

|    | A                                                                                     | B                                           | C                                           | D                                                  | E                                                                                            | F |
|----|---------------------------------------------------------------------------------------|---------------------------------------------|---------------------------------------------|----------------------------------------------------|----------------------------------------------------------------------------------------------|---|
| 1  | <b>Workstations Policy Setting Description</b>                                        | <b>CIS Recommendations</b>                  | <b>Current Domain Policy</b>                | <b>Planned Domain Policy - BNL</b>                 |                                                                                              |   |
| 2  |                                                                                       |                                             |                                             |                                                    |                                                                                              |   |
| 3  | <b>1. Service Packs &amp; Security Updates (Domain Level)</b>                         |                                             |                                             |                                                    |                                                                                              |   |
| 4  |                                                                                       |                                             |                                             |                                                    |                                                                                              |   |
| 5  | <b>1.1 - Patches</b>                                                                  |                                             |                                             |                                                    |                                                                                              |   |
| 6  | XP                                                                                    | SP2                                         | SP2                                         | SP2                                                |                                                                                              |   |
| 7  | <b>1.2 - Updates</b>                                                                  |                                             |                                             |                                                    |                                                                                              |   |
| 8  | Security Updates                                                                      | All Critical and Important Security Updates | All Critical and Important Security Updates | All Critical and Important Security Updates (WSUS) | Would be on regular schedule based (in tune with maintenance for example)                    |   |
| 9  |                                                                                       |                                             |                                             |                                                    |                                                                                              |   |
| 10 | <b>2. Auditing and Account Policies (Apply at Domain Level)</b>                       |                                             |                                             |                                                    |                                                                                              |   |
| 11 |                                                                                       |                                             |                                             |                                                    |                                                                                              |   |
| 12 | <b>2.1 - Major Auditing and Account Policies Requirements</b>                         |                                             |                                             |                                                    |                                                                                              |   |
| 13 | 2.1.1 - Minimum password length                                                       | 8 characters                                | 8 characters                                | 8 characters                                       |                                                                                              |   |
| 14 | 2.1.2 - Maximum password age                                                          | 90 days                                     | 180 days                                    | 180                                                |                                                                                              |   |
| 15 |                                                                                       |                                             |                                             |                                                    |                                                                                              |   |
| 16 | <b>2.2 - Minor Auditing and Account Policies Requirements</b>                         |                                             |                                             |                                                    |                                                                                              |   |
| 17 |                                                                                       |                                             |                                             |                                                    |                                                                                              |   |
| 18 | <b>2.2.1 - Audit Policy</b>                                                           |                                             |                                             |                                                    |                                                                                              |   |
| 19 | 2.2.1.1 - Audit account logon events                                                  | Success, Failure                            | Success, Failure                            | Success, Failure                                   |                                                                                              |   |
| 20 | 2.2.1.2 - Audit account management                                                    | Success, Failure                            | Success, Failure                            | Success, Failure                                   |                                                                                              |   |
| 21 | 2.2.1.3 - Audit directory service access                                              | Not Defined                                 | Success, Failure                            | Not Defined                                        |                                                                                              |   |
| 22 | 2.2.1.4 - Audit logon events                                                          | Success, Failure                            | Success, Failure                            | Success, Failure                                   |                                                                                              |   |
| 23 | 2.2.1.5 - Audit object access                                                         | Failure                                     | Failure                                     | Failure                                            |                                                                                              |   |
| 24 | 2.2.1.6 - Audit policy change                                                         | Success                                     | Success, Failure                            | Success, Failure                                   |                                                                                              |   |
| 25 | 2.2.1.7 - Audit privilege use                                                         | Failure                                     | Success, Failure                            | Failure                                            |                                                                                              |   |
| 26 | 2.2.1.8 - Audit process tracking                                                      | Not Defined                                 | Not Defined                                 | Not Defined                                        |                                                                                              |   |
| 27 | 2.2.1.9 - Audit system events                                                         | Success                                     | Success, Failure                            | Success, Failure                                   |                                                                                              |   |
| 28 |                                                                                       |                                             |                                             |                                                    |                                                                                              |   |
| 29 | <b>2.2.2 - Account Policy</b>                                                         |                                             |                                             |                                                    |                                                                                              |   |
| 30 | 2.2.2.1 - Minimum Password Age                                                        | 1 day                                       | 0 day                                       | 1 day                                              |                                                                                              |   |
| 31 | 2.2.2.2 - Maximum Password Age                                                        | 90 days                                     | 180 days                                    | 180                                                | 6 months may be short for operational needs, propose 10 months=300 days (for possible merged |   |
| 32 | 2.2.2.3 - Minimum Password Length                                                     | 8 characters                                | 8 characters                                | 8 characters                                       |                                                                                              |   |
| 33 | 2.2.2.4 - Password Complexity                                                         | Enabled                                     | Enabled                                     | Enabled *** enable PW.dll w/dictionary             |                                                                                              |   |
| 34 | 2.2.2.5 - Password History                                                            | 24 Passwords Remembered                     | 5 Passwords Remembered                      | 24 Passwords Remembered                            |                                                                                              |   |
| 35 | 2.2.2.6 - Store Passwords using Reversible Encryption                                 | Disabled                                    | Disabled                                    | Disabled                                           |                                                                                              |   |
| 36 |                                                                                       |                                             |                                             |                                                    |                                                                                              |   |
| 37 | <b>2.2.3 - Account Lockout Policy</b>                                                 |                                             |                                             |                                                    |                                                                                              |   |
| 38 | 2.2.3.1 - Account Lockout Duration                                                    | 15 minutes                                  | 0 minutes                                   | 0 minutes                                          | TBC - no good for any categories                                                             |   |
| 39 | 2.2.3.2 - Account Lockout Threshold                                                   | 50 attempts                                 | 5 attempts                                  | 5 attempts                                         | TBC - no good, too low comparing to CIS recommendations                                      |   |
| 40 | 2.2.3.3 - Reset Account Lockout After                                                 | 15 minutes                                  | 30 minutes                                  | 30 minutes                                         | TBC - no good                                                                                |   |
| 41 |                                                                                       |                                             |                                             |                                                    |                                                                                              |   |
| 42 | <b>2.2.4 - Event Log Settings (w/SNARE)</b>                                           |                                             |                                             |                                                    |                                                                                              |   |
| 43 | <b>(Application, Security and System Logs)</b>                                        |                                             |                                             |                                                    |                                                                                              |   |
| 44 | 2.2.4.1 - Application Log                                                             |                                             |                                             |                                                    |                                                                                              |   |
| 45 | 2.2.4.1.1 - Maximum Event Log Size                                                    | 16 MB                                       | 2048 kb                                     | 25 MB                                              | ?? Laptop / does this imply it rotate ? Delete ? What?                                       |   |
| 46 | 2.2.4.1.2 - Restrict Guest Access                                                     | Enabled                                     | Not Defined                                 | Enabled                                            |                                                                                              |   |
| 47 | 2.2.4.1.3 - Log Retention Method                                                      | As Needed                                   | As Needed                                   | As Needed                                          |                                                                                              |   |
| 48 | 2.2.4.1.4 - Log Retention                                                             | Not Defined                                 | Not Defined                                 | Not Defined                                        |                                                                                              |   |
| 49 |                                                                                       |                                             |                                             |                                                    |                                                                                              |   |
| 50 | 2.2.4.2 - Security Log                                                                |                                             |                                             |                                                    |                                                                                              |   |
| 51 | 2.2.4.2.1 - Maximum Event Log Size                                                    | 80 MB                                       | 2048 kb                                     | 80 MB                                              | ?? Laptop / does this imply it rotate ? Delete ? What?                                       |   |
| 52 | 2.2.4.2.2 - Restrict Guest Access                                                     | Enabled                                     | Not Defined                                 | Enabled                                            |                                                                                              |   |
| 53 | 2.2.4.2.3 - Log Retention Method                                                      | As Needed                                   | As Needed                                   | As Needed                                          |                                                                                              |   |
| 54 | 2.2.4.2.4 - Log Retention                                                             | Not Defined                                 | Not Defined                                 | Not Defined                                        |                                                                                              |   |
| 55 |                                                                                       |                                             |                                             |                                                    |                                                                                              |   |
| 56 | 2.2.4.3 - System Log                                                                  |                                             |                                             |                                                    |                                                                                              |   |
| 57 | 2.2.4.3.1 - Maximum Event Log Size                                                    | 16 MB                                       | 2048 kb                                     | 25 MB                                              | ?? Laptop / does this imply it rotate ? Delete ? What?                                       |   |
| 58 | 2.2.4.3.2 - Restrict Guest Access                                                     | Enabled                                     | Not Defined                                 | Enabled                                            |                                                                                              |   |
| 59 | 2.2.4.3.3 - Log Retention Method                                                      | As Needed                                   | As Needed                                   | As Needed                                          |                                                                                              |   |
| 60 | 2.2.4.3.4 - Log Retention                                                             | Not Defined                                 | Not Defined                                 | Not Defined                                        |                                                                                              |   |
| 61 |                                                                                       |                                             |                                             |                                                    |                                                                                              |   |
| 62 | <b>3. Security Settings</b>                                                           |                                             |                                             |                                                    |                                                                                              |   |
| 63 |                                                                                       |                                             |                                             |                                                    |                                                                                              |   |
| 64 | <b>3.1 Major Security Settings</b>                                                    |                                             |                                             |                                                    |                                                                                              |   |
| 65 | 3.1.1 - Network Access: Allow Anonymous SID/Name Translation:                         | Disabled                                    | Not Defined                                 | Disabled                                           |                                                                                              |   |
| 66 | 3.1.2 - Network Access: Do not allow Anonymous Enumeration of SAM Accounts            | Enabled                                     | Not Defined                                 | Enabled                                            |                                                                                              |   |
| 67 | 3.1.3 - Network Access: Do not allow Anonymous Enumeration of SAM Accounts and Shares | Enabled                                     | Not Defined                                 | Enabled                                            |                                                                                              |   |
| 68 | 3.1.4 - Data Execution Protection                                                     | Enabled                                     | Not Defined                                 | Enabled                                            |                                                                                              |   |
| 69 |                                                                                       |                                             |                                             |                                                    |                                                                                              |   |
| 70 | <b>3.2 Minor Security Settings</b>                                                    |                                             |                                             |                                                    |                                                                                              |   |
| 71 | <b>3.2.1 - Security Options</b>                                                       |                                             |                                             |                                                    |                                                                                              |   |
| 72 | 3.2.1.1 - Accounts: Administrator Account Status                                      | Not Defined                                 | Not Defined                                 | Enabled                                            |                                                                                              |   |
| 73 | 3.2.1.2 - Accounts: Guest Account Status                                              | Disabled                                    | Not Defined                                 | Disabled                                           |                                                                                              |   |
| 74 | 3.2.1.3 - Accounts: Limit local account use of blank passwords to console logon only  | Enabled                                     | Not Defined                                 | Enabled                                            |                                                                                              |   |
| 75 | 3.2.1.4 - Accounts: Rename Administrator Account                                      | User Defined Value                          | Not Defined                                 | User Defined Value                                 | staradmin - may not be good for developer nodes                                              |   |

|     | A                                                                                                                                | B                                                                                                                             | C           | D                                                                                                                             | E                                                                                                  | F |
|-----|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|---|
| 76  | 3.2.1.5 - Accounts: Rename Guest Account                                                                                         | User Defined Value                                                                                                            | Not Defined | User Defined Value                                                                                                            | disabled on STAR domain                                                                            |   |
| 77  | 3.2.1.6 - Audit: Audit the access of global system objects                                                                       | Not Defined                                                                                                                   | Not Defined | Not Defined                                                                                                                   |                                                                                                    |   |
| 78  | 3.2.1.7 - Audit: Audit the use of backup and restore privilege                                                                   | Not Defined                                                                                                                   | Not Defined | Not Defined                                                                                                                   |                                                                                                    |   |
| 79  | 3.2.1.8 - Audit: Shut Down system immediately if unable to log security alerts                                                   | Not Defined                                                                                                                   | Not Defined | Not Defined                                                                                                                   |                                                                                                    |   |
| 80  | 3.2.1.9 - DCOM: Machine Access Restrictions (SP2 only)                                                                           | Not Defined                                                                                                                   | Not Defined | Not Defined                                                                                                                   |                                                                                                    |   |
| 81  | 3.2.1.10 - DCOM: Machine Launch Restrictions (SP2 only)                                                                          | Not Defined                                                                                                                   | Not Defined | Not Defined                                                                                                                   |                                                                                                    |   |
| 82  | 3.2.1.11 - Devices: Allow undock without having to log on                                                                        | Not Defined                                                                                                                   | Not Defined | Not Defined                                                                                                                   |                                                                                                    |   |
| 83  | 3.2.1.12 - Devices: Allowed to format and eject removable media                                                                  | Administrators, Interactive Users                                                                                             | Not Defined | Administrators, Interactive Users                                                                                             | user here means non-administrators?                                                                |   |
| 84  | 3.2.1.13 - Devices: Prevent users from installing printer drivers                                                                | Enabled                                                                                                                       | Not Defined | Enabled                                                                                                                       |                                                                                                    |   |
| 85  | 3.2.1.14 - Devices: Restrict CD-ROM Access to Locally Logged-On User Only                                                        | Not Defined                                                                                                                   | Not Defined | Enabled                                                                                                                       |                                                                                                    |   |
| 86  | 3.2.1.15 - Devices: Restrict Floppy Access to Locally Logged-On User Only                                                        | Not Defined                                                                                                                   | Not Defined | Enabled                                                                                                                       |                                                                                                    |   |
| 87  | 3.2.1.16 - Devices: Unsigned Driver Installation Behavior Warn, but allow...                                                     | Warn, but allow...                                                                                                            | Not Defined | Warn, but allow...                                                                                                            |                                                                                                    |   |
| 88  | 3.2.1.17 - Domain Controller: Allow Server Operators to Schedule Tasks                                                           | Not Applicable                                                                                                                | Not Defined | Not Applicable                                                                                                                |                                                                                                    |   |
| 89  | 3.2.1.18 - Domain Controller: LDAP Server Signing Requirements                                                                   | Not Applicable                                                                                                                | Not Defined | Not Applicable                                                                                                                |                                                                                                    |   |
| 90  | 3.2.1.19 - Domain Controller: Refuse machine account password changes                                                            | Not Applicable                                                                                                                | Not Defined | Not Applicable                                                                                                                |                                                                                                    |   |
| 91  | 3.2.1.20 - Domain Member: Digitally Encrypt or Sign Secure Channel Data (Always)                                                 | Enabled                                                                                                                       | Not Defined | Enabled                                                                                                                       |                                                                                                    |   |
| 92  | 3.2.1.21 - Domain Member: Digitally Encrypt Secure Channel Data (When Possible)                                                  | Enabled                                                                                                                       | Not Defined | Enabled                                                                                                                       |                                                                                                    |   |
| 93  | 3.2.1.22 - Domain Member: Digitally Sign Secure Channel Data (When Possible)                                                     | Enabled                                                                                                                       | Not Defined | Enabled                                                                                                                       |                                                                                                    |   |
| 94  | 3.2.1.23 - Domain Member: Disable Machine Account Password Changes                                                               | Disabled                                                                                                                      | Not Defined | Disabled                                                                                                                      |                                                                                                    |   |
| 95  | 3.2.1.24 - Domain Member: Maximum Machine Account Password Age                                                                   | 30 Days                                                                                                                       | Not Defined | 30 Days                                                                                                                       | This seems awfully small, even for a domain account ... questionable for laptop only               |   |
| 96  | 3.2.1.25 - Domain Member: Require Strong (Windows 2000 or later) Session Key                                                     | Enabled                                                                                                                       | Not Defined | Enabled                                                                                                                       |                                                                                                    |   |
| 97  | 3.2.1.26 - Interactive Logon: Do Not Display Last User Name Enabled                                                              | Enabled                                                                                                                       | Not Defined | Enabled                                                                                                                       |                                                                                                    |   |
| 98  | 3.2.1.27 - Interactive Logon: Do not require CTRL+ALT+DEL                                                                        | Disabled                                                                                                                      | Not Defined | Disabled                                                                                                                      | This means HAS CTRL+ALT+DELETE (we are fine with that)                                             |   |
| 99  | 3.2.1.28 - Interactive Logon: Message Text for Users Attempting to Log On                                                        | Custom, or DoJ Approved                                                                                                       | Not Defined | Scripted Registry Entry                                                                                                       | Is this a banner issue?? YES                                                                       |   |
| 100 | 3.2.1.29 - Interactive Logon: Message Title for Users Attempting to Log On                                                       | Custom, or DoJ Approved                                                                                                       | Not Defined | Scripted Registry Entry                                                                                                       | Is this a banner issue?? YES                                                                       |   |
| 101 | 3.2.1.30 - Interactive Logon: Number of Previous Logons to Cache                                                                 | 2                                                                                                                             | Not Defined | 2                                                                                                                             |                                                                                                    |   |
| 102 | 3.2.1.31 - Interactive Logon: Prompt User to Change Password Before Expiration                                                   | 14                                                                                                                            | Not Defined | 14                                                                                                                            |                                                                                                    |   |
| 103 | 3.2.1.32 - Interactive Logon: Require Domain Controller authentication to unlock workstation                                     | Enabled                                                                                                                       | Not Defined | Enabled                                                                                                                       | ??? What does this mean / for local accounts then? - Claim is that this setting does nothing       |   |
| 104 | 3.2.1.33 - Interactive Logon: Smart Card Removal Behavior Lock Workstation                                                       | Lock Workstation                                                                                                              | Not Defined | Lock Workstation                                                                                                              | ???                                                                                                |   |
| 105 | 3.2.1.34 - Microsoft Network Client: Digitally sign communications (always)                                                      | Enabled                                                                                                                       | Not Defined | Enabled                                                                                                                       |                                                                                                    |   |
| 106 | 3.2.1.35 - Microsoft Network Client: Digitally sign communications (if server agrees)                                            | Enabled                                                                                                                       | Not Defined | Enabled                                                                                                                       |                                                                                                    |   |
| 107 | 3.2.1.36 - Microsoft Network Client: Send Unencrypted Password to Connect to Third-Party SMB Server                              | Disabled                                                                                                                      | Not Defined | Disabled                                                                                                                      |                                                                                                    |   |
| 108 | 3.2.1.37 - Microsoft Network Server: Amount of Idle Time Required Before Disconnecting Session                                   | 15 minutes                                                                                                                    | Not Defined | 15 minutes                                                                                                                    |                                                                                                    |   |
| 109 | 3.2.1.38 - Microsoft Network Server: Digitally sign communications (always)                                                      | Enabled                                                                                                                       | Not Defined | Enabled                                                                                                                       |                                                                                                    |   |
| 110 | 3.2.1.39 - Microsoft Network Server: Digitally sign communications (if client agrees)                                            | Enabled                                                                                                                       | Not Defined | Enabled                                                                                                                       |                                                                                                    |   |
| 111 | 3.2.1.40 - Microsoft Network Server: Disconnect clients when logon hours expire                                                  | Enabled                                                                                                                       | Not Defined | Enabled                                                                                                                       |                                                                                                    |   |
| 112 | 3.2.1.41 - Network Access: Do not allow storage of credentials or .NET passports for network authentication                      | Enabled                                                                                                                       | Not Defined | Enabled                                                                                                                       |                                                                                                    |   |
| 113 | 3.2.1.42 - Network Access: Let Everyone permissions apply to anonymous users                                                     | Disabled                                                                                                                      | Not Defined | Disabled                                                                                                                      | ???                                                                                                |   |
| 114 | 3.2.1.43 - Network Access: Named pipes that can be accessed anonymously                                                          | COMNAP, COMNODE, SQL\QUERY                                                                                                    | Not Defined | COMNAP, COMNODE, SQL\QUERY, SPOOLSS, LLSRPC, BROWSER                                                                          |                                                                                                    |   |
| 115 | 3.2.1.44 - Network Access: Remotely accessible registry paths                                                                    | Not Defined                                                                                                                   | Not Defined | Not Defined                                                                                                                   |                                                                                                    |   |
| 116 | 3.2.1.45 - Network Access: Shares that can be accessed anonymously                                                               | Not Defined                                                                                                                   | Not Defined | Not Defined                                                                                                                   |                                                                                                    |   |
| 117 | 3.2.1.46 - Network Access: Sharing and security model for local accounts Classic                                                 | Classic                                                                                                                       | Not Defined | Classic                                                                                                                       |                                                                                                    |   |
| 118 | 3.2.1.47 - Network Security: Do not store LAN Manager password hash value on next password change                                | Enabled                                                                                                                       | Not Defined | Enabled                                                                                                                       |                                                                                                    |   |
| 119 | 3.2.1.48 - Network Security: Force logoff when logon hours expire                                                                | Enabled                                                                                                                       | Disabled    | Enabled                                                                                                                       | I do not know what this means ... / should not have this since we do not have "work hours"         |   |
| 120 | 3.2.1.49 - Network Security: LAN Manager Authentication Level Send NTLMv2 Send NTLMv2, refuse LM Send NTLMv2, refuse LM and NTLM | Send NTLM v2 & refuse LM                                                                                                      | Not Defined | Send NTLM v2 & refuse LM                                                                                                      |                                                                                                    |   |
| 121 | 3.2.1.50 - Network Security: LDAP client signing requirements                                                                    | Negotiate Signing                                                                                                             | Not Defined | Negotiate Signing                                                                                                             |                                                                                                    |   |
| 122 | 3.2.1.51 - Network Security: Minimum session security for NTLM SSP based (including secure RPC) clients                          | Require Message Integrity<br>Require message confidentiality<br>Require NTLMv2 session security<br>Require 128-bit encryption | Not Defined | Require Message Integrity<br>Require message confidentiality<br>Require NTLMv2 session security<br>Require 128-bit encryption |                                                                                                    |   |
| 123 | 3.2.1.52 - Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers                          | Require Message Integrity<br>Require message confidentiality<br>Require NTLMv2 session security<br>Require 128-bit encryption | Not Defined | Require Message Integrity<br>Require message confidentiality<br>Require NTLMv2 session security<br>Require 128-bit encryption |                                                                                                    |   |
| 124 | 3.2.1.53 - Recovery Console: Allow Automatic Administrative Logon                                                                | Disabled                                                                                                                      | Not Defined | Disabled                                                                                                                      |                                                                                                    |   |
| 125 | 3.2.1.54 - Recovery Console: Allow Floppy Copy and Access to All Drives and All Folders                                          | Not Defined                                                                                                                   | Not Defined | Disabled                                                                                                                      | This would NOT be good as Disabled / I do not understand the reason / admin need password-         |   |
| 126 | 3.2.1.55 - Shutdown: Allow System to be Shut Down Without Having to Log On                                                       | Disabled                                                                                                                      | Not Defined | Disabled                                                                                                                      |                                                                                                    |   |
| 127 | 3.2.1.56 - Shutdown: Clear Virtual Memory Pagefile                                                                               | Not Defined                                                                                                                   | Not Defined | Enabled                                                                                                                       | ARGHHHHH!!!! Try this on my 1 GB RAM Laptop with 1.5 GB of page .... security argument under       |   |
| 128 | 3.2.1.57 - System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing                               | Not Defined                                                                                                                   | Not Defined | Not Defined                                                                                                                   |                                                                                                    |   |
| 129 | 3.2.1.58 - System objects: Default owner for objects created by members of the Administrators group                              | CREATOR OWNER                                                                                                                 | Not Defined | CREATOR OWNER                                                                                                                 | Do not understand the implication... may affect programs / should be fine (explicit ownership so n |   |
| 130 | 3.2.1.59 - System objects: Require case insensitivity for non-Windows subsystems                                                 | Enabled                                                                                                                       | Not Defined | Enabled                                                                                                                       |                                                                                                    |   |
| 131 | 3.2.1.60 - System objects: Strengthen default permissions of internal system objects                                             | Enabled                                                                                                                       | Not Defined | Enabled                                                                                                                       | Side effects??                                                                                     |   |
| 132 |                                                                                                                                  |                                                                                                                               |             |                                                                                                                               |                                                                                                    |   |
| 133 | 3.2.2 - Additional Registry Settings                                                                                             |                                                                                                                               |             |                                                                                                                               |                                                                                                    |   |

|     | A                                                                                                                                                                             | B               | C           | D                                                     | E                                                 | F |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-------------|-------------------------------------------------------|---------------------------------------------------|---|
|     | 3.2.2.1 - Suppress Dr. Watson Crash Dumps:<br>HKLM\Software\Microsoft\DrWatson\CreateCrashDump                                                                                | Not Defined     | Not Defined | (REG_DWORD) 0                                         |                                                   |   |
| 134 | 3.2.2.2 - Disable Automatic Execution of the System Debugger:<br>HKLM\Software\Microsoft\Windows NT\CurrentVersion\AEDebug\Auto                                               | Not Defined     | Not Defined | (REG_DWORD) 0                                         | Not sure this is good for developer's machine     |   |
| 135 | 3.2.2.3 - Disable autoplay from any disk type, regardless of application:<br>HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun              | (REG_DWORD) 255 | Not Defined | (REG_DWORD) 255                                       |                                                   |   |
| 136 | 3.2.2.4 - Disable autoplay for current user:<br>HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun                                           | (REG_DWORD) 255 | Not Defined | (REG_DWORD) 255                                       |                                                   |   |
| 137 | 3.2.2.5 - Disable autoplay for the default profile:<br>HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun                             | (REG_DWORD) 255 | Not Defined | (REG_DWORD) 255                                       |                                                   |   |
| 138 | 3.2.2.6 - Disable Automatic Logon: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon                                                                  | Not Defined     | Not Defined | (REG_DWORD) 0                                         |                                                   |   |
| 139 | 3.2.2.7 - Disable automatic reboots after a Blue Screen of Death:<br>HKLM\System\CurrentControlSet\Control\CrashControl\AutoReboot                                            | Not Defined     | Not Defined | (REG_DWORD) 0                                         | 0 means disable the disable feature ..            |   |
| 140 | 3.2.2.8 - Disable CD Autorun: HKLM\System\CurrentControlSet\Services\CDRom\Autorun (REG_DWORD)                                                                                | (REG_DWORD) 0   | Not Defined | (REG_DWORD) 0                                         |                                                   |   |
| 141 | 3.2.2.9 - Remove administrative shares on workstation (Professional):<br>HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks                          | Not Defined     | Not Defined | Not Defined                                           |                                                   |   |
| 142 | 3.2.2.10 - Protect against Computer Browser Spoofing Attacks:<br>HKLM\System\CurrentControlSet\Services\MrxSmb\Parameters\RefuseReset                                         | Not Defined     | Not Defined | (REG_DWORD) 1                                         |                                                   |   |
| 143 | 3.2.2.11 - Protect against source-routing spoofing:<br>HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting                                         | (REG_DWORD) 2   | Not Defined | (REG_DWORD) 2                                         |                                                   |   |
| 144 | 3.2.2.12 - Protect the Default Gateway network setting:<br>HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect                                         | Not Defined     | Not Defined | (REG_DWORD) 0                                         |                                                   |   |
| 145 | 3.2.2.13 - Ensure ICMP Routing via shortest path first:<br>HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect                                         | Not Defined     | Not Defined | (REG_DWORD) 0                                         |                                                   |   |
| 146 | 3.2.2.14 - Help protect against packet fragmentation:<br>HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery                                          | Not Defined     | Not Defined | (REG_DWORD) 0                                         | ???                                               |   |
| 147 | 3.2.2.15 - Manage Keep-alive times:<br>HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime                                                                  | Not Defined     | Not Defined | (REG_DWORD) 300000                                    |                                                   |   |
| 148 | 3.2.2.16 - Protect Against Malicious Name-Release Attacks:<br>HKLM\System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand                                   | Not Defined     | Not Defined | (REG_DWORD) 1                                         |                                                   |   |
| 149 | 3.2.2.17 - Ensure Router Discovery is Disabled:<br>HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery (REG_DWORD)                                 | Not Defined     | Not Defined | (REG_DWORD) 0                                         |                                                   |   |
| 150 | 3.2.2.18 - Protect against SYN Flood attacks:<br>HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect                                                     | Not Defined     | Not Defined | (REG_DWORD) 2                                         |                                                   |   |
| 151 | 3.2.2.19 - SYN Attack protection – Manage TCP Maximum half-open sockets:<br>HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen                            | Not Defined     | Not Defined | (REG_DWORD) 100                                       |                                                   |   |
| 152 | 3.2.2.20 - SYN Attack protection – Manage TCP Maximum half-open retired sockets:<br>HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenRetired (REG_DWORD) | Not Defined     | Not Defined | (REG_DWORD) 80                                        |                                                   |   |
| 153 | 3.2.2.21 - Enable IPsec to protect Kerberos RSVP Traffic:<br>HKLM\System\CurrentControlSet\Services\IPSEC\NoDefaultExempt                                                     | (REG_DWORD) 1   | Not Defined | (REG_DWORD) 1                                         |                                                   |   |
| 154 | 3.2.2.22 - Hide workstation from Network Browser listing:<br>HKLM\System\CurrentControlSet\Services\Lanmanserver\Parameters\Hidden                                            | Not Defined     | Not Defined | (REG_DWORD) 1                                         |                                                   |   |
| 155 | 3.2.2.23 - Enable Safe DLL Search Mode:<br>HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode                                                            | (REG_DWORD) 1   | Not Defined | (REG_DWORD) 1                                         |                                                   |   |
| 156 | 3.2.2.24 - Disable WebDAV basic authentication (SP 2 only):<br>HKLM\System\CurrentControlSet\Services\WebClient\Parameters\UseBasicAuth                                       | (REG_DWORD) 1   | Not Defined | (REG_DWORD) 1                                         |                                                   |   |
| 157 | 3.2.2.25 - Disable basic authentication over a clear channel (SP 2 only):<br>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\DisableBasicOverClearChannel     | Not Defined     | Not Defined | Not Defined                                           |                                                   |   |
| 158 | 3.2.2.26 - USB Block Storage Device Policy (SP2 only):<br>HKLM\System\CurrentControlSet\Control\StorageDevicePolicies                                                         | Not Defined     | Not Defined | Not Defined                                           |                                                   |   |
| 159 | 3.2.2.27 - DTC Access (SP2 only): HKLM\Software\Microsoft\MSDTC                                                                                                               | Not Defined     | Not Defined | Not Defined                                           |                                                   |   |
| 160 |                                                                                                                                                                               |                 |             |                                                       |                                                   |   |
| 161 |                                                                                                                                                                               |                 |             |                                                       |                                                   |   |
| 162 | <u>4. Additional Security Protection</u>                                                                                                                                      |                 |             |                                                       |                                                   |   |
| 163 |                                                                                                                                                                               |                 |             |                                                       |                                                   |   |
| 164 | <b>4.1 - Available Services</b>                                                                                                                                               |                 |             |                                                       |                                                   |   |
| 165 | 4.1.1 - Alerter                                                                                                                                                               | Disabled        | Not Defined | Disabled                                              |                                                   |   |
| 166 | 4.1.2 - Automatic Updates                                                                                                                                                     | Not Defined     | Not Defined | Automatic *add Authenticated Users - Read Permissions | Download but do not install by default during run |   |
| 167 | 4.1.3 - Background Intelligent Transfer Service                                                                                                                               | Not Defined     | Not Defined | Not Defined                                           |                                                   |   |
| 168 | 4.1.4 - Clipbook                                                                                                                                                              | Disabled        | Not Defined | Disabled                                              |                                                   |   |
| 169 | 4.1.5 - Computer Browser                                                                                                                                                      | Not Defined     | Not Defined | Disabled                                              |                                                   |   |
| 170 | 4.1.6 - Fax Service                                                                                                                                                           | Not Defined     | Not Defined | Disabled                                              |                                                   |   |
| 171 | 4.1.7 - FTP Publishing Service                                                                                                                                                | Disabled        | Not Defined | Disabled                                              |                                                   |   |
| 172 | 4.1.8 - IIS Admin Service                                                                                                                                                     | Disabled        | Not Defined | Disabled                                              |                                                   |   |
| 173 | 4.1.9 - Indexing Service                                                                                                                                                      | Not Defined     | Not Defined | Not Defined                                           |                                                   |   |

|     | A                                                                       | B                                                     | C           | D                                                     | E                                                                                               | F |
|-----|-------------------------------------------------------------------------|-------------------------------------------------------|-------------|-------------------------------------------------------|-------------------------------------------------------------------------------------------------|---|
| 174 | 4.1.10 - Messenger                                                      | Disabled                                              | Not Defined | Disabled                                              |                                                                                                 |   |
| 175 | 4.1.11 - Net Logon                                                      | Not Defined                                           | Not Defined | Not Defined                                           |                                                                                                 |   |
| 176 | 4.1.12 - NetMeeting Remote Desktop Sharing                              | Disabled                                              | Not Defined | Disabled                                              |                                                                                                 |   |
| 177 | 4.1.13 - Remote Desktop Help Session Manager                            | Not Defined                                           | Not Defined | Not Defined                                           |                                                                                                 |   |
| 178 | 4.1.14 - Remote Registry Service                                        | Not Defined                                           | Not Defined | Automatic                                             | We would ask for "disabled" - may allow easier SMS install                                      |   |
| 179 | 4.1.15 - Routing and Remote Access                                      | Disabled                                              | Not Defined | Disabled                                              |                                                                                                 |   |
| 180 | 4.1.16 - Simple Mail Transfer Protocol (SMTP)                           | Disabled                                              | Not Defined | Disabled                                              |                                                                                                 |   |
| 181 | 4.1.17 - Simple Network Management Protocol (SNMP) Service              | Disabled                                              | Not Defined | Disabled                                              |                                                                                                 |   |
| 182 | 4.1.18 - Simple Network Management Protocol (SNMP) Trap                 | Disabled                                              | Not Defined | Disabled                                              |                                                                                                 |   |
| 183 | 4.1.19 - Task Scheduler                                                 | Not Defined                                           | Not Defined | Not Defined                                           |                                                                                                 |   |
| 184 | 4.1.20 - Telnet                                                         | Disabled                                              | Not Defined | Disabled                                              |                                                                                                 |   |
| 185 | 4.1.21 - Terminal Services                                              | Not Defined                                           | Not Defined | Not Defined                                           | Would disable this for general desktop                                                          |   |
| 186 | 4.1.22 - Universal Plug and Play Device Host                            | Disabled                                              | Not Defined | Disabled                                              | ?? Need to be checked                                                                           |   |
| 187 | 4.1.23 - World Wide Web Publishing Services                             | Disabled                                              | Not Defined | Disabled                                              |                                                                                                 |   |
| 188 |                                                                         |                                                       |             |                                                       |                                                                                                 |   |
| 189 | 4.2 - User Rights                                                       |                                                       |             |                                                       |                                                                                                 |   |
| 190 | 4.2.1 - Access this computer from the network                           | Not Defined                                           | Not Defined | Users, Administrators                                 | Could have been anonymous? Is this what it means                                                |   |
| 191 | 4.2.2 - Act as part of the operating system                             | None                                                  | Not Defined | None                                                  |                                                                                                 |   |
| 192 | 4.2.3 - Add workstations to domain                                      | Not Applicable                                        | Not Defined | Not Applicable                                        |                                                                                                 |   |
| 193 | 4.2.4 - Adjust memory quotas for a process                              | Not Defined                                           | Not Defined | Not Defined                                           |                                                                                                 |   |
| 194 | 4.2.5 - Allow logon through Terminal services                           | Not Defined                                           | Not Defined | Not Defined                                           | disabled                                                                                        |   |
| 195 | 4.2.6 - Back up files and directories                                   | Not Defined                                           | Not Defined | Administrators, Backup Operators                      |                                                                                                 |   |
| 196 | 4.2.7 - Bypass traverse checking                                        | Not Defined                                           | Not Defined | Users                                                 |                                                                                                 |   |
| 197 | 4.2.8 - Change the system time                                          | Administrators                                        | Not Defined | Administrators                                        |                                                                                                 |   |
| 198 | 4.2.9 - Create a pagelfile                                              | Administrators                                        | Not Defined | Administrators                                        |                                                                                                 |   |
| 199 | 4.2.10 - Create a token object                                          | None                                                  | Not Defined | None                                                  |                                                                                                 |   |
| 200 | 4.2.11 - Create permanent shared objects                                | None                                                  | Not Defined | None                                                  |                                                                                                 |   |
| 201 | 4.2.12 - Debug Programs                                                 | Administrators                                        | Not Defined | Not Defined                                           |                                                                                                 |   |
| 202 | 4.2.13 - Deny access to this computer from the network                  | Guests, Support_388945a0                              | Not Defined | Guests, Support_388945a0                              |                                                                                                 |   |
| 203 | 4.2.14 - Deny logon as a batch job                                      | Not Defined                                           | Not Defined | Not Defined                                           | enabled                                                                                         |   |
| 204 | 4.2.15 - Deny logon as a service                                        | Not Defined                                           | Not Defined | Not Defined                                           | enabled                                                                                         |   |
| 205 | 4.2.16 - Deny logon locally                                             | Not Defined                                           | Not Defined | Not Defined                                           |                                                                                                 |   |
| 206 | 4.2.17 - Deny logon through Terminal Service                            | Not Defined                                           | Not Defined | Not Defined                                           | enabled                                                                                         |   |
| 207 | 4.2.18 - Enable computer and user accounts to be trusted for delegation | Not Applicable                                        | Not Defined | Not Applicable                                        |                                                                                                 |   |
| 208 | 4.2.19 - Force shutdown from a remote system                            | Administrators                                        | Not Defined | Administrators                                        |                                                                                                 |   |
| 209 | 4.2.20 - Generate security audits                                       | Local Service, Network Service                        | Not Defined | None                                                  |                                                                                                 |   |
| 210 | 4.2.21 - Increase scheduling priority                                   | Administrators                                        | Not Defined | Administrators                                        |                                                                                                 |   |
| 211 | 4.2.22 - Load and unload device drivers                                 | Administrators                                        | Not Defined | Administrators                                        | Does this prevent from software installation?                                                   |   |
| 212 | 4.2.23 - Lock pages in memory                                           | None                                                  | Not Defined | None                                                  |                                                                                                 |   |
| 213 | 4.2.24 - Log on as a batch job                                          | Not Defined                                           | Not Defined | Not Defined                                           |                                                                                                 |   |
| 214 | 4.2.25 - Log on as a service                                            | Not Defined                                           | Not Defined | Not Defined                                           |                                                                                                 |   |
| 215 | 4.2.26 - Log on locally                                                 | Users, Administrators                                 | Not Defined | Users, Administrators                                 |                                                                                                 |   |
| 216 | 4.2.27 - Manage auditing and security log                               | Administrators                                        | Not Defined | Administrators                                        |                                                                                                 |   |
| 217 | 4.2.28 - Modify firmware environment values                             | Administrators                                        | Not Defined | Administrators                                        |                                                                                                 |   |
| 218 | 4.2.29 - Perform volume maintenance tasks                               | Administrators                                        | Not Defined | Administrators                                        |                                                                                                 |   |
| 219 | 4.2.30 - Profile single process                                         | Administrators                                        | Not Defined | Administrators                                        |                                                                                                 |   |
| 220 | 4.2.31 - Profile system performance                                     | Administrators                                        | Not Defined | Administrators                                        |                                                                                                 |   |
| 221 | 4.2.32 - Remove computer from docking station                           | Users, Administrators                                 | Not Defined | Users, Administrators                                 |                                                                                                 |   |
| 222 | 4.2.33 - Replace a process level token                                  | Local Service, Network Service                        | Not Defined | None                                                  |                                                                                                 |   |
| 223 | 4.2.34 - Restore files and directories                                  | Administrators                                        | Not Defined | Administrators                                        |                                                                                                 |   |
| 224 | 4.2.35 - Shut down the system                                           | Users, Administrators                                 | Not Defined | Users, Administrators                                 |                                                                                                 |   |
| 225 | 4.2.36 - Synchronize directory service data                             | Not Applicable                                        | Not Defined | Not Applicable                                        |                                                                                                 |   |
| 226 | 4.2.37 - Take ownership of file or other objects                        | Administrators                                        | Not Defined | Administrators                                        |                                                                                                 |   |
| 227 |                                                                         |                                                       |             |                                                       |                                                                                                 |   |
| 228 | 4.3 - Other System Requirements                                         |                                                       |             |                                                       |                                                                                                 |   |
| 229 | 4.3.1 - Ensure volumes are using the NTFS file system                   | All volumes                                           | Not Defined | VBScript to verify NTFS                               | Would set as "Not defined" / perhaps system disk only (this is seen as sending an Email warning |   |
| 230 | 4.3.2 - Disable NetBIOS                                                 | Not Defined                                           | Not Defined | Not Defined                                           |                                                                                                 |   |
| 231 | 4.3.3 - Enable the Internet Connection Firewall                         | Not Defined                                           | Not Defined | Disabled                                              | This means disble Windows firewall and enable TrendMicro (third party)                          |   |
| 232 | 4.3.4 - Restricted Groups                                               | Remote Desktop Users: None                            | Not Defined | Remote Desktop Users: None                            |                                                                                                 |   |
| 233 |                                                                         |                                                       |             |                                                       |                                                                                                 |   |
| 234 | 4.4 - File                                                              |                                                       |             |                                                       |                                                                                                 |   |
| 235 | 4.4.1 - File Permissions                                                |                                                       |             |                                                       |                                                                                                 |   |
| 236 | 4.4.1.1 %SystemRoot%\system32\at.exe                                    | Administrators: Full; System: Full                    | Not Defined | Administrators: Full; System: Full                    |                                                                                                 |   |
| 237 | 4.4.1.2 %SystemRoot%\system32\attrib.exe                                | Administrators: Full; System: Full                    | Not Defined | Administrators: Full; System: Full                    |                                                                                                 |   |
| 238 | 4.4.1.3 %SystemRoot%\system32\cdps.exe                                  | Administrators: Full; System: Full                    | Not Defined | Administrators: Full; System: Full                    |                                                                                                 |   |
| 239 | 4.4.1.4 %SystemRoot%\system32\debug.exe                                 | Administrators: Full; System: Full                    | Not Defined | Administrators: Full; System: Full                    |                                                                                                 |   |
| 240 | 4.4.1.5 %SystemRoot%\system32\drwatson.exe                              | Administrators: Full; System: Full                    | Not Defined | Administrators: Full; System: Full                    |                                                                                                 |   |
| 241 | 4.4.1.6 %SystemRoot%\system32\drwtsn32.exe                              | Administrators: Full; System: Full                    | Not Defined | Administrators: Full; System: Full                    |                                                                                                 |   |
| 242 | 4.4.1.7 %SystemRoot%\system32\edlin.exe                                 | Administrators: Full; System: Full; Interactive: Full | Not Defined | Administrators: Full; System: Full; Interactive: Full |                                                                                                 |   |
| 243 | 4.4.1.8 %SystemRoot%\system32\eventcreate.exe                           | Administrators: Full; System: Full                    | Not Defined | Administrators: Full; System: Full                    |                                                                                                 |   |
| 244 | 4.4.1.9 %SystemRoot%\system32\eventtriggers.exe                         | Administrators: Full; System: Full                    | Not Defined | Administrators: Full; System: Full                    |                                                                                                 |   |
| 245 | 4.4.1.10 %SystemRoot%\system32\ftp.exe                                  | Administrators: Full; System: Full; Interactive: Full | Not Defined | Administrators: Full; System: Full; Interactive: Full |                                                                                                 |   |
| 246 | 4.4.1.11 %SystemRoot%\system32\net.exe                                  | Administrators: Full; System: Full; Interactive: Full | Not Defined | Administrators: Full; System: Full; Interactive: Full |                                                                                                 |   |
| 247 | 4.4.1.12 %SystemRoot%\system32\net1.exe                                 | Administrators: Full; System: Full; Interactive: Full | Not Defined | Administrators: Full; System: Full; Interactive: Full |                                                                                                 |   |
| 248 | 4.4.1.13 %SystemRoot%\system32\netsh.exe                                | Administrators: Full; System: Full                    | Not Defined | Administrators: Full; System: Full                    |                                                                                                 |   |
| 249 | 4.4.1.14 %SystemRoot%\system32\rpc.exe                                  | Administrators: Full; System: Full                    | Not Defined | Administrators: Full; System: Full                    |                                                                                                 |   |
| 250 | 4.4.1.15 %SystemRoot%\system32\reg.exe                                  | Administrators: Full; System: Full                    | Not Defined | Administrators: Full; System: Full                    |                                                                                                 |   |

|     | A                                                                            | B                                                                                                                                                                                                                                                                                                                                           | C           | D                                                                                                                                                                                                                                                                                                                                           | E                           | F |
|-----|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|---|
| 251 | 4.4.1.16 %SystemRoot%\regedit.exe                                            | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 252 | 4.4.1.17 %SystemRoot%\system32\regedit32.exe                                 | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 253 | 4.4.1.18 %SystemRoot%\system32\regsvr32.exe                                  | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 254 | 4.4.1.19 %SystemRoot%\system32\rexc.exe                                      | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 255 | 4.4.1.20 %SystemRoot%\system32\rsh.exe                                       | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 256 | 4.4.1.21 %SystemRoot%\system32\runas.exe                                     | Administrators: Full; System: Full; Interactive: Full                                                                                                                                                                                                                                                                                       | Not Defined | Administrators: Full; System: Full; Interactive: Full                                                                                                                                                                                                                                                                                       |                             |   |
| 257 | 4.4.1.22 %SystemRoot%\system32\isc.exe                                       | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 258 | 4.4.1.23 %SystemRoot%\system32\subst.exe                                     | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 259 | 4.4.1.24 %SystemRoot%\system32\telnet.exe                                    | Administrators: Full; System: Full; Interactive: Full                                                                                                                                                                                                                                                                                       | Not Defined | Administrators: Full; System: Full; Interactive: Full                                                                                                                                                                                                                                                                                       |                             |   |
| 260 | 4.4.1.25 %SystemRoot%\system32\tftp.exe                                      | Administrators: Full; System: Full; Interactive: Full                                                                                                                                                                                                                                                                                       | Not Defined | Administrators: Full; System: Full; Interactive: Full                                                                                                                                                                                                                                                                                       |                             |   |
| 261 | 4.4.1.26 %SystemRoot%\system32\tlntsvr.exe                                   | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 262 |                                                                              |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 263 | <b>5 - Administrative Templates</b>                                          |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 264 |                                                                              |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 265 | <b>5.1 - System</b>                                                          |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 266 | 5.1.1 Remote Procedure Call                                                  |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 267 | 5.1.1.1 RPC Endpoint Mapper Client Authentication (SP2 only)                 | Not Defined                                                                                                                                                                                                                                                                                                                                 | Not Defined | Not Defined                                                                                                                                                                                                                                                                                                                                 |                             |   |
| 268 | 5.1.1.2 Restrictions for Unauthenticated RPC clients (SP2 only)              | Not Defined                                                                                                                                                                                                                                                                                                                                 | Not Defined | Not Defined                                                                                                                                                                                                                                                                                                                                 |                             |   |
| 269 |                                                                              |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 270 | <b>5.2 Network</b>                                                           |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 271 | 5.2.1 Network Connections                                                    |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 272 | 5.2.1.1 Windows Firewall                                                     | Enabled                                                                                                                                                                                                                                                                                                                                     | Not Defined | <b>Disabled</b>                                                                                                                                                                                                                                                                                                                             | See also 231 (same menaing) |   |
| 273 |                                                                              |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 274 | <b>5.3 - Windows Components</b>                                              |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 275 | <b>5.3.1 Security Center</b>                                                 |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 276 | 5.3.1.1 Turn on Security Center (Domain PCs Only) (SP2 only)                 | Enabled                                                                                                                                                                                                                                                                                                                                     | Not Defined | Enabled                                                                                                                                                                                                                                                                                                                                     |                             |   |
| 277 |                                                                              |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 278 |                                                                              |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 279 | <b>Additional Security Settings - BNL</b>                                    |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 280 | (Settings taken from the CIS Windows 2000 Level-2 Benchmark)                 |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 281 |                                                                              |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 282 | <b>4.4 File and Registry Permissions</b>                                     |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 283 | <b>4.4.1 File Permissions</b>                                                |                                                                                                                                                                                                                                                                                                                                             |             |                                                                                                                                                                                                                                                                                                                                             |                             |   |
| 284 | 4.4.1.1 %SystemDrive%\                                                       | Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List                                                                                                                                                                                                                                                      | Not Defined | Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List                                                                                                                                                                                                                                                      |                             |   |
| 285 | 4.4.1.2 %SystemDrive%\autoexec.bat                                           | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 286 | 4.4.1.3 %SystemDrive%\boot.ini                                               | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 287 | 4.4.1.4 %SystemDrive%\config.sys                                             | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 288 | 4.4.1.5 %SystemDrive%\io.sys                                                 | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 289 | 4.4.1.6 %SystemDrive%\msdos.sys                                              | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 290 | 4.4.1.7 %SystemDrive%\ntbootdd.sys                                           | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 291 | 4.4.1.8 %SystemDrive%\ntdetect.com                                           | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 292 | 4.4.1.9 %SystemDrive%\ntldr                                                  | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 293 | 4.4.1.10 %SystemDrive%\Documents and Settings                                | Administrators: Full; System: Full; Users: Read and Execute, List                                                                                                                                                                                                                                                                           | Not Defined | Administrators: Full; System: Full; Users: Read and Execute, List                                                                                                                                                                                                                                                                           |                             |   |
| 294 | 4.4.1.11 %SystemDrive%\Documents and Settings\Administrator                  | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 295 | 4.4.1.12 %SystemDrive%\Documents and Settings\All Users                      | Administrators: Full; System: Full; Users: Read and Execute, List                                                                                                                                                                                                                                                                           | Not Defined | Administrators: Full; System: Full; Users: Read and Execute, List                                                                                                                                                                                                                                                                           |                             |   |
| 296 | 4.4.1.13 %SystemDrive%\Documents and Settings\All Users\Documents\I\DrWatson | Administrators: Full; System: Full; Creator Owner: Full; Users: Traverse Folder/Execute File, List Folder/Read Data, Read Attributes, Read Extended Attributes, Read Permissions (This folder, subfolders, and files); Users: Traverse Folder/Execute Files, Create Files/Write Data, Create Folder/Append Data (Subfolders and files only) | Not Defined | Administrators: Full; System: Full; Creator Owner: Full; Users: Traverse Folder/Execute File, List Folder/Read Data, Read Attributes, Read Extended Attributes, Read Permissions (This folder, subfolders, and files); Users: Traverse Folder/Execute Files, Create Files/Write Data, Create Folder/Append Data (Subfolders and files only) |                             |   |
| 297 | 4.4.1.14 %SystemDrive%\Documents and Settings\Default User                   | Administrators: Full; System: Full; Users: Read and Execute, List                                                                                                                                                                                                                                                                           | Not Defined | Administrators: Full; System: Full; Users: Read and Execute, List                                                                                                                                                                                                                                                                           |                             |   |
| 298 | 4.4.1.15 %ProgramFiles%                                                      | Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List                                                                                                                                                                                                                                                      | Not Defined | Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List                                                                                                                                                                                                                                                      |                             |   |
| 299 | 4.4.1.16 %Program Files%\Resource Kit                                        | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 300 | 4.4.1.17 %Program Files%\Resource Pro Kit                                    | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 301 | 4.4.1.18 %SystemRoot%                                                        | Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List                                                                                                                                                                                                                                                      | Not Defined | Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List                                                                                                                                                                                                                                                      |                             |   |
| 302 | 4.4.1.19 %SystemRoot%\\$NtServicePackUninstall\$                             | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 303 | 4.4.1.20 %SystemRoot%\CSC                                                    | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          | Not Defined | Administrators: Full; System: Full                                                                                                                                                                                                                                                                                                          |                             |   |
| 304 | 4.4.1.21 %SystemRoot%\Debug                                                  | Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List                                                                                                                                                                                                                                                      | Not Defined | Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List                                                                                                                                                                                                                                                      |                             |   |
| 305 | 4.4.1.22 %SystemRoot%\Debug\UserMode                                         | Administrators: Full; System: Full; Users: Traverse Folder/Execute File, List folder/Read data, Create files/Write data (This folder, only); Create files/Write data, Create folders/Append data (Files Only)                                                                                                                               | Not Defined | Administrators: Full; System: Full; Users: Traverse Folder/Execute File, List folder/Read data, Create files/Write data (This folder, only); Create files/Write data, Create folders/Append data (Files Only)                                                                                                                               |                             |   |
| 306 | 4.4.1.23 %SystemRoot%\Offline Web Pages                                      | Ignore Parent Permission Changes                                                                                                                                                                                                                                                                                                            | Not Defined | Ignore Parent Permission Changes                                                                                                                                                                                                                                                                                                            |                             |   |
| 307 | 4.4.1.24 %SystemRoot%\Registration                                           | Administrators: Full; System: Full; Users: Read                                                                                                                                                                                                                                                                                             | Not Defined | Administrators: Full; System: Full; Users: Read                                                                                                                                                                                                                                                                                             |                             |   |

|     | A                                                                                                                                                                                                                                    | B                                                                                                                                                                                             | C           | D                                                                                                                                                                                             | E | F |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|
| 308 | 4.4.1.25 %SystemRoot%\repair                                                                                                                                                                                                         | Administrators: Full; System: Full                                                                                                                                                            | Not Defined | Administrators: Full; System: Full                                                                                                                                                            |   |   |
| 309 | 4.4.1.26 %SystemRoot%\security                                                                                                                                                                                                       | Administrators: Full; System: Full; Creator Owner: Full                                                                                                                                       | Not Defined | Administrators: Full; System: Full; Creator Owner: Full                                                                                                                                       |   |   |
| 310 | 4.4.1.27 %SystemRoot%\system32                                                                                                                                                                                                       | Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List                                                                                                        | Not Defined | Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List                                                                                                        |   |   |
| 311 | 4.4.1.29 %SystemRoot%\system32\ntbackup.exe                                                                                                                                                                                          | Administrators: Full; System: Full                                                                                                                                                            | Not Defined | Administrators: Full; System: Full                                                                                                                                                            |   |   |
| 312 | 4.4.1.35 %SystemRoot%\system32\secdit.exe                                                                                                                                                                                            | Administrators: Full; System: Full                                                                                                                                                            | Not Defined | Administrators: Full; System: Full                                                                                                                                                            |   |   |
| 313 | 4.4.1.36 %SystemRoot%\system32\lppmgmt                                                                                                                                                                                               | Administrators: Full; System: Full; Users: Read and Execute, List                                                                                                                             | Not Defined | Administrators: Full; System: Full; Users: Read and Execute, List                                                                                                                             |   |   |
| 314 | 4.4.1.37 %SystemRoot%\system32\config                                                                                                                                                                                                | Administrators: Full; System: Full                                                                                                                                                            | Not Defined | Administrators: Full; System: Full                                                                                                                                                            |   |   |
| 315 | 4.4.1.38 %SystemRoot%\system32\dlcache                                                                                                                                                                                               | Administrators: Full; System: Full; Creator Owner: Full                                                                                                                                       | Not Defined | Administrators: Full; System: Full; Creator Owner: Full                                                                                                                                       |   |   |
| 316 | 4.4.1.39 %SystemRoot%\system32\DTCLog                                                                                                                                                                                                | Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List                                                                                                        | Not Defined | Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List                                                                                                        |   |   |
| 317 | 4.4.1.40 %SystemRoot%\system32\Group Policy                                                                                                                                                                                          | Administrators: Full; System: Full; Authenticated Users: Read and Execute, List                                                                                                               | Not Defined | Administrators: Full; System: Full; Authenticated Users: Read and Execute, List                                                                                                               |   |   |
| 318 | 4.4.1.41 %SystemRoot%\system32\ias                                                                                                                                                                                                   | Administrators: Full; System: Full; Creator Owner: Full                                                                                                                                       | Not Defined | Administrators: Full; System: Full; Creator Owner: Full                                                                                                                                       |   |   |
| 319 | 4.4.1.42 %SystemRoot%\system32\NTMSData                                                                                                                                                                                              | Administrators: Full; System: Full                                                                                                                                                            | Not Defined | Administrators: Full; System: Full                                                                                                                                                            |   |   |
| 320 | 4.4.1.43 %SystemRoot%\system32\reinstallbackups                                                                                                                                                                                      | Administrators: Full; System: Full; Creator Owner: Full; Power Users: Read and Execute, List                                                                                                  | Not Defined | Administrators: Full; System: Full; Creator Owner: Full; Power Users: Read and Execute, List                                                                                                  |   |   |
| 321 | 4.4.1.44 %SystemRoot%\system32\Setup                                                                                                                                                                                                 | Administrators: Full; System: Full; Users: Read and Execute, List                                                                                                                             | Not Defined | Administrators: Full; System: Full; Users: Read and Execute, List                                                                                                                             |   |   |
| 322 | 4.4.1.45 %SystemRoot%\system32\spool\printers                                                                                                                                                                                        | Administrators: Full; System: Full; Creator Owner: Full; Users: Traverse Folder, Execute File, Read, Read Extended Attributes, Create folders, Append Data                                    | Not Defined | Administrators: Full; System: Full; Creator Owner: Full; Users: Traverse Folder, Execute File, Read, Read Extended Attributes, Create folders, Append Data                                    |   |   |
| 323 | 4.4.1.46 %SystemRoot%\Tasks                                                                                                                                                                                                          | (Do not allow permissions on this folder to be replaced)                                                                                                                                      | Not Defined | (Do not allow permissions on this folder to be replaced)                                                                                                                                      |   |   |
| 324 | 4.4.1.47 %SystemDrive%\System Volume Information                                                                                                                                                                                     | (Do not allow permissions on this folder to be replaced)                                                                                                                                      | Not Defined | (Do not allow permissions on this folder to be replaced)                                                                                                                                      |   |   |
| 325 |                                                                                                                                                                                                                                      |                                                                                                                                                                                               |             |                                                                                                                                                                                               |   |   |
| 326 | 4.4.2 Registry Permissions                                                                                                                                                                                                           |                                                                                                                                                                                               |             |                                                                                                                                                                                               |   |   |
| 327 | * Unless stated otherwise, Administrators or System Full Control is full control for the designated key and all subkeys. Creator Owner Full Control is for subkeys only. Users permissions are for current key, subkeys, and values. |                                                                                                                                                                                               |             |                                                                                                                                                                                               |   |   |
| 328 | 4.4.2.1 HKLM\Software\Classes                                                                                                                                                                                                        | Administrators: Full; System: Full; Creator Owner: Full; Users: Read                                                                                                                          | Not Defined | Administrators: Full; System: Full; Creator Owner: Full; Users: Read                                                                                                                          |   |   |
| 329 | 4.4.2.2 HKLM\Software                                                                                                                                                                                                                | Administrators Full; System: Full; Creator Owner: Full; ers: Read                                                                                                                             | Not Defined | Administrators Full; System: Full; Creator Owner: Full; ers: Read                                                                                                                             |   |   |
| 330 | 4.4.2.3 HKLM\Software\Microsoft\Net DDE                                                                                                                                                                                              | Administrators: Full; System: Full                                                                                                                                                            | Not Defined | Administrators: Full; System: Full                                                                                                                                                            |   |   |
| 331 | 4.4.2.5 HKLM\Software\Microsoft\Windows NT\CurrentVersion\Asr\Commands                                                                                                                                                               | Administrators: Full; System: Full; Creator Owner: Full; Users: Read; Backup Operators: Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, Read (this key and subkeys) | Not Defined | Administrators: Full; System: Full; Creator Owner: Full; Users: Read; Backup Operators: Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, Read (this key and subkeys) |   |   |
| 332 | 4.4.2.6 HKLM\Software\Microsoft\Windows NT\CurrentVersion\Perflib                                                                                                                                                                    | Administrators: Full; System: Full; Creator Owner: Full; Interactive: Read (this key and subkeys)                                                                                             | Not Defined | Administrators: Full; System: Full; Creator Owner: Full; Interactive: Read (this key and subkeys)                                                                                             |   |   |
| 333 | 4.4.2.7 HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy                                                                                                                                                                  | Administrators: Full; System: Full; Authenticated Users: Read Authenticated Users: Read                                                                                                       | Not Defined | Administrators: Full; System: Full; Authenticated Users: Read Authenticated Users: Read                                                                                                       |   |   |
| 334 | 4.4.2.8 HKLM\Software\Microsoft\Windows\CurrentVersion\Installer                                                                                                                                                                     | Administrators Full; System: Full; Users: Read                                                                                                                                                | Not Defined | Administrators Full; System: Full; Users: Read                                                                                                                                                |   |   |
| 335 | 4.4.2.9 HKLM\Software\Microsoft\Windows\CurrentVersion\Policies                                                                                                                                                                      | Administrators: Full; System: Full; Authenticated Users: Read                                                                                                                                 | Not Defined | Administrators: Full; System: Full; Authenticated Users: Read                                                                                                                                 |   |   |
| 336 | 4.4.2.10 HKLM\System                                                                                                                                                                                                                 | Administrators Full; System: Full; Creator Owner: Full; Users: Read                                                                                                                           | Not Defined | Administrators Full; System: Full; Creator Owner: Full; Users: Read                                                                                                                           |   |   |
| 337 | 4.4.2.11 HKLM\System\Clone                                                                                                                                                                                                           | Allow inheritable permissions to propagate to this object                                                                                                                                     | Not Defined | Allow inheritable permissions to propagate to this object                                                                                                                                     |   |   |
| 338 | 4.4.2.12 HKLM\System\Control\Set001                                                                                                                                                                                                  | Administrators Full; System: Full; Creator Owner: Full; Users: Read                                                                                                                           | Not Defined | Administrators Full; System: Full; Creator Owner: Full; Users: Read                                                                                                                           |   |   |
| 339 | 4.4.2.13 HKLM\System\Control\Set00x * Apply these permissions to all control sets other than CurrentControlSet.                                                                                                                      | Administrators Full; System: Full; Creator Owner: Full; Users: Read                                                                                                                           | Not Defined | Administrators Full; System: Full; Creator Owner: Full; Users: Read                                                                                                                           |   |   |
| 340 | 4.4.2.14 HKLM\System\CurrentControlSet\Control\SecurePipeServers\WinReg                                                                                                                                                              | Administrators: Full                                                                                                                                                                          | Not Defined | Administrators: Full; Local Service: Read                                                                                                                                                     |   |   |
| 341 | 4.4.2.15 HKLM\System\CurrentControlSet\Control\WMI\Security                                                                                                                                                                          | Administrators: Full; System: Full; Creator Owner: Full (this key and subkeys)                                                                                                                | Not Defined | Administrators: Full; System: Full; Creator Owner: Full (this key and subkeys)                                                                                                                |   |   |
| 342 | 4.4.2.16 HKLM\System\CurrentControlSet\Enum                                                                                                                                                                                          | (Do not allow permissions on this key to be replaced)                                                                                                                                         | Not Defined | (Do not allow permissions on this key to be replaced)                                                                                                                                         |   |   |
| 343 | 4.4.2.17 HKLM\System\CurrentControlSet\Hardware Profiles                                                                                                                                                                             | Administrators Full; System: Full; Creator Owner: Full; Users: Read                                                                                                                           | Not Defined | Administrators Full; System: Full; Creator Owner: Full; Users: Read                                                                                                                           |   |   |
| 344 | 4.4.2.18 HKLM\System\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers                                                                                                                                                    | Administrators Full; System: Full; Creator Owner: Full                                                                                                                                        | Not Defined | Administrators Full; System: Full; Creator Owner: Full                                                                                                                                        |   |   |

|     | A                                                                            | B                                                                            | C           | D                                                                            | E | F |
|-----|------------------------------------------------------------------------------|------------------------------------------------------------------------------|-------------|------------------------------------------------------------------------------|---|---|
|     | 4.4.2.19                                                                     |                                                                              |             | Administrators Full; System: Full; Creator Owner: Full                       |   |   |
| 345 | HKLM\System\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities      | Administrators Full; System: Full; Creator Owner: Full                       | Not Defined | Owner: Full                                                                  |   |   |
| 346 | 4.4.2.20 HKU\Default -                                                       | Administrators Full; System: Full; Creator Owner: Full; Users: Read          | Not Defined | Administrators Full; System: Full; Creator Owner: Full; Users: Read          |   |   |
| 347 | 4.4.2.21 HKU\DefaultSoftware\Microsoft\NetDDE - Administrators Full; System: | Full                                                                         | Not Defined | Full                                                                         |   |   |
| 348 | 4.4.2.22 HKU\DefaultSoftware\Microsoft\Protected Storage System Provider     | No entries                                                                   | Not Defined | No entries                                                                   |   |   |
| 349 |                                                                              |                                                                              |             |                                                                              |   |   |
| 350 | 4.4.3 File and Registry Auditing                                             |                                                                              |             |                                                                              |   |   |
| 351 | 4.4.3.1 %SystemDrive% - Everyone: Failures                                   | (this folder, propagate inheritable permissions to all subfolders and files) | Not Defined | (this folder, propagate inheritable permissions to all subfolders and files) |   |   |
| 352 | 4.4.3.2 HKLM\Software - Everyone: Failures                                   | (this key, propagate inheritable permission to all subkeys)                  | Not Defined | (this key, propagate inheritable permission to all subkeys)                  |   |   |
| 353 | 4.4.3.3 HKLM\System - Everyone: Failures                                     | (this key, propagate inheritable permission to all subkeys)                  | Not Defined | (this key, propagate inheritable permission to all subkeys)                  |   |   |

[illegible]



[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]