	**Registry Restoration**
Program:	**RegRest.exe**
Interface:	**Command line.**

Purpose: Restores all or part of the registry from a backup file.

Description: RegRest restores registry hive files from backups created by RegBack. You can backup and restore the registry manually, or in batch files, using the RegBack and RegRest tools. RegRest performs a ReplaceKey operation, which swaps backup files for the default files that the Emergency Repair Disk or Windows 2000 Setup programs installed, and saves the default files under other file names.

Name:	**Services List**
Program:	**ScList.exe**
Interface:	**Command line.**

Purpose: Shows services and their status on local and remote computers.

Description: ScList can show currently running services, stopped services, or all services on a local or remote computer. It cannot be used to start or stop services like NetSvc.

ScList displays a list of all services on a computer and shows the status of each.

Typical Uses: ScList is particularly useful in determining what services are running on a physically remote or blind (no monitor) system. To enable ScList to report on the status of services on a computer, however, the Server service must be running on it.

See Also: NetSvc.exe

Name:	**Security Configuration Manager Templates for IIS**
Program:	**SecTemplates.msc**
Interface:	**MMC Snap-in.**

Purpose: Defines IIS security policies through IIS Security Templates.

Description: Setting security policy on a Web server by hand is both tedious and error-prone. Security policies can be easily standardized and implemented by means of security templates. A security template is a physical file representation of a security configuration. The Windows 2000 Resource Kit includes two IIS-specific security templates:

- Secure Internet Web Server template
- Secure Intranet Web Server template

These templates are designed for use with the Security Configuration and Analysis snap-in, a Windows 2000 tool that provides a single point of administration for Windows 2000 system security. You can also make your own security templates, or modify the ones provided on the Resource Kit CD.

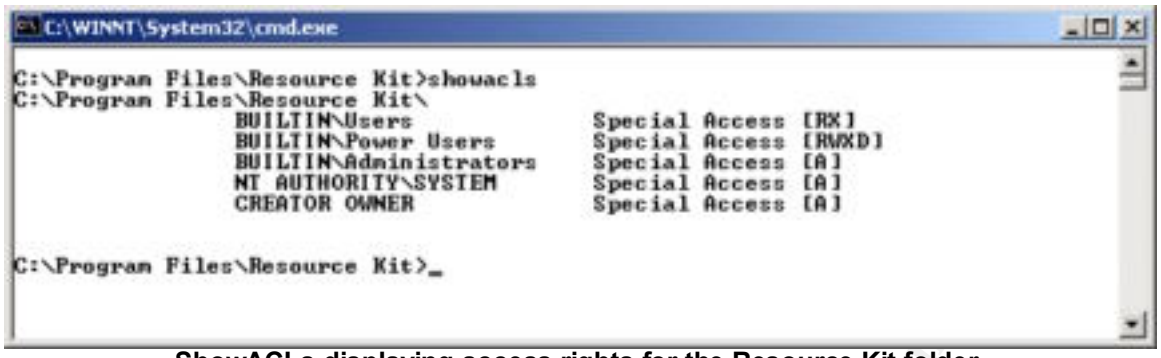
References:

See Randy Smith's article at
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=15969&pg=1

Name:	**Show Access Control Lists**
Program:	**ShowACLs.exe**
Interface:	**Command line.**

Purpose: Displays access rights for files, folders, and trees.

Description: ShowACLs enumerates access rights for files, folders, and trees. It allows masking to enumerate only specific ACLs.



ShowACLs displaying access rights for the Resource Kit folder.

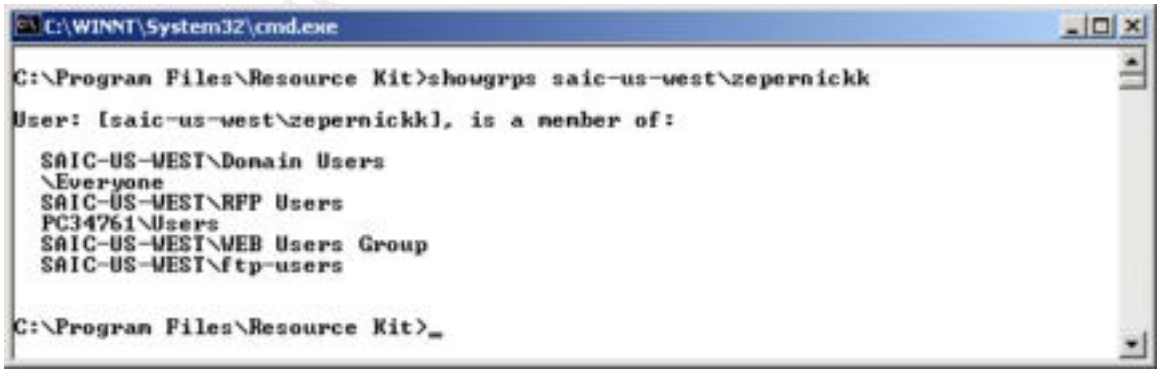
The most useful feature of ShowACLs is the ability to show permissions for a particular user. The method that ShowACLs uses to perform this is by enumerating the local and global groups that the particular user belongs to and matching the users security identifier (SID) and the SIDs of the groups the users belongs to, to the SIDs in each ACE entry.

Note: One of the problems with a command-line tool like ShowACLs is the amount of information that is contained in the ACL. The first version of ShowACLs attempted to display all the data in the access mask, which was very confusing. The latest version has adopted the "standard" permissions, Full, Change and Read-Only where appropriate. If a mask does not match these predefined values, then a raw dump of the mask is performed.

Name:	**Show Groups**
Program:	**ShowGrps.exe**
Interface:	**Command line.**

Purpose: Shows the groups to which a user belongs.

Description: ShowGrps shows the groups to which a user belongs, even within a given network domain.



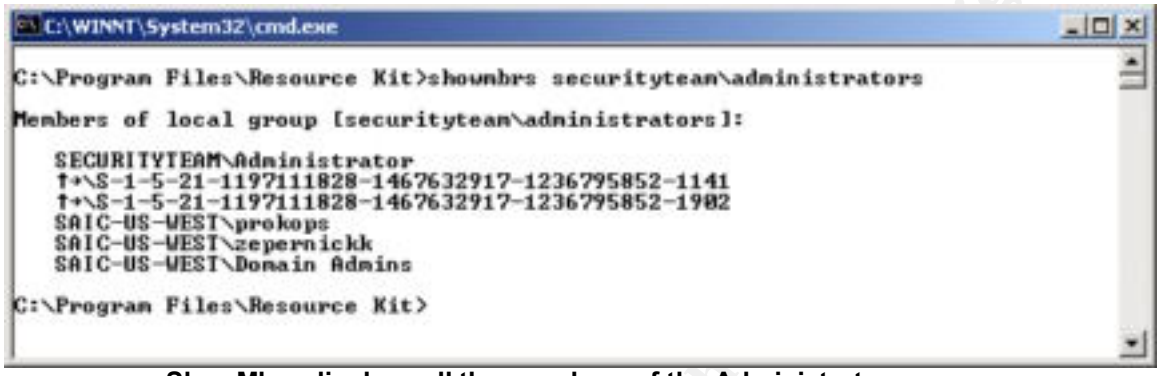
ShowGrps displays all the groups I'm a member of.

Name:	**Show Members**
Program:	**ShowMbrs.exe**

Interface:	Command line.

Purpose: Shows the user names of members of a group.

Description: ShowMbrs shows the user names of members of a given group, even within a given network domain.



ShowMbrs displays all the members of the Administrators group.

Name:	Show Privileges
Program:	ShowPriv.exe
Interface:	Command line.

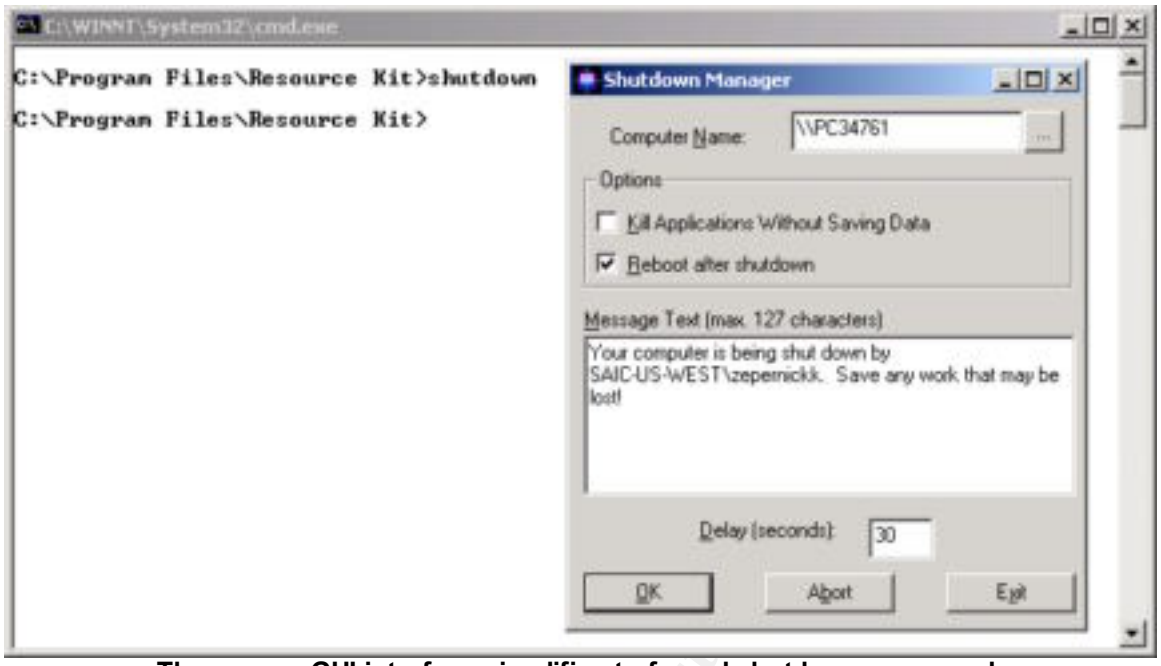
Purpose: Displays the users and groups granted a particular privilege on the local computer.

Description: ShowPriv is a command-line tool that displays the users and groups granted a particular privilege. This tool must be run locally on the target computer or on a domain controller to display users and groups with domain privileges.

Name:	Remote Shutdown
Program:	Shutdown.exe
Interface:	Command line.

Purpose: Shuts down or reboots a local or remote computer.

Description: Remote Shutdown is a tool that allows you to remotely shut down or reboot a computer running Windows 2000 or Windows NT 4. ShutDown provides system shutdown and restart options from both the command-line and, optionally, a pop-up GUI.



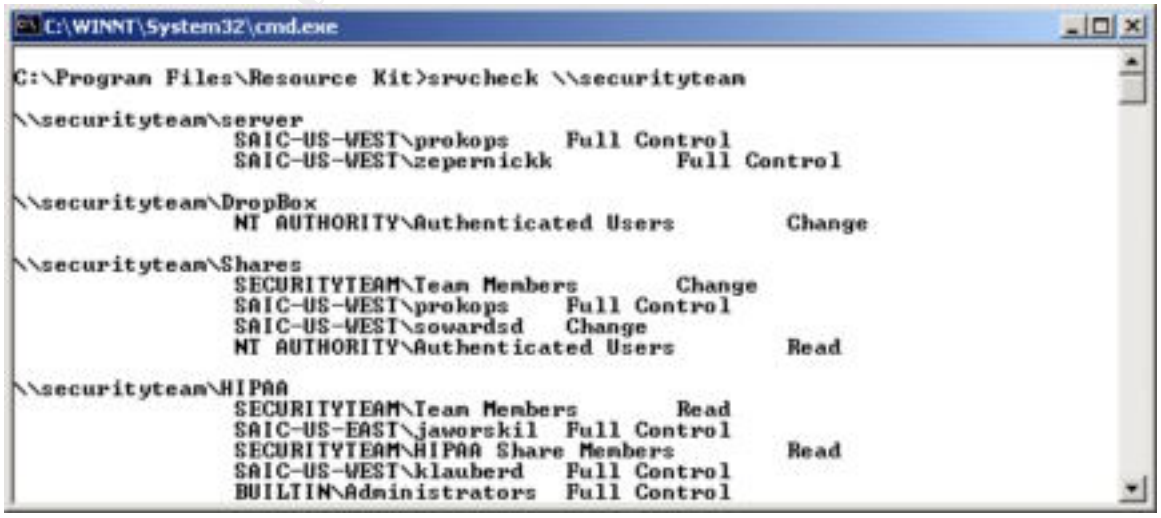
The pop-up GUI interface simplifies to forced shutdown command.

Typical Uses: Subtle reminder to the kids that it's past their bedtime! Great practical joke to play on your boss, too!

Name:	**Server Share Check**
Program:	**SrvCheck.exe**
Interface:	**Command line.**

Purpose: Lists shares on a computer and enumerates the ACLs for each one.

Description: SrvCheck lists the shares on a local or remote computer running Windows 2000 and enumerates the users on the access control lists for each share.

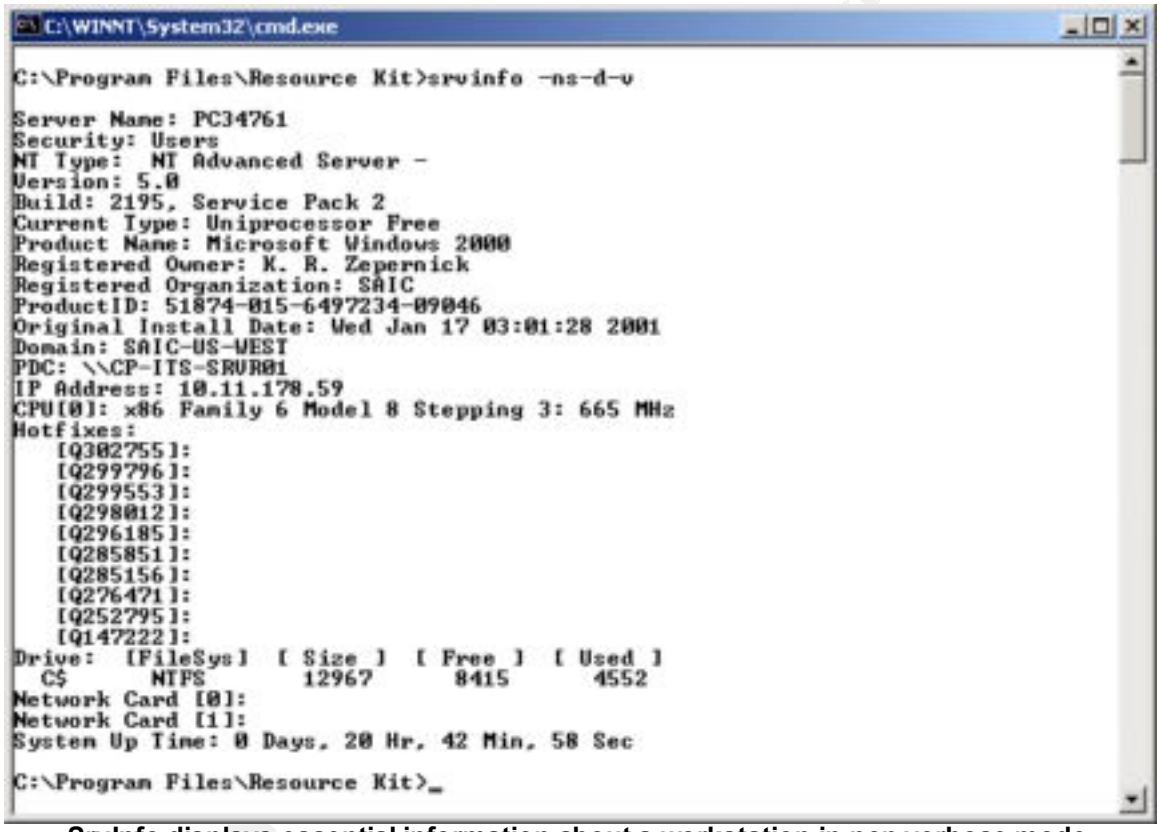


SrvCheck shows all the shares and ACLs on each shared folder on the server.

Name:	**Server Information**
Program:	**SrvInfo.exe**
Interface:	**Command line.**

Purpose: Displays network, disk drive, and service information about a server.

Description: SrvInfo displays information about a local or remote server, including available disk space, partition types, and status of services.



SrvInfo displays essential information about a workstation in non-verbose mode.

Name:	**SubInACL**
Program:	**SubInACL.exe**
Interface:	**Command line.**

Purpose: Migrates security information between users, groups, and domains.

Description: With SubInACL, administrators can obtain security information on files, registry keys, and services, and transfer this information from user to user, from local or global group to group, and from domain to domain. SubInAcl enables administrators to:

- Display security information associated with files, registry keys, or services, including owner, group, permissions access control list (ACL), discretionary access control list (DACL), and system access control list (SACL).
- Change the owner of an object.
- Replace the security information for one identifier (account, group, well-known security identifier (SID)) with that of another identifier.
- Migrate security information on objects. This is useful if you have reorganized a network's domains and need to migrate the security information on files from one domain to another.

Name:	**Service ACL Editor**
Program:	**SvcACLs.exe**
Interface:	**Command line.**

Purpose: Sets access control lists on services.

Description: SvcACLs sets access control lists (ACLs) on service objects, enabling administrators to delegate control of services.

Name:	**Service Monitoring Tool**
Program:	**SvcMon.exe**
Interface:	**Service.**

Purpose: Monitors services on a computer, and notifies the administrator when changes occur.

Description: SvcMon monitors services on local and remote computers for changes in state (starting or stopping). To detect these changes, Service Monitoring Tool implements a polling scheme. When a monitored service stops or starts, Service Monitoring Tool notifies you by sending e-mail. In addition, SvcMon is capable of program tracing or logging. You can enable logging by modifying the registry.

Name:	**User Manager for Domains**
Program:	**UsrMgr.exe**
Interface:	**GUI.**

Purpose: Manage Windows NT domains from Windows 2000 workstations.

Description: User Manager for Domains is a Windows NT 4.0 tool you can use to manage security for Windows NT 4.0 domains, member servers, and workstations. With User Manager for Domains you can:

- Select the domain or computer to be administered.

- Create and manage user accounts.
- Create and manage groups.
- Manage the security policies.

Note: For Windows 2000 domains, member servers, and Windows 2000 Professional computers, use Active Directory and the other Windows 2000 administrative tools instead.

Name:	**User Statistics**
Program:	**UsrStat.exe**
Interface:	**Command line.**

Purpose: Displays the user name, full name, and last logon date and time for each user in a given domain.

Description: This User Statistics command line utility displays user name, full name, and last logon date and time for each user account across all domain controllers.

References

Smith, Randy Franklin. "Top 10 Security Tools in the Win2K Server Resource Kit." *Windows 2000 Magazine,* December 2000. http://www.win2000mag.com/Articles/Index.cfm?ArticleID=15969&pg=1

Kiely, Don. "Security Tools in the Windows 2000 Resource Kit." *ITworld.com,* December 2000. http://www.itworld.com/nl/nt2k_sec/12042000/pf_index.html

_____. "Extracting event logs with DUMPEL.EXE." *Exploring Windows NT for Professionals,* September 1996. http://www.elementkjournals.com/ewn/9609/ewn9692.htm

Shinder, Thomas W. "Cool RK Tools: The CyberSafe Log Analyst." *Swynk.com,* ____. http://www.swynk.com/friends/shinder/cybersafe.asp

General References

Microsoft Technet. http://microsoft.com/technet/

Microsoft Windows 2000 Resource Kits.
http://www.microsoft.com/windows2000/techinfo/reskit/default.asp