Nessus Report

Report

24/Feb/2012:17:48:03 GMT

Table Of Contents

Compliance 'FAILED'.....9

- 2.1.1 Minimum Password Length: at least 8 characters.....10
- 2.2.1.1 Audit Account Logon Events: Success and Failure.....11
- 2.2.1.2 Audit Account Managemement: Success and Failure.....12
- 2.2.1.4 Audit Logon Events: Success and Failure.....13
- 2.2.1.5 Audit Object Access: Failure (minimum).....14
- 2.2.1.6 Audit Policy Change: Success and Failure.....15
- 2.2.1.7 Audit Privilege Use: Failure (minimum).....16
- 2.2.1.9 Audit System Events: Success and Failure.....17
- 2.2.2.1 Minimum Password Age: 1 day.....18
- 2.2.2.3 Minimum Password Length: 8 characters.....19
- 2.2.2.4 Password Complexity: Enabled.....20
- 2.2.2.5 Password History: 24 Passwords Remembered.....21
- 2.2.3.2 Account Lockout Threshold: 3 Bad Logon Attempts.....22
- 2.2.4.1.1 Maximum Event Log Size (Application): 80Mb.....23
- 2.2.4.1.3 Log Retention Method (Application): Overwrite Events As Needed.....24
- 2.2.4.2.1 Maximum Event Log Size (Security): 80Mb.....25
- 2.2.4.2.3 Log Retention Method (Security): Overwrite Events As Needed.....26
- 2.2.4.3.1 Maximum Event Log Size (System): 80Mb.....27
- 2.2.4.3.3 Log Retention Method (System): Overwrite Events As Needed.....28
- 3.1.1 Additional Restrictions for Anonymous Connections: No Access Without Explicit Anonymous Permissions.....29
- 3.2.1.2 Allow System to be Shut Down Without Having to Log On: Disabled.....30
- 3.2.1.9 Clear Virtual Memory Pagefile When System Shuts Down: Enabled.....31
- 3.2.1.13 Digitally Sign Server Communication (When Possible): Enabled.....32
- 3.2.1.15 Do Not Display Last User Name in Logon Screen: Enabled.....33
- 3.2.1.16 LAN Manager Authentication Level: 'Send NTLMv2 response only'.....34
- 3.2.1.17 Message Text for Users Attempting to Log On: Custom Message or 35
- 3.2.1.18 Message Title for Users Attempting to Log On: Warning: or custom title.....36
- 3.2.1.19 Number of Previous Logons to Cache: 0.....37
- 3.2.1.21 Prevent Users from Installing Printer Drivers: Enabled.....38
- 3.2.1.25 Rename Administrator Account: Anything but Administrator.....39
- 3.2.1.26 Rename Guest Account: Any value other than Guest.....40
- 3.2.1.28 Restrict Floppy Access to Locally Logged-On User Only: Enabled.....41
- 3.2.1.35 Smart Card Removal Behavior: Lock Workstation (minimum) 42
- 3.2.1.38 Unsigned Non-Driver Installation Behavior: Warn, but allow installation (minimum) or Do Not Allow Installation.....43
- 3.2.2.1 Suppress Dr. Watson Crash Dumps: HKLM\Software\Microsoft\DrWatson\CreateCrashDump: 0.....44
- 3.2.2.2 Disable Automatic Execution of the System Debugger: HKLM\Software\Microsoft\Windows NT \CurrentVersion\AEDebug\Auto: 0.....45
- 3.2.2.7 Disable automatic reboots after a Blue Screen of Death: HKLM\System\CurrentControlSet\Control \CrashControl: 0.....46
- 3.2.2.8 Disabled CD Autorun: HKLM\System\CurrentControlSet\Services\CDrom\Autorun: 0.....47
- 3.2.2.13 Ensure ICMP Routing via shortest path first: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters \EnableICMPRedirect: 0.....48

- 4.1 Available Servcies (MSFtpsvc): Permissions on FTP Publishing Service: Administrators: Full Control; System: Read, Start, Stop, and Pause....49
- 4.1 Available Services (Alerter): Permissions on Alerter: Administrators: Full Control; System: Read, Start, Stop, and Pause....50
- 4.1 Available Services (Browser): Permissions on Computer Browser: Administrators: Full Control; System: Read, Start, Stop, and Pause....51
- 4.1 Available Services (ClipSrv): Permissions on Clipbook: Administrators: Full Control; System: Read, Start, Stop, and Pause....52
- 4.1 Available Services (FAX): Permissions on Fax Service: Administrators: Full Control: System; Read, Start, Stop, and Pause....53
- 4.1 Available Services (IISADMIN): Permissions on IIS Admin Services: Administrators: Full Control; System: Read, Start, Stop, and Pause....54
- 4.1 Available Services (Messenger): Permissions on Messenger: Administrators: Full Control; System: Read, Start, Stop, and Pause....55
- 4.1 Available Services (RemoteAccess): Permissions on Routing and Remote Access: Administrators: Full Control; System: Read, Start, Stop, Pause....56
- 4.1 Available Services (RemoteRegistry): Permissions on Remote Registry Service: Administrators: Full Control; System: Read, Start, Stop, and Pause....57
- 4.1 Available Services (SMTPSVC): Permissions on SMTP: Administrators: Full Control; System: Read, Start, Stop, Pause....58
- 4.1 Available Services (SharedAccess): Permissions on Internet Connection Sharing: Administrators: Full Control; System: Read, Start, Stop, and Pause....59
- 4.1 Available Services (TlntSvr): Permissions on Telnet: Administrators: Full Control; System: Read, Start, Stop, and Pause....60
- 4.1 Available Services (W3SVC): Permissions on World Wide Web Publishing Service: Administrators: Full Control; System: Read, Start, Stop, and Pause....61
- 4.1 Available Services (mnmsrvc): Permissions on NetMeeting Remote Desktop Sharing: Administrators: Full Control; System: Read, Start, Stop, and Pause....62
- 4.1.1 Alerter (Alerter): Disabled....63
- 4.1.2 Clipbook (ClipSrv): Disabled....64
- 4.1.3 Computer Browser (Browser): Disabled....65
- 4.1.4 Fax Service (FAX): Disabled....66
- 4.1.5 FTP Publishing Service (MSFtpsvc): Disabled (Warning: This will disable FTP Servers)....67
- 4.1.6 IIS Admin Service (IISADMIN): Disabled (Warning: This will disable Internet Information Services)....68
- 4.1.7 Internet Connection Sharing (SharedAccess): Disabled....69
- 4.1.8 Messenger (Messenger): Disabled....70
- 4.1.9 NetMeeting Remote Desktop Sharing (mnmsrvc): Disabled....71
- 4.1.10 Remote Registry Service (RemoteRegistry): Disabled....72
- 4.1.12 Simple Mail Transfer Protocol (SMTP) (SMTPSVC): Disabled (Warning: This will disable certain functions on SMTP/IIS Servers!)....73
- 4.1.15 Telnet (TlntSvr): Disabled....74
- 4.1.16 World Wide Web Publishing Services (W3SVC): Disabled (Warning: This will disable Internet Information Services!)....75
- 4.2.1 Access this computer from the network (SeNetworkLogonRight): Users, Administrators (or none)....76
- 4.2.4 Back up files and directories (SeBackupPrivilege): Administrators....77
- 4.2.5 Bypass travrse checking (SeChangeNotifyPrivilege): Users....78
- 4.2.6 Change the system time (SeSystemTimePrivilege): Administrators....79
- 4.2.10 Debug programs (SeDebugPrivilege): None....80
- 4.2.11 Deny access to this computer from the network (SeDenyNetworkLogonRight): Guests....81
- 4.2.24 Log on locally (SeInteractiveLogonRight): Administrators....82
- 4.2.27 Profile single process (SeProfileSingleProcessPrivilege): Administrators....83
- 4.2.29 Remove computer from docking station (SeUndockPrivilege): Administrators....84

- 4.2.31 Restore files and directories (SeRestorePrivilege): Administrators..... 85
- 4.2.32 Shut down the system (SeShutdownPrivilege): Administrators..... 86
- 4.4.1.1 %SystemDrive%\ - Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List..... 87
- 4.4.1.2 %SystemDrive%\autoexec.bat: Administrators: Full; System: Full..... 88
- 4.4.1.3 %SystemDrive%\boot.ini - Administrators: Full; System: Full..... 89
- 4.4.1.4 %SystemDrive%\config.sys - Administrators: Full; System: Full..... 90
- 4.4.1.5 %SystemDrive%\io.sys - Administrators: Full; System: Full..... 91
- 4.4.1.6 %SystemDrive%\msdos.sys - Administrators: Full; System: Full..... 92
- 4.4.1.8 %SystemDrive%\ntdetect.com - Administrators: Full; System: Full..... 93
- 4.4.1.9 %SystemDrive%\ntldr - Administrators: Full; System: Full..... 94
- 4.4.1.10 %SystemDrive%\Documents and Settings - Administrators: Full; System: Full; Creater Owner: Full; Users: Read and Execute, List..... 95
- 4.4.1.11 %SystemDrive%\Documents and Settings\Administrator - Administrators: Full; System: Full..... 96
- 4.4.1.12 %SystemDrive%\Documents and Settings\All Users - Administrators: Full; System: Full; Creater Owner: Full; Users: Read and Execute, List..... 97
- 4.4.1.14 %SystemDrive%\Documents and Settings\Default User - Administrators: Full; System: Full; Users: Read & Execute, List..... 98
- 4.4.1.17 %ProgramFiles% - Administrators: Full; System: Full; Creater Owner: Full; Users: Read and Execute, List..... 99
- 4.4.1.19 %SystemRoot% - Administrators: Full; System: Full; Creater Owner: Full; Users: Read and Execute, List..... 100
- 4.4.1.21 %SystemRoote%\CSC - Administrators: Full; System: Full..... 101
- 4.4.1.22 %SystemRoot%\Debug - Administrators: Full; System: Full; Creater Owner: Full; Users: Read and Execute, List..... 102
- 4.4.1.23 %SystemRoot%\Debug\UserMode - Administrators: Full; System: Full; Users (This folder, only): Traverse Folders/Execute Files, List folder/Read data, Create files/Write data; Users (Files only): Create Files/Write Data; Create folders/Append data..... 103
- 4.4.1.25 %SystemRoot%\Registration - Administrators: Full; System: Full; Users: Read..... 104
- 4.4.1.26 %SystemRoot%\repair - Administrators: Full; System: Full..... 105
- 4.4.1.27 %SystemRoot%\security - Administrators: Full; System: Full; Creater Owner: Full..... 106
- 4.4.1.28 %SystemRoot%\system32 - Administrators: Full; System: Full; Creater Owner: Full; Users: Read and Execute, List..... 107
- 4.4.1.29 %SystemRoot%\system32\at.exe - Administrators: Full; System: Full..... 108
- 4.4.1.30 %SystemRoot%\system32\Ntbackup.exe - Administrators: Full; System: Full..... 109
- 4.4.1.31 %SystemRoot%\system32\rcp.exe - Administrators: Full; System: Full..... 110
- 4.4.1.32 %SystemRoot%\regedit.exe - Administrators: Full; System: Full..... 111
- 4.4.1.33 %SystemRoot%\system32\regedt32.exe - Administrators: Full; System: Full..... 112
- 4.4.1.34 %SystemRoot%\system32\rexec.exe - Administrators: Full; System: Full..... 113
- 4.4.1.35 %SystemRoot%\system32\rsh.exe - Administrators: Full; System: Full..... 114
- 4.4.1.36 %SystemRoot%\system32\secedit.exe - Administrators: Full; System: Full..... 115
- 4.4.1.38 %SystemRoot%\config - Administrators: Full; System: Full..... 116
- 4.4.1.40 %SystemRoot%\system32\DTCLog - Administrators: Full; System: Full; Users: Read and Execute, List..... 117
- 4.4.1.43 %SystemRoot%\system32\NTMSData - Administrators: Full; System: Full..... 118
- 4.4.1.45 %SystemRoot%\system32\Setup - Admininstrators: Full; System: Full; Users: Read and Execute, List..... 119
- 4.4.1.46 %SystemRoot%\system32\spool\printers - Administrators: Full; System: Full; Creater Owner: Full; Users: Traverse Folder/Execute file, Read, Read Extended Attributes, Create folders, Append Data..... 120
- 4.4.1.48 %SystemRoot%\Temp - Administrators: Full; System: Full; Creater Owner: Full; Users: Traverse Folders/Execute Files, Create Files/Write Data, Create Folders/Append Data..... 121

- 4.4.2.1 HKLM\Software\Classes - Administrators: Full; System: Full; Creater Owner: Full; Users: Read.....122
- 4.4.2.2 HKLM\Software - Administrators: Full; System: Full; Creater Owner: Full; Users: Read.....123
- 4.4.2.3 HKLM\Software\Microsoft\NetDDE - Administrators: Full; System: Full.....124
- 4.4.2.4 HKLM\Software\Microsoft\OS/2 Subsystem for NT - Administrators: Full System: FUll; Creater Owner: Full.....125
- 4.4.2.5 HKLM\Software\Microsoft\Windows NT\CurrentVersion\AsrCommands - Administrators: Full; System: Full; Creater Owner: Full; Users: Read; Backup Operators (this key and subkeys): Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, Read.....126
- 4.4.2.8 HKLM\Software\Microsoft\Windows\CurrentVersion\Installer - Administrators: Full; System: Full; Users: Read.....127
- 4.4.2.10 HKLM\System - Administrators: Full; System: Full; Creater Owner: Full; Users: Read.....128
- 4.4.2.12 HKLM\System\ControlSet001 - Administrators: Full; System: Full; Creater Owner: Full; Users: Read.....129
- 4.4.2.13 HKLM\System\ControlSet002 - Administrators: Full; System: Full; Creater Owner: Full; Users: Read.....130
- 4.4.2.14 HKLM\System\CurrentControlSet\Control\SecurePipeServers\WinReg - Administrators: Full; System: Full; Backup Operators: Query Value, Enumerate Subkeys, Notify, Read Permissions.....131
- 4.4.2.15 HKLM\System\CurrentControlSet\Control\WMI\Security - Administrators: Full; System: Full; Creater Owner (this key and subkeys): Full.....132
- 4.4.2.17 HKLM\System\CurrentControlSet\Hardware Profiles - Administrators: Full; System: Full; Creater Owner: Full; Users: Read.....133
- 4.4.2.20 HKU\.Default - Administrators: Full; System: Full; Creater Owner: Full; Users: Read.....134
- 4.4.2.21 HKU\.Default\Software\Microsoft\NetDDE.....135
- 4.4.3.1 %SystemDrive% - Everyone: Failures (this folder, propagate inheritable permissions to all subfolders).....136
- 4.4.3.2 HKLM\Software - Everyone: Failures (this key, propagate inheritable permissions to all subfolders).....137
- 4.4.3.3 HKLM\System - Everyone: Failures (this key, propagate inheritable permissions to all subfolders).....138

Compliance 'SKIPPED'.....139

Compliance 'PASSED'.....140

- 2.1.2 Maximum Password Age: no more than 90 days old.....141
- 2.2.2.2 Maximum Password Age: 90 days.....142
- 2.2.2.6 Store Passwords using Reversible Encryption: Disabled.....143
- 2.2.3.1 Account Lockout Duration: 15 minutes.....144
- 2.2.3.3 Reset Account Lockout After: 15 Minutes.....145
- 3.2.1.3 Allowed to Eject Removable NTFS Media: Administrators.....146
- 3.2.1.4 Amount of Idle Time Required Before Disconnecting Session: 30 Minutes.....147
- 3.2.1.7 Automatically Log Off Users When Logon Time Expires: Enabled.....148
- 3.2.1.11 Digitally Sign Client Communication (When Possible): Enabled.....149
- 3.2.1.20 Prevent System Maintenance of Computer Account Password: Disabled.....150
- 3.2.1.22 Prompt User to Change Password Before Expiration: 14 days.....151
- 3.2.1.23 Recovery Console: Allow Automatic Administrative Logon: Disabled.....152
- 3.2.1.24 Recover Console: Allow Floppy Copy and Access to All Drives and All Folders: Disabled.....153
- 3.2.1.30 Secure Channel: Digitally Encrypt Secure Channel Data (When Possible): Enabled.....154
- 3.2.1.31 Secure Channel: Digitally Sign Secure Channel Data (When Possible): Enabled.....155
- 3.2.1.33 Send Unencrypted Password to Connect to Third-Part SMB Servers: Disabled.....156
- 3.2.1.36 Strengthen Default Permissions of Global System Objects (i.e. Symbolic Links): Enabled.....157
- 3.2.1.37 Unsigned Driver Installation Behavior: Warn, but allow installation (minimum) or Do Not Allow Installation.....158
- 3.2.2.4 Disable Automatic Logon: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon \AutoAdminLogon: 0.....159
- 3.2.2.21 Enable IPSec to protect Kerberos RSVP Traffic: HKLM\System\CurrentControlSet\Services\IPSEC \NoDefaultExempt: 1.....160

- 4.1 Available Services (SNMP): Permissions on SNMP: Administrators: Full Control; System: Read, Start, Stop, and Pause..... 161
- 4.1 Available Services (SNMPTRAP): Permissions on SNMP Trap: Administrators: Full Control; Sytem: Read, Start, Stop, and Pause.....162
- 4.1.11 Routing and Remote Access (RemoteAccess): Disabled.....163
- 4.1.13 Simple Network Management Protocol (SNMP) Service: Disabled.....164
- 4.1.14 Simple Network Management Protocol (SNMP) Trap (SNMPTRAP): Disabled..... 165
- 4.2.2 Act as part of the operating system (SeTcbPrivilege): None..... 166
- 4.2.7 Create a pagefile (SeCreatePagefilePrivilege): Administrators..... 167
- 4.2.8 Create a token object (SeCreateTokenPrivilege): None.....168
- 4.2.9 Create permanent shared objects (SeCreatePermanentPrivilege): None..... 169
- 4.2.16 Force shutdown from a remote system (SeRemoteShutdownPrivilege): Administrators.....170
- 4.2.17 Generate security audits (SeAuditPrivilege): None..... 171
- 4.2.18 Increase quotas: Administrators..... 172
- 4.2.19 Increase schedulign priority (SeIncreaseBasePriorityPrivilege): Administrators.....173
- 4.2.20 Load and unload device drivers (SeLoadDriverPrivilege): Administrators.....174
- 4.2.21 Lock pages in memory (SeLockMemoryPrivilege): None.....175
- 4.2.25 Manage auditing and security log (SeSecurityPrivilege): Administrators.....176
- 4.2.26 Modify firmware environment values (SeSystemEnvironmentPrivilege): Administrators..... 177
- 4.2.28 Profile system performance (SeSystemProfilePrivilege): Administrators.....178
- 4.2.30 Replace a process level token (SeAssignPrimaryTokenPrivilege): None.....179
- 4.2.34 Take ownership of files or other objects (SeTakeOwnershipPrivilege): Administrators.....180
- 4.4.1.7 %SystemDrive%\ntbootdd.sys - Administrators: Full; System: Full..... 181
- 4.4.1.13 %SystemDrive%\Documents and Settings\All Users\Documents\DrWatson - Administrators: Full; System: Full; Creater Owner: Full; Users (This folder, subfolders and files): Traverse Folder/Execute File, List Folder/Read Data, Read Attributes, Read Extended Attributes, Read Permissions; Users (Subfolders and files only): Traverse Folder/Execute Files, Create Files/Write Data, Create Folder/Append Data.....182
- 4.4.1.16 %SystemDrive%\Temp - Administrators: Full; System: Full; Creater Owner: Full; Users: Traverse Folders/Execute Files, Create Files/Write Data, Create Folders/Append Data.....183
- 4.4.1.18 %SystemDrive%\Program Files\Resource Kit - Administrators: Full; System: Full.....184
- 4.4.1.20 %SystemRoot%\$NtServicePackUninstall$ - Administrators: Full; System: Full..... 185
- 4.4.1.37 %SystemRoot%\system32\appmgmt - Administrators: Full; System: Full; Users: Read and Execute, List..... 186
- 4.4.1.39 %SystemRoot%\system32\dllcache - Adminstrators: Full; System: Full; Creater Owner: Full.....187
- 4.4.1.41 %SystemRoot%\system32\GroupPolicy - Administrators: Full; System: Full; Authenticated Users: Read and Execute, List.....188
- 4.4.1.42 %SystemRoot%\system32\ias - Administrators: Full; System: Full; Creater Owner: Full..... 189
- 4.4.1.44 %SystemRoot%\system32\reinstallbackups - Administrators: Full; System: Full; Creater Owner: Full.....190
- 4.4.2.6 HKLM\Software\Microsoft\Windows NT\CurrentVersion\Perflib - Administrators: Full; System: Full; Creator ... (see CIS Doc)..... 191
- 4.4.2.7 HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy - Administrators: Full; System: Full; Authenticated Users: Read..... 192
- 4.4.2.9 HKLM\Software\Microsoft\Windows\CurrentVersion\Policies - Administrators: Full; System: Full; Authenticated Users: Read..... 193
- 4.4.2.13 HKLM\System\ControlSet003 - Administrators Full; System: Full; Creator Owner: Full; Users: Read.....194
- 4.4.2.13 HKLM\System\ControlSet004 - Administrators Full; System: Full; Creator Owner: Full; Users: Read.....195
- 4.4.2.13 HKLM\System\ControlSet005 - Administrators Full; System: Full; Creator Owner: Full; Users: Read.....196
- 4.4.2.13 HKLM\System\ControlSet006 - Administrators Full; System: Full; Creator Owner: Full; Users: Read.....197
- 4.4.2.13 HKLM\System\ControlSet007 - Administrators Full; System: Full; Creator Owner: Full; Users: Read.....198
- 4.4.2.13 HKLM\System\ControlSet008 - Administrators Full; System: Full; Creator Owner: Full; Users: Read.....199

- 4.4.2.13 HKLM\System\ControlSet009 - Administrators Full; System: Full; Creator Owner: Full; Users: Read..... 200

Compliance 'INFO', 'WARNING', 'ERROR'..... 201

- 2.2.4.1.2 Restrict Guest Access to Logs: Enabled..... 202
- 2.2.4.2.2 Restrict Guest Access to Logs (Security): Enabled..... 203
- 2.2.4.3.2 Restrict Guest Access to Logs (System): Enabled..... 204
- 3.2.1.14 Disable CTRL+ALT+Delete Requirement for Logon: Disabled..... 205
- 3.2.2.3 Disable autoplay from any disk type, regardless of application: HKLM\Software\Microsoft\Windows \CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun: 255..... 206
- 3.2.2.3.1 Disable autoplay for current user: HKCU\Sofware\Microsoft\Windows\CurrentVersion\Policies\Explorer \NoDriveTypeAutoRun: 255. Cannot determine this value remotely, if using Security Center please check value and recast result to passed or failed..... 207
- 3.2.2.5 Mask any typed passwords with asterisks: HKLM\Software\Microsoft\Windows\CurrentVersion\Policies \Network\HideSharePwds: 1..... 208
- 3.2.2.6 Disable Dial-in access to the server: HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Network \NoDialIn: 1..... 209
- 3.2.2.9 Remove administrative shares on servers: HKLM\System\CurrentControlSet\Services\LanmanServer \Parameters\AutoShareServer: 0..... 210
- 3.2.2.10 Protect against Computer Browsing Spoofing Attacks: HKLM\System\CurrentControlSet\Services\MrxSmb \Parameters\RefuseReset: 1..... 211
- 3.2.2.11 Protect against source-routing spoofing: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters \DisableIPSourceRouting: 2..... 212
- 3.2.2.12 Protect the Default Gateway netowrk setting: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters \EnableDeadGWDetect: 0..... 213
- 3.2.2.14 Help protect against packet fragmentation: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters \EnablePMTUDiscovery: 0..... 214
- 3.2.2.15 Manage keep-alive times: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime: 300000..... 215
- 3.2.2.16 Protect Against Malicious Name-Release Attacks: HKLM\System\CurrentControlSet\Services\NetBt \Parameters\NoNameReleaseOnDemand: 1..... 216
- 3.2.2.17 Ensure Router Discover is Disabled: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters \SynAttackProtect: 0..... 217
- 3.2.2.18 Protect against SYN Flood attacks: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters \SynAttackProtect: 2..... 218
- 3.2.2.19 SYN attack protection - Manage TCP Maximum half-open sockets: HKLM\System\CurrentControlSet \Services\Tcpip\Parameters\TcpMaxHalfOpen: 100 or 500..... 219
- 3.2.2.20 SYN Attack protection - Manage TCP Maximum half-open retired sockets: HKLM\System \CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenRetired: 80 or 400..... 220
- 4.4.1.15 %SystemDrive%\System Volume Information - Do not allow permissions this folder to be replaced. Cannot determine this value remotely, if using Security Center please check value and recast result to passed or failed... 221
- 4.4.1.24 %SystemRoot%\Offline Web Pages - Do not allow permissions on this key to be replaced - Do not allow permissions this folder to be replaced. Cannot determine this value remotely, if using Security Center please check value and recast result to passed or failed..... 222
- 4.4.1.47 %SystemRoot%\Tasks - Do not allow permissions on this key to be replaced. Cannot determine this value remotely, if using Security Center please check value and recast result to passed or failed..... 223
- 4.4.2.11 HKLM\System\Clone - Allow inheritable permissions to propogate to this object. Cannot determine this value remotely, if using Security Center please check value and recast result to passed or failed..... 224
- 4.4.2.16 HKLM\System\CurrentControlSet\Enum - Administrators: Read; System: Full; Authenticated Users: Read (Do not allow permissions on this key to be replaced). Cannot determine this value remotely, if using Security Center please check value and recast result to passed or failed..... 225
- 4.4.2.18 HKLM\System\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers - Administrators Full; System: Full; Creator Owner: Full..... 226
- 4.4.2.19 HKLM\System\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities - Administrators Full; System: Full; Creator Owner: Full..... 227

•4.4.2.22 HKU\.Default\Software\Microsoft\Protected Storage System Provider - No entries. Cannot determine this value remotely, if using Security Center please check value and recast result to passed or failed..... 228

Compliance 'FAILED'

2.1.1 Minimum Password Length: at least 8 characters

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 21

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

[8..4294967295]

Hosts

192.168.1.205	`0`

2.2.1.1 Audit Account Logon Events: Success and Failure

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 21

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"success, failure"

Hosts

192.168.1.205	`"no auditing"`

2.2.1.2 Audit Account Managemement: Success and Failure

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 22

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"success, failure"

Hosts

192.168.1.205	`"no auditing"`

2.2.1.4 Audit Logon Events: Success and Failure

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 22

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"success, failure"

Hosts

192.168.1.205	`"no auditing"`

2.2.1.5 Audit Object Access: Failure (minimum)

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 22

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"failure" || "success, failure"

Hosts

192.168.1.205	`"no auditing"`

2.2.1.6 Audit Policy Change: Success and Failure

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 22

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"success, failure"

Hosts

192.168.1.205	`"no auditing"`

2.2.1.7 Audit Privilege Use: Failure (minimum)

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 22

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"failure" || "success, failure"

Hosts

192.168.1.205	`"no auditing"`

2.2.1.9 Audit System Events: Success and Failure

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 23

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"success, failure"

Hosts

192.168.1.205	`"no auditing"`

2.2.2.1 Minimum Password Age: 1 day

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 23

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

[1..4294967295]

Hosts

192.168.1.205	`0`

2.2.2.3 Minimum Password Length: 8 characters

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 23

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

[8..4294967295]

Hosts

192.168.1.205	`0`

2.2.2.4 Password Complexity: Enabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 23

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

1

Hosts

192.168.1.205	`0`

2.2.2.5 Password History: 24 Passwords Remembered

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 24

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

[24..4294967295]

Hosts

192.168.1.205	`0`

2.2.3.2 Account Lockout Threshold: 3 Bad Logon Attempts

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 24

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

[1..3]

Hosts

192.168.1.205	`0`

2.2.4.1.1 Maximum Event Log Size (Application): 80Mb

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 25

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

[81920..4294967295]

Hosts

192.168.1.205	512

2.2.4.1.3 Log Retention Method (Application): Overwrite Events As Needed

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 25

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

0

Hosts

192.168.1.205	`604800`

2.2.4.2.1 Maximum Event Log Size (Security): 80Mb

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 25

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

[81920..4294967295]

Hosts

192.168.1.205	512

2.2.4.2.3 Log Retention Method (Security): Overwrite Events As Needed

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 25

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

0

Hosts

192.168.1.205	`604800`

2.2.4.3.1 Maximum Event Log Size (System): 80Mb

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 25

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

[81920..4294967295]

Hosts

192.168.1.205	512

2.2.4.3.3 Log Retention Method (System): Overwrite Events As Needed

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 25

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

0

Hosts

192.168.1.205	`604800`

3.1.1 Additional Restrictions for Anonymous Connections: No Access Without Explicit Anonymous Permissions

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 25

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

2

Hosts

192.168.1.205	`0`

3.2.1.2 Allow System to be Shut Down Without Having to Log On: Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 26

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"disabled"

Hosts

192.168.1.205	`"enabled"`

3.2.1.9 Clear Virtual Memory Pagefile When System Shuts Down: Enabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 27

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"enabled"

Hosts

192.168.1.205	`"disabled"`

3.2.1.13 Digitally Sign Server Communication (When Possible): Enabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 27

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"enabled"

Hosts

192.168.1.205	`"disabled"`

3.2.1.15 Do Not Display Last User Name in Logon Screen: Enabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 28

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"enabled"

Hosts

192.168.1.205	`"disabled"`

3.2.1.16 LAN Manager Authentication Level: 'Send NTLMv2 response only'

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 28

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

[3..5]

Hosts

192.168.1.205	`0`

3.2.1.17 Message Text for Users Attempting to Log On: Custom Message or ...

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 29

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

""

Hosts

192.168.1.205	""

3.2.1.18 Message Title for Users Attempting to Log On: Warning: or custom title

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 29

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

""

Hosts

192.168.1.205	""

3.2.1.19 Number of Previous Logons to Cache: 0

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 29

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

0

Hosts

192.168.1.205	`10`

3.2.1.21 Prevent Users from Installing Printer Drivers: Enabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 30

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"enabled"

Hosts

192.168.1.205	`"disabled"`

3.2.1.25 Rename Administrator Account: Anything but Administrator

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 31

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"administrator"

Hosts

192.168.1.205	`"Administrator"`

3.2.1.26 Rename Guest Account: Any value other than Guest

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 31

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"guest"

Hosts

192.168.1.205	`"Guest"`

3.2.1.28 Restrict Floppy Access to Locally Logged-On User Only: Enabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 31

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"enabled"

Hosts

192.168.1.205	`"disabled"`

3.2.1.35 Smart Card Removal Behavior: Lock Workstation (minimum)

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 33

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

[1..2]

Hosts

192.168.1.205	`0`

3.2.1.38 Unsigned Non-Driver Installation Behavior: Warn, but allow installation (minimum) or Do Not Allow Installation

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 33

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

[1..2]

Hosts

192.168.1.205	`0`

3.2.2.1 Suppress Dr. Watson Crash Dumps: HKLM\Software\Microsoft\DrWatson\CreateCrashDump: 0

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 34

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

0

Hosts

192.168.1.205	1

3.2.2.2 Disable Automatic Execution of the System Debugger: HKLM\Software\Microsoft\Windows NT \CurrentVersion\AEDebug\Auto: 0

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 34

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

0

Hosts

192.168.1.205	1

3.2.2.7 Disable automatic reboots after a Blue Screen of Death: HKLM\System\CurrentControlSet\Control\CrashControl: 0

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 35

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

0

Hosts

192.168.1.205	1

3.2.2.8 Disabled CD Autorun: HKLM\System\CurrentControlSet\Services\CDrom\Autorun: 0

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 35

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

0

Hosts

192.168.1.205	1

3.2.2.13 Ensure ICMP Routing via shortest path first: HKLM\System\CurrentControlSet\Services \Tcpip\Parameters\EnableICMPRedirect: 0

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 36

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

0

Hosts

192.168.1.205	1

4.1 Available Servcies (MSFtpsvc): Permissions on FTP Publishing Service: Administrators: Full Control; System: Read, Start, Stop, and Pause

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 39

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "read" | "start, stop and pause"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "change template" | "delete"
| "enumerate dependents" | "full control" | "interrogate" |
"pause and continue" | "query status" | "query template" | "read
permissions" | "start" | "stop" | "take ownership" | "user-defined
control"

authenticated users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions" | "user-defined control"

power users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read permissions"
| "start" | "stop" | "user-defined control"

system:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read [...]
```

4.1 Available Services (Alerter): Permissions on Alerter: Administrators: Full Control; System: Read, Start, Stop, and Pause

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 38

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "read" | "start, stop and pause"

Hosts

192.168.1.205

```
1-5-11:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions" | "user-defined control"

1-5-18:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read permissions"
| "start" | "stop" | "user-defined control"

1-5-32-544:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "change template" | "delete"
| "enumerate dependents" | "full control" | "interrogate" |
"pause and continue" | "query status" | "query template" | "read
permissions" | "start" | "stop" | "take ownership" | "user-defined
control"

1-5-32-547:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read permissions"
| "s [...]
```

4.1 Available Services (Browser): Permissions on Computer Browser: Administrators: Full Control; System: Read, Start, Stop, and Pause

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 39

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "read" | "start, stop and pause"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "change template" | "delete"
| "enumerate dependents" | "full control" | "interrogate" |
"pause and continue" | "query status" | "query template" | "read
permissions" | "start" | "stop" | "take ownership" | "user-defined
control"

authenticated users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions" | "user-defined control"

power users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions" | "start" | "user-defined
control"

system:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read permissions"
| "start" | "stop" [...]
```

4.1 Available Services (ClipSrv): Permissions on Clipbook: Administrators: Full Control; System: Read, Start, Stop, and Pause

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 38

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "read" | "start, stop and pause"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this object and child objects"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "change template" | "delete"
| "enumerate dependents" | "full control" | "interrogate" |
"pause and continue" | "query status" | "query template" | "read
permissions" | "start" | "stop" | "take ownership" | "user-defined
control"

everyone:
 + Apply To: "this object and child objects"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions"

interactive:
 + Apply To: "this object and child objects"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "start"

power users:
 + Apply To: "this object and child objects"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions"
```

4.1 Available Services (FAX): Permissions on Fax Service: Administrators: Full Control: System; Read, Start, Stop, and Pause

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 39

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "read" | "start, stop and pause"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "change template" | "delete"
| "enumerate dependents" | "full control" | "interrogate" |
"pause and continue" | "query status" | "query template" | "read
permissions" | "start" | "stop" | "take ownership" | "user-defined
control"

authenticated users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions" | "user-defined control"

everyone:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "query status" | "start"

power users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read permissions"
| "start" | "stop" | "user-defined control"

system:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 [...]
```

4.1 Available Services (IISADMIN): Permissions on IIS Admin Services: Administrators: Full Control; System: Read, Start, Stop, and Pause

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 39

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "read" | "start, stop and pause"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "change template" | "delete"
| "enumerate dependents" | "full control" | "interrogate" |
"pause and continue" | "query status" | "query template" | "read
permissions" | "start" | "stop" | "take ownership" | "user-defined
control"

authenticated users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions" | "user-defined control"

power users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read permissions"
| "start" | "stop" | "user-defined control"

system:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read [...]
```

4.1 Available Services (Messenger): Permissions on Messenger: Administrators: Full Control; System: Read, Start, Stop, and Pause

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 39

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "read" | "start, stop and pause"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "change template" | "delete"
| "enumerate dependents" | "full control" | "interrogate" |
"pause and continue" | "query status" | "query template" | "read
permissions" | "start" | "stop" | "take ownership" | "user-defined
control"

authenticated users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions" | "user-defined control"

power users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions" | "start" | "user-defined
control"

system:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read permissions"
| "start" | "stop" [...]
```

4.1 Available Services (RemoteAccess): Permissions on Routing and Remote Access: Administrators: Full Control; System: Read, Start, Stop, Pause

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 40

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "read" | "start, stop and pause"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "change template" | "delete"
| "enumerate dependents" | "full control" | "interrogate" |
"pause and continue" | "query status" | "query template" | "read
permissions" | "start" | "stop" | "take ownership" | "user-defined
control"

authenticated users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions" | "user-defined control"

power users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read permissions"
| "start" | "stop" | "user-defined control"

system:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read [...]
```

4.1 Available Services (RemoteRegistry): Permissions on Remote Registry Service: Administrators: Full Control; System: Read, Start, Stop, and Pause

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 40

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "read" | "start, stop and pause"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "change template" | "delete"
| "enumerate dependents" | "full control" | "interrogate" |
"pause and continue" | "query status" | "query template" | "read
permissions" | "start" | "stop" | "take ownership" | "user-defined
control"

authenticated users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions" | "user-defined control"

power users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions" | "start" | "user-defined
control"

system:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read permissions"
| "start" | "stop" [...]
```

4.1 Available Services (SMTPSVC): Permissions on SMTP: Administrators: Full Control; System: Read, Start, Stop, Pause

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 40

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "read" | "start, stop and pause"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "change template" | "delete"
| "enumerate dependents" | "full control" | "interrogate" |
"pause and continue" | "query status" | "query template" | "read
permissions" | "start" | "stop" | "take ownership" | "user-defined
control"

authenticated users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions" | "user-defined control"

power users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read permissions"
| "start" | "stop" | "user-defined control"

system:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read [...]
```

4.1 Available Services (SharedAccess): Permissions on Internet Connection Sharing: Administrators: Full Control; System: Read, Start, Stop, and Pause

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 39

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "read" | "start, stop and pause"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "change template" | "delete"
| "enumerate dependents" | "full control" | "interrogate" |
"pause and continue" | "query status" | "query template" | "read
permissions" | "start" | "stop" | "take ownership" | "user-defined
control"

authenticated users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions" | "user-defined control"

power users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read permissions"
| "start" | "stop" | "user-defined control"

system:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read [...]
```

4.1 Available Services (TlntSvr): Permissions on Telnet: Administrators: Full Control; System: Read, Start, Stop, and Pause

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 41

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "read" | "start, stop and pause"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "change template" | "delete"
| "enumerate dependents" | "full control" | "interrogate" |
"pause and continue" | "query status" | "query template" | "read
permissions" | "start" | "stop" | "take ownership" | "user-defined
control"

authenticated users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions" | "user-defined control"

power users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read permissions"
| "start" | "stop" | "user-defined control"

system:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read [...]
```

4.1 Available Services (W3SVC): Permissions on World Wide Web Publishing Service: Administrators: Full Control; System: Read, Start, Stop, and Pause

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 41

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "read" | "start, stop and pause"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "change template" | "delete"
| "enumerate dependents" | "full control" | "interrogate" |
"pause and continue" | "query status" | "query template" | "read
permissions" | "start" | "stop" | "take ownership" | "user-defined
control"

authenticated users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions" | "user-defined control"

power users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read permissions"
| "start" | "stop" | "user-defined control"

system:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read [...]
```

4.1 Available Services (mnmsrvc): Permissions on NetMeeting Remote Desktop Sharing: Administrators: Full Control; System: Read, Start, Stop, and Pause

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 39

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this object only"
|- Inheritance: "not used"
|- Allow: "read" | "start, stop and pause"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "change template" | "delete"
| "enumerate dependents" | "full control" | "interrogate" |
"pause and continue" | "query status" | "query template" | "read
permissions" | "start" | "stop" | "take ownership" | "user-defined
control"

authenticated users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "query status"
| "query template" | "read permissions" | "user-defined control"

power users:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read permissions"
| "start" | "stop" | "user-defined control"

system:
 + Apply To: "this object only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate dependents" | "interrogate" | "pause and
continue" | "query status" | "query template" | "read [...]
```

4.1.1 Alerter (Alerter): Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 38

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"disabled"

Hosts

192.168.1.205	`"manual"`

4.1.2 Clipbook (ClipSrv): Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 38

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"disabled"

Hosts

192.168.1.205	`"manual"`

4.1.3 Computer Browser (Browser): Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 39

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"disabled"

Hosts

192.168.1.205	`"automatic"`

4.1.4 Fax Service (FAX): Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 39

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"disabled"

Hosts

192.168.1.205	`"manual"`

4.1.5 FTP Publishing Service (MSFtpsvc): Disabled (Warning: This will disable FTP Servers)

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 39

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"disabled"

Hosts

192.168.1.205	`"automatic"`

4.1.6 IIS Admin Service (IISADMIN): Disabled (Warning: This will disable Internet Information Services)

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 39

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"disabled"

Hosts

192.168.1.205	`"automatic"`

4.1.7 Internet Connection Sharing (SharedAccess): Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 39

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"disabled"

Hosts

192.168.1.205	`"manual"`

4.1.8 Messenger (Messenger): Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 39

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"disabled"

Hosts

192.168.1.205	`"automatic"`

4.1.9 NetMeeting Remote Desktop Sharing (mnmsrvc): Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 39

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"disabled"

Hosts

192.168.1.205	`"manual"`

4.1.10 Remote Registry Service (RemoteRegistry): Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 40

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"disabled"

Hosts

192.168.1.205	`"automatic"`

4.1.12 Simple Mail Transfer Protocol (SMTP) (SMTPSVC): Disabled (Warning: This will disable certain functions on SMTP/IIS Servers!)

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 40

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"disabled"

Hosts

192.168.1.205	`"automatic"`

4.1.15 Telnet (TlntSvr): Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 41

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"disabled"

Hosts

192.168.1.205	`"manual"`

4.1.16 World Wide Web Publishing Services (W3SVC): Disabled (Warning: This will disable Internet Information Services!)

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 41

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"disabled"

Hosts

192.168.1.205	`"automatic"`

4.2.1 Access this computer from the network (SeNetworkLogonRight): Users, Administrators (or none)

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 41

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"users" && "administrators"

Hosts

192.168.1.205	`"backup operators" && "power users" && "users" && "administrators" && "iwam_windows2000" && "iusr_windows2000" && "everyone"`

4.2.4 Back up files and directories (SeBackupPrivilege): Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 42

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"administrators"

Hosts

192.168.1.205	`"backup operators" && "administrators"`

4.2.5 Bypass travrse checking (SeChangeNotifyPrivilege): Users

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 42

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"users"

Hosts

192.168.1.205	`"backup operators" && "power users" && "users" && "administrators" && "everyone"`

4.2.6 Change the system time (SeSystemTimePrivilege): Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 42

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"administrators"

Hosts

192.168.1.205	`"power users" && "administrators"`

4.2.10 Debug programs (SeDebugPrivilege): None

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 42

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

""

Hosts

192.168.1.205	`"administrators"`

4.2.11 Deny access to this computer from the network (SeDenyNetworkLogonRight): Guests

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 43

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"guests"

Hosts

192.168.1.205	NULL

4.2.24 Log on locally (SeInteractiveLogonRight): Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 44

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"administrators"

Hosts

192.168.1.205	`"backup operators" && "power users" && "users" && "administrators" && "guest" && "iusr_windows2000"`

4.2.27 Profile single process (SeProfileSingleProcessPrivilege): Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 44

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"administrators"

Hosts

192.168.1.205	`"power users" && "administrators"`

4.2.29 Remove computer from docking station (SeUndockPrivilege): Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 44

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"administrators"

Hosts

192.168.1.205	`"power users" && "users" && "administrators"`

4.2.31 Restore files and directories (SeRestorePrivilege): Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 45

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"administrators"

Hosts

192.168.1.205	`"backup operators" && "administrators"`

4.2.32 Shut down the system (SeShutdownPrivilege): Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 45

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

"administrators"

Hosts

192.168.1.205	`"backup operators" && "power users" && "users" && "administrators"`

4.4.1.1 %SystemDrive%\ - Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 46

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subfolders and files only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "list folder contents" | "list folder contents"

Hosts

192.168.1.205

```
everyone:
 + Apply To: "this folder, subfolders and files"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"
```

4.4.1.2 %SystemDrive%\autoexec.bat: Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 46

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
everyone:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"
```

4.4.1.3 %SystemDrive%\boot.ini - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

power users:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

system:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions" |
"take ownership" | "trav [...]
```

4.4.1.4 %SystemDrive%\config.sys - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
everyone:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"
```

4.4.1.5 %SystemDrive%\io.sys - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
everyone:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"
```

4.4.1.6 %SystemDrive%\msdos.sys - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
everyone:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"
```

4.4.1.8 %SystemDrive%\ntdetect.com - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

power users:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

system:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions" |
"take ownership" | "trav [...]
```

4.4.1.9 %SystemDrive%\ntldr - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

power users:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

system:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions" |
"take ownership" | "trav [...]
```

4.4.1.10 %SystemDrive%\Documents and Settings - Administrators: Full; System: Full; Creater Owner: Full; Users: Read and Execute, List

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "list folder contents" | "list folder contents"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

everyone:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
exten [...]
```

4.4.1.11 %SystemDrive%\Documents and Settings\Administrator - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrator:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data" |
" [...]
```

4.4.1.12 %SystemDrive%\Documents and Settings\All Users - Administrators: Full; System: Full; Creater Owner: Full; Users: Read and Execute, List

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "list folder contents" | "list folder contents"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

everyone:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
exten [...]
```

4.4.1.14 %SystemDrive%\Documents and Settings\Default User - Administrators: Full; System: Full; Users: Read & Execute, List

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "list folder contents" | "list folder contents"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

everyone:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
exten [...]
```

4.4.1.17 %ProgramFiles% - Administrators: Full; System: Full; Creater Owner: Full; Users: Read and Execute, List

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subfolders and files only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "list folder contents" | "list folder contents"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

creator owner:
 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data
[...]
```

4.4.1.19 %SystemRoot% - Administrators: Full; System: Full; Creater Owner: Full; Users: Read and Execute, List

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subfolders and files only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "list folder contents" | "list folder contents"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

creator owner:
 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data
[...]
```

4.4.1.21 %SystemRoote%\CSC - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"
```

4.4.1.22 %SystemRoot%\Debug - Administrators: Full; System: Full; Creater Owner: Full; Users: Read and Execute, List

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subfolders and files only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "list folder contents" | "list folder contents"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder, subfolders and files"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

creator owner:
 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

power users:
 + Apply To: "this folder, subfolders and files"
 |- Inheritance: "inherited"
 |- Allow: "create files  [...]
```

4.4.1.23 %SystemRoot%\Debug\UserMode - Administrators: Full; System: Full; Users (This folder, only): Traverse Folders/Execute Files, List folder/Read data, Create files/Write data; Users (Files only): Create Files/Write Data; Create folders/Append data

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this folder only"
|- Inheritance: "not used"
|- Allow: "traverse folder / execute file" | "list folder / read data" | "create files / write data"
+ Apply To: "files only"
|- Inheritance: "not used"
|- Allow: "create files / write data" | "create folders / append data"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

power users:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "create files / write data" | "create folders / append
d [...]
```

4.4.1.25 %SystemRoot%\Registration - Administrators: Full; System: Full; Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "read"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder and files"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

everyone:
 + Apply To: "this folder and files"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions"

system:
 + Apply To: "this folder and files"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions" |
"take ownership" | "traverse folder / execute f [...]
```

4.4.1.26 %SystemRoot%\repair - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

creator owner:
 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data
[...]
```

4.4.1.27 %SystemRoot%\security - Administrators: Full; System: Full; Creater Owner: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subfolders and files only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

creator owner:
 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data
[...]
```

4.4.1.28 %SystemRoot%\system32 - Administrators: Full; System: Full; Creater Owner: Full; Users: Read and Execute, List

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subfolders and files only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "list folder contents" | "list folder contents"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

creator owner:
 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data
[...]
```

4.4.1.29 %SystemRoot%\system32\at.exe - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

everyone:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

power users:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

system:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write  [...]
```

4.4.1.30 %SystemRoot%\system32\Ntbackup.exe - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

everyone:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

power users:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

system:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write  [...]
```

4.4.1.31 %SystemRoot%\system32\rcp.exe - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

everyone:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

power users:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

system:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write  [...]
```

4.4.1.32 %SystemRoot%\regedit.exe - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

power users:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

system:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions" |
"take ownership" | "trav [...]
```

4.4.1.33 %SystemRoot%\system32\regedt32.exe - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

everyone:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

power users:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

system:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write  [...]
```

4.4.1.34 %SystemRoot%\system32\rexec.exe - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

everyone:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

power users:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

system:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write  [...]
```

4.4.1.35 %SystemRoot%\system32\rsh.exe - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

everyone:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

power users:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

system:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write  [...]
```

4.4.1.36 %SystemRoot%\system32\secedit.exe - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

everyone:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

power users:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "list folder / read data" | "read attributes" | "read
extended attributes" | "read permissions" | "traverse folder /
execute file"

system:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write  [...]
```

4.4.1.38 %SystemRoot%\config - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder, subfolders and files"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

creator owner:
 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

power users:
 + Apply To: "this folder, subfolders and files"
 |- Inheritance: "inherited"
 |- Allow: "create files  [...]
```

4.4.1.40 %SystemRoot%\system32\DTCLog - Administrators: Full; System: Full; Users: Read and Execute, List

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subfolders and files only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "list folder contents" | "list folder contents"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder, subfolders and files"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

creator owner:
 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

power users:
 + Apply To: "this folder, subfolders and files"
 |- Inheritance: "inherited"
 |- Allow: "create files  [...]
```

4.4.1.43 %SystemRoot%\system32\NTMSData - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

system:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"
```

4.4.1.45 %SystemRoot%\system32\Setup - Admininstrators: Full; System: Full; Users: Read and Execute, List

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "list folder contents" | "list folder contents"

Hosts

192.168.1.205

```
everyone:
 + Apply To: "this folder, subfolders and files"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"
```

4.4.1.46 %SystemRoot%\system32\spool\printers - Administrators: Full; System: Full; Creater Owner: Full; Users: Traverse Folder/Execute file, Read, Read Extended Attributes, Create folders, Append Data

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subfolders and files only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "traverse folder / execute file" | "read attributes" | "read extended attributes" | "create folders / append data"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder, subfolders and files"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

creator owner:
 + Apply To: "this folder, subfolders and files"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

power users:
 + Apply To: "this folder and subfolders"
 |- Inheritance: "not inherited"
 |- Allow: " [...]
```

4.4.1.48 %SystemRoot%\Temp - Administrators: Full; System: Full; Creater Owner: Full; Users: Traverse Folders/Execute Files, Create Files/Write Data, Create Folders/Append Data

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subfolders and files only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not used"
|- Allow: "traverse folder / execute file" | "create files / write data" | "create folders / append data"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this folder only"
 |- Inheritance: "not inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data"
| "create folders / append data" | "delete" | "delete subfolder
and files" | "full control" | "list folder / read data" | "read
attributes" | "read extended attributes" | "read permissions"
| "take ownership" | "traverse folder / execute file" | "write
attributes" | "write extended attributes"

creator owner:
 + Apply To: "subfolders and files only"
 |- Inheritance: "inherited"
 |- Allow: "change permissions" | "create files / write data
[...]
```

4.4.2.1 HKLM\Software\Classes - Administrators: Full; System: Full; Creater Owner: Full; Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subkeys only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "read"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

creator owner:
 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

everyone:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate subkeys" | "notify" | "query value" | "read
control"

 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "enumerate subkeys" | "notify" | "qu [...]
```

4.4.2.2 HKLM\Software - Administrators: Full; System: Full; Creater Owner: Full; Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subkeys only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "read"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

creator owner:
 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

power users:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "create subkey" | "delete" | "enumerate subkeys" |
"notify" | "query value" | "read control" | "set value"

 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
  [...]
```

4.4.2.3 HKLM\Software\Microsoft\NetDDE - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

creator owner:
 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

system:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

 + [...]
```

4.4.2.4 HKLM\Software\Microsoft\OS/2 Subsystem for NT - Administrators: Full System: FUll; Creater Owner: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subkeys only"
|- Inheritance: "not used"
|- Allow: "full control" | "query value" | "set value" | "create subkey" | "enumerate subkeys" | "notify" | "create link" | "delete" | "write dac" | "write owner" | "read control"
system:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this key and subkeys"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

everyone:
 + Apply To: "this key and subkeys"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate subkeys" | "notify" | "query value" | "read
control"
```

4.4.2.5 HKLM\Software\Microsoft\Windows NT\CurrentVersion\AsrCommands - Administrators: Full; System: Full; Creater Owner: Full; Users: Read; Backup Operators (this key and subkeys): Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
backup operators:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "query value" | "set value" | "create subkey" | "enumerate subkeys" | "notify" | "delete" | "read"
creator owner:
+ Apply To: "subkeys only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "read"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

backup operators:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "create subkey" | "delete" | "enumerate subkeys" |
"notify" | "query value" | "read control" | "set value"

 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create subkey" | "delete" | "enumerate subkeys" |
"notify" | "query value" | "read control" | "set value"

creator owner:
 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "en [...]
```

4.4.2.8 HKLM\Software\Microsoft\Windows\CurrentVersion\Installer - Administrators: Full; System: Full; Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "read"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this key and subkeys"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

everyone:
 + Apply To: "this key and subkeys"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate subkeys" | "notify" | "query value" | "read
control"

system:
 + Apply To: "this key and subkeys"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"
```

4.4.2.10 HKLM\System - Administrators: Full; System: Full; Creater Owner: Full; Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subkeys only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "read"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

creator owner:
 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

power users:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate subkeys" | "notify" | "query value" | "read
control"

 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "enumerate subkeys" | "notify" |  [...]
```

4.4.2.12 HKLM\System\ControlSet001 - Administrators: Full; System: Full; Creater Owner: Full; Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subkeys only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "read"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this key and subkeys"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

creator owner:
 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

power users:
 + Apply To: "this key and subkeys"
 |- Inheritance: "inherited"
 |- Allow: "enumerate subkeys" | "notify" | "query value" | "read
control"

system:
 + Apply To: "this key and subkeys"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

users:
 + Apply To: "this key and subkeys"
 |- Inheritance: "inherited"
 |- A [...]
```

4.4.2.13 HKLM\System\ControlSet002 - Administrators: Full; System: Full; Creater Owner: Full; Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subkeys only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "read"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this key and subkeys"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

creator owner:
 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

power users:
 + Apply To: "this key and subkeys"
 |- Inheritance: "inherited"
 |- Allow: "enumerate subkeys" | "notify" | "query value" | "read
control"

system:
 + Apply To: "this key and subkeys"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

users:
 + Apply To: "this key and subkeys"
 |- Inheritance: "inherited"
 |- A [...]
```

4.4.2.14 HKLM\System\CurrentControlSet\Control\SecurePipeServers\WinReg - Administrators: Full; System: Full; Backup Operators: Query Value, Enumerate Subkeys, Notify, Read Permissions

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 50

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
backup operators:
+ Apply To: "this key only"
|- Inheritance: "not used"
|- Allow: "read"
system:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

backup operators:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate subkeys" | "notify" | "query value" | "read
control"
```

4.4.2.15 HKLM\System\CurrentControlSet\Control\WMI\Security - Administrators: Full; System: Full; Creater Owner (this key and subkeys): Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 50

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this key only"
|- Inheritance: "not used"
+ Apply To: "subkeys only"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subkeys only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "enumerate subkeys" | "notify" | "query value" | "read
control"

creator owner:
 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

system:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "del [...]
```

4.4.2.17 HKLM\System\CurrentControlSet\Hardware Profiles - Administrators: Full; System: Full; Creater Owner: Full; Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 50

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subkeys only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "read"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this key and subkeys"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

creator owner:
 + Apply To: "this key and subkeys"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

power users:
 + Apply To: "this key and subkeys"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate subkeys" | "notify" | "query value" | "read
control"

system:
 + Apply To: "this key and subkeys"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

users:
 + Apply To: "this key and subkeys"
 |- Inherit [...]
```

4.4.2.20 HKU\.Default - Administrators: Full; System: Full; Creater Owner: Full; Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 50

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
creator owner:
+ Apply To: "subkeys only"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
users:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "read"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

creator owner:
 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

power users:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "enumerate subkeys" | "notify" | "query value" | "read
control"

 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "enumerate subkeys" | "notify" |  [...]
```

4.4.2.21 HKU\.Default\Software\Microsoft\NetDDE

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 50

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

administrators:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"
system:
+ Apply To: "this key and subkeys"
|- Inheritance: "not used"
|- Allow: "full control"

Hosts

192.168.1.205

```
administrators:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

creator owner:
 + Apply To: "subkeys only"
 |- Inheritance: "inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

system:
 + Apply To: "this key only"
 |- Inheritance: "not inherited"
 |- Allow: "create link" | "create subkey" | "delete" | "enumerate
subkeys" | "full control" | "notify" | "query value" | "read
control" | "set value" | "write dac" | "write owner"

 + [...]
```

4.4.3.1 %SystemDrive% - Everyone: Failures (this folder, propagate inheritable permissions to all subfolders)

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 50

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

everyone:
+ Apply To: "this folder, subfolders and files"
|- Inheritance: "not inherited"
|- Deny: "full control"

Hosts

192.168.1.205

4.4.3.2 HKLM\Software - Everyone: Failures (this key, propagate inheritable permissions to all subfolders)

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 50

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

everyone:
+ Apply To: "this key and subkeys"
|- Inheritance: "not inherited"
|- Deny: "full control"

Hosts

192.168.1.205

4.4.3.3 HKLM\System - Everyone: Failures (this key, propagate inheritable permissions to all subfolders)

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 50

Audit File

CIS_W2KSrvr_L2_v2.audit

Policy Value

everyone:
+ Apply To: "this key and subkeys"
|- Inheritance: "not inherited"
|- Deny: "full control"

Hosts

192.168.1.205

Compliance 'SKIPPED'

Compliance 'PASSED'

2.1.2 Maximum Password Age: no more than 90 days old

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 21

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

2.2.2.2 Maximum Password Age: 90 days

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 23

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

2.2.2.6 Store Passwords using Reversible Encryption: Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 24

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

2.2.3.1 Account Lockout Duration: 15 minutes

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 24

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

2.2.3.3 Reset Account Lockout After: 15 Minutes

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 24

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

3.2.1.3 Allowed to Eject Removable NTFS Media: Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 26

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

3.2.1.4 Amount of Idle Time Required Before Disconnecting Session: 30 Minutes

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 26

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

3.2.1.7 Automatically Log Off Users When Logon Time Expires: Enabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 26

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

3.2.1.11 Digitally Sign Client Communication (When Possible): Enabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 27

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

3.2.1.20 Prevent System Maintenance of Computer Account Password: Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 29

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

3.2.1.22 Prompt User to Change Password Before Expiration: 14 days

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 30

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

3.2.1.23 Recovery Console: Allow Automatic Administrative Logon: Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 30

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

3.2.1.24 Recover Console: Allow Floppy Copy and Access to All Drives and All Folders: Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 30

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

3.2.1.30 Secure Channel: Digitally Encrypt Secure Channel Data (When Possible): Enabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 32

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

3.2.1.31 Secure Channel: Digitally Sign Secure Channel Data (When Possible): Enabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 32

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

3.2.1.33 Send Unencrypted Password to Connect to Third-Part SMB Servers: Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 32

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

3.2.1.36 Strengthen Default Permissions of Global System Objects (i.e. Symbolic Links): Enabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 33

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

3.2.1.37 Unsigned Driver Installation Behavior: Warn, but allow installation (minimum) or Do Not Allow Installation

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 33

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

3.2.2.4 Disable Automatic Logon: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon \AutoAdminLogon: 0

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 34

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

3.2.2.21 Enable IPSec to protect Kerberos RSVP Traffic: HKLM\System\CurrentControlSet\Services\IPSEC\NoDefaultExempt: 1

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 38

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.1 Available Services (SNMP): Permissions on SNMP: Administrators: Full Control; System: Read, Start, Stop, and Pause

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 41

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.1 Available Services (SNMPTRAP): Permissions on SNMP Trap: Administrators: Full Control; Sytem: Read, Start, Stop, and Pause

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 41

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.1.11 Routing and Remote Access (RemoteAccess): Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 40

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.1.13 Simple Network Management Protocol (SNMP) Service: Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 40

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.1.14 Simple Network Management Protocol (SNMP) Trap (SNMPTRAP): Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 41

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.2.2 Act as part of the operating system (SeTcbPrivilege): None

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 42

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.2.7 Create a pagefile (SeCreatePagefilePrivilege): Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 42

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.2.8 Create a token object (SeCreateTokenPrivilege): None

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 42

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.2.9 Create permanent shared objects (SeCreatePermanentPrivilege): None

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 42

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.2.16 Force shutdown from a remote system (SeRemoteShutdownPrivilege): Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 43

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.2.17 Generate security audits (SeAuditPrivilege): None

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 43

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.2.18 Increase quotas: Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 43

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.2.19 Increase schedulign priority (SeIncreaseBasePriorityPrivilege): Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 43

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.2.20 Load and unload device drivers (SeLoadDriverPrivilege): Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 43

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.2.21 Lock pages in memory (SeLockMemoryPrivilege): None

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 44

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.2.25 Manage auditing and security log (SeSecurityPrivilege): Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 44

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.2.26 Modify firmware environment values (SeSystemEnvironmentPrivilege): Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 44

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.2.28 Profile system performance (SeSystemProfilePrivilege): Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 44

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.2.30 Replace a process level token (SeAssignPrimaryTokenPrivilege): None

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 44

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.2.34 Take ownership of files or other objects (SeTakeOwnershipPrivilege): Administrators

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 45

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.1.7 %SystemDrive%\ntbootdd.sys - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.1.13 %SystemDrive%\Documents and Settings\All Users\Documents\DrWatson - Administrators: Full; System: Full; Creater Owner: Full; Users (This folder, subfolders and files): Traverse Folder/ Execute File, List Folder/Read Data, Read Attributes, Read Extended Attributes, Read Permissions; Users (Subfolders and files only): Traverse Folder/Execute Files, Create Files/Write Data, Create Folder/Append Data

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.1.16 %SystemDrive%\Temp - Administrators: Full; System: Full; Creater Owner: Full; Users: Traverse Folders/Execute Files, Create Files/Write Data, Create Folders/Append Data

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.1.18 %SystemDrive%\Program Files\Resource Kit - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.1.20 %SystemRoot%\$NtServicePackUninstall$ - Administrators: Full; System: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.1.37 %SystemRoot%\system32\appmgmt - Administrators: Full; System: Full; Users: Read and Execute, List

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.1.39 %SystemRoot%\system32\dllcache - Adminstrators: Full; System: Full; Creater Owner: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.1.41 %SystemRoot%\system32\GroupPolicy - Administrators: Full; System: Full; Authenticated Users: Read and Execute, List

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.1.42 %SystemRoot%\system32\ias - Administrators: Full; System: Full; Creater Owner: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.1.44 %SystemRoot%\system32\reinstallbackups - Administrators: Full; System: Full; Creater Owner: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.2.6 HKLM\Software\Microsoft\Windows NT\CurrentVersion\Perflib - Administrators: Full; System: Full; Creator ... (see CIS Doc)

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.2.7 HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy - Administrators: Full; System: Full; Authenticated Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.2.9 HKLM\Software\Microsoft\Windows\CurrentVersion\Policies - Administrators: Full; System: Full; Authenticated Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.2.13 HKLM\System\ControlSet003 - Administrators Full; System: Full; Creator Owner: Full; Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.2.13 HKLM\System\ControlSet004 - Administrators Full; System: Full; Creator Owner: Full; Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.2.13 HKLM\System\ControlSet005 - Administrators Full; System: Full; Creator Owner: Full; Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.2.13 HKLM\System\ControlSet006 - Administrators Full; System: Full; Creator Owner: Full; Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.2.13 HKLM\System\ControlSet007 - Administrators Full; System: Full; Creator Owner: Full; Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.2.13 HKLM\System\ControlSet008 - Administrators Full; System: Full; Creator Owner: Full; Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.2.13 HKLM\System\ControlSet009 - Administrators Full; System: Full; Creator Owner: Full; Users: Read

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

Compliance 'INFO', 'WARNING', 'ERROR'

2.2.4.1.2 Restrict Guest Access to Logs: Enabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 25

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_QUERY_VALUE: an error happened while querying the value` `Windows error code: ERROR_FILE_NOT_FOUND`

2.2.4.2.2 Restrict Guest Access to Logs (Security): Enabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 25

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_QUERY_VALUE: an error happened while querying the value` `Windows error code: ERROR_FILE_NOT_FOUND`

2.2.4.3.2 Restrict Guest Access to Logs (System): Enabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 25

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_QUERY_VALUE: an error happened while querying the value` `Windows error code: ERROR_FILE_NOT_FOUND`

3.2.1.14 Disable CTRL+ALT+Delete Requirement for Logon: Disabled

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 28

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_QUERY_VALUE: an error happened while querying the value` `Windows error code: ERROR_FILE_NOT_FOUND`

3.2.2.3 Disable autoplay from any disk type, regardless of application: HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun: 255

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 34

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_OPEN_KEY: an error happened while opening the key` `Windows error code: ERROR_FILE_NOT_FOUND`

3.2.2.3.1 Disable autoplay for current user: HKCU\Sofware\Microsoft\Windows\CurrentVersion \Policies\Explorer\NoDriveTypeAutoRun: 255. Cannot determine this value remotely, if using Security Center please check value and recast result to passed or failed

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

3.2.2.5 Mask any typed passwords with asterisks: HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Network\HideSharePwds: 1

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 35

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_OPEN_KEY: an error happened while opening the key` `Windows error code: ERROR_FILE_NOT_FOUND`

3.2.2.6 Disable Dial-in access to the server: HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Network\NoDialIn: 1

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 35

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_OPEN_KEY: an error happened while opening the key` `Windows error code: ERROR_FILE_NOT_FOUND`

3.2.2.9 Remove administrative shares on servers: HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer: 0

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 35

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_QUERY_VALUE: an error happened while querying the value` `Windows error code: ERROR_FILE_NOT_FOUND`

3.2.2.10 Protect against Computer Browsing Spoofing Attacks: HKLM\System\CurrentControlSet\Services\MrxSmb\Parameters\RefuseReset: 1

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 35

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_QUERY_VALUE: an error happened while querying the value` `Windows error code: ERROR_FILE_NOT_FOUND`

3.2.2.11 Protect against source-routing spoofing: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting: 2

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 36

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_QUERY_VALUE: an error happened while querying the value` `Windows error code: ERROR_FILE_NOT_FOUND`

3.2.2.12 Protect the Default Gateway netowrk setting: HKLM\System\CurrentControlSet\Services \Tcpip\Parameters\EnableDeadGWDetect: 0

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 36

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_QUERY_VALUE: an error happened while querying the value` `Windows error code: ERROR_FILE_NOT_FOUND`

3.2.2.14 Help protect against packet fragmentation: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery: 0

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 36

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_QUERY_VALUE: an error happened while querying the value` `Windows error code: ERROR_FILE_NOT_FOUND`

3.2.2.15 Manage keep-alive times: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime: 300000

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 36

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_QUERY_VALUE: an error happened while querying the value` `Windows error code: ERROR_FILE_NOT_FOUND`

3.2.2.16 Protect Against Malicious Name-Release Attacks: HKLM\System\CurrentControlSet\Services\NetBt\Parameters\NoNameReleaseOnDemand: 1

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 37

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_QUERY_VALUE: an error happened while querying the value` `Windows error code: ERROR_FILE_NOT_FOUND`

3.2.2.17 Ensure Router Discover is Disabled: HKLM\System\CurrentControlSet\Services\Tcpip \Parameters\SynAttackProtect: 0

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 37

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_QUERY_VALUE: an error happened while querying the value` `Windows error code: ERROR_FILE_NOT_FOUND`

3.2.2.18 Protect against SYN Flood attacks: HKLM\System\CurrentControlSet\Services\Tcpip \Parameters\SynAttackProtect: 2

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 37

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_QUERY_VALUE: an error happened while querying the value` `Windows error code: ERROR_FILE_NOT_FOUND`

3.2.2.19 SYN attack protection - Manage TCP Maximum half-open sockets: HKLM\System \CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen: 100 or 500

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 37

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_QUERY_VALUE: an error happened while querying the value` `Windows error code: ERROR_FILE_NOT_FOUND`

3.2.2.20 SYN Attack protection - Manage TCP Maximum half-open retired sockets: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenRetired: 80 or 400

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 37

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_QUERY_VALUE: an error happened while querying the value` `Windows error code: ERROR_FILE_NOT_FOUND`

4.4.1.15 %SystemDrive%\System Volume Information - Do not allow permissions this folder to be replaced. Cannot determine this value remotely, if using Security Center please check value and recast result to passed or failed

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 47

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.1.24 %SystemRoot%\Offline Web Pages - Do not allow permissions on this key to be replaced - Do not allow permissions this folder to be replaced. Cannot determine this value remotely, if using Security Center please check value and recast result to passed or failed

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 48

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.1.47 %SystemRoot%\Tasks - Do not allow permissions on this key to be replaced. Cannot determine this value remotely, if using Security Center please check value and recast result to passed or failed

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.2.11 HKLM\System\Clone - Allow inheritable permissions to propogate to this object. Cannot determine this value remotely, if using Security Center please check value and recast result to passed or failed

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 49

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.2.16 HKLM\System\CurrentControlSet\Enum - Administrators: Read; System: Full; Authenticated Users: Read (Do not allow permissions on this key to be replaced). Cannot determine this value remotely, if using Security Center please check value and recast result to passed or failed

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 50

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205

4.4.2.18 HKLM\System\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers - Administrators Full; System: Full; Creator Owner: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 50

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_OPEN_KEY: an error happened while opening the key`

4.4.2.19 HKLM\System\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities - Administrators Full; System: Full; Creator Owner: Full

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 50

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205	`REG_ERROR_OPEN_KEY: an error happened while opening the key`

4.4.2.22 HKU\.Default\Software\Microsoft\Protected Storage System Provider - No entries. Cannot determine this value remotely, if using Security Center please check value and recast result to passed or failed

Info

ref: https://benchmarks.cisecurity.org/tools2/windows/CIS_Win2k_Srv_Benchmark_v2.2.1.pdf pg. 50

Audit File

CIS_W2KSrvr_L2_v2.audit

Hosts

192.168.1.205