Nessus Report

Report

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

Table Of Contents

Compliance Executive

Compliance Tests

FAILED	2.1.1 Minimum Password Length: at least 8 characters
PASSED	2.1.2 Maximum Password Age: no more than 90 days old
FAILED	2.2.1.1 Audit Account Logon Events: Success and Failure
FAILED	2.2.1.2 Audit Account Managemement: Success and Failure
FAILED	2.2.1.4 Audit Logon Events: Success and Failure
FAILED	2.2.1.5 Audit Object Access: Failure (minimum)
FAILED	2.2.1.6 Audit Policy Change: Success and Failure
FAILED	2.2.1.7 Audit Privilege Use: Failure (minimum)
FAILED	2.2.1.9 Audit System Events: Success and Failure
FAILED	2.2.2.1 Minimum Password Age: 1 day
PASSED	2.2.2.2 Maximum Password Age: 90 days
FAILED	2.2.2.3 Minimum Password Length: 8 characters
FAILED	2.2.2.4 Password Complexity: Enabled
FAILED	2.2.2.5 Password History: 24 Passwords Remembered
PASSED	2.2.2.6 Store Passwords using Reversible Encryption: Disabled
PASSED	2.2.3.1 Account Lockout Duration: 15 minutes
FAILED	2.2.3.2 Account Lockout Threshold: 3 Bad Logon Attempts
PASSED	2.2.3.3 Reset Account Lockout After: 15 Minutes
FAILED	2.2.4.1.1 Maximum Event Log Size (Application): 80Mb
FAILED	2.2.4.1.3 Log Retention Method (Application): Overwrite Events As Needed
FAILED	2.2.4.2.1 Maximum Event Log Size (Security): 80Mb
FAILED	2.2.4.2.3 Log Retention Method (Security): Overwrite Events As Needed
FAILED	2.2.4.3.1 Maximum Event Log Size (System): 80Mb
FAILED	2.2.4.3.3 Log Retention Method (System): Overwrite Events As Needed
FAILED	3.1.1 Additional Restrictions for Anonymous Connections: No Access Without Explicit Anonymous Permissions
FAILED	3.2.1.2 Allow System to be Shut Down Without Having to Log On: Disabled
PASSED	3.2.1.3 Allowed to Eject Removable NTFS Media: Administrators
PASSED	3.2.1.4 Amount of Idle Time Required Before Disconnecting Session: 30 Minutes
PASSED	3.2.1.7 Automatically Log Off Users When Logon Time Expires: Enabled
FAILED	3.2.1.9 Clear Virtual Memory Pagefile When System Shuts Down: Enabled

PASSED 3.2.1.11 Digitally Sign Client Communication (When Possible): Enabled

FAILED 3.2.1.13 Digitally Sign Server Communication (When Possible): Enabled

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

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

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

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

FAILED 3.2.1.19 Number of Previous Logons to Cache: 0

PASSED 3.2.1.20 Prevent System Maintenance of Computer Account Password: Disabled

FAILED 3.2.1.21 Prevent Users from Installing Printer Drivers: Enabled

PASSED 3.2.1.22 Prompt User to Change Password Before Expiration: 14 days

PASSED 3.2.1.23 Recovery Console: Allow Automatic Administrative Logon: Disabled

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

FAILED 3.2.1.25 Rename Administrator Account: Anything but Administrator

FAILED 3.2.1.26 Rename Guest Account: Any value other than Guest

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

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

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

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

FAILED 3.2.1.35 Smart Card Removal Behavior: Lock Workstation (minimum)

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

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

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

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

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

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

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

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

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

PASSED	3.2.2.21 Enable IPSec to protect Kerberos RSVP Traffic: HKLM\System\CurrentControlSet\Services \IPSEC\NoDefaultExempt: 1
FAILED	4.1 Available Servcies (MSFtpsvc): Permissions on FTP Publishing Service: Administrators: Full Control; System: Read, Start, Stop, and Pause
FAILED	4.1 Available Services (Alerter): Permissions on Alerter: Administrators: Full Control; System: Read, Start, Stop, and Pause
FAILED	4.1 Available Services (Browser): Permissions on Computer Browser: Administrators: Full Control; System: Read, Start, Stop, and Pause
FAILED	4.1 Available Services (ClipSrv): Permissions on Clipbook: Administrators: Full Control; System: Read, Start, Stop, and Pause
FAILED	4.1 Available Services (FAX): Permissions on Fax Service: Administrators: Full Control: System; Read, Start, Stop, and Pause
FAILED	4.1 Available Services (IISADMIN): Permissions on IIS Admin Services: Administrators: Full Control; System: Read, Start, Stop, and Pause
FAILED	4.1 Available Services (Messenger): Permissions on Messenger: Administrators: Full Control; System: Read, Start, Stop, and Pause
FAILED	4.1 Available Services (RemoteAccess): Permissions on Routing and Remote Access: Administrators: Full Control; System: Read, Start, Stop, Pause
FAILED	4.1 Available Services (RemoteRegistry): Permissions on Remote Registry Service: Administrators: Full Control; System: Read, Start, Stop, and Pause
FAILED	4.1 Available Services (SMTPSVC): Permissions on SMTP: Administrators: Full Control; System: Read, Start, Stop, Pause
PASSED	4.1 Available Services (SNMP): Permissions on SNMP: Administrators: Full Control; System: Read, Start, Stop, and Pause
PASSED	4.1 Available Services (SNMPTRAP): Permissions on SNMP Trap: Administrators: Full Control; Sytem: Read, Start, Stop, and Pause
FAILED	4.1 Available Services (SharedAccess): Permissions on Internet Connection Sharing: Administrators: Full Control; System: Read, Start, Stop, and Pause
FAILED	4.1 Available Services (TlntSvr): Permissions on Telnet: Administrators: Full Control; System: Read, Start, Stop, and Pause
FAILED	4.1 Available Services (W3SVC): Permissions on World Wide Web Publishing Service: Administrators: Full Control; System: Read, Start, Stop, and Pause
FAILED	4.1 Available Services (mnmsrvc): Permissions on NetMeeting Remote Desktop Sharing: Administrators: Full Control; System: Read, Start, Stop, and Pause
FAILED	4.1.1 Alerter (Alerter): Disabled
FAILED	4.1.2 Clipbook (ClipSrv): Disabled
FAILED	4.1.3 Computer Browser (Browser): Disabled
FAILED	4.1.4 Fax Service (FAX): Disabled
FAILED	4.1.5 FTP Publishing Service (MSFtpsvc): Disabled (Warning: This will disable FTP Servers)
FAILED	4.1.6 IIS Admin Service (IISADMIN): Disabled (Warning: This will disable Internet Information Services)

FAILED 4.1.7 Internet Connection Sharing (SharedAccess): Disabled

FAILED 4.1.8 Messenger (Messenger): Disabled

FAILED 4.1.9 NetMeeting Remote Desktop Sharing (mnmsrvc): Disabled

FAILED 4.1.10 Remote Registry Service (RemoteRegistry): Disabled

PASSED 4.1.11 Routing and Remote Access (RemoteAccess): Disabled

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

PASSED 4.1.13 Simple Network Management Protocol (SNMP) Service: Disabled

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

FAILED 4.1.15 Telnet (TlntSvr): Disabled

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

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

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

FAILED 4.2.4 Back up files and directories (SeBackupPrivilege): Administrators

FAILED 4.2.5 Bypass travrse checking (SeChangeNotifyPrivilege): Users

FAILED 4.2.6 Change the system time (SeSystemTimePrivilege): Administrators

PASSED 4.2.7 Create a pagefile (SeCreatePagefilePrivilege): Administrators

PASSED 4.2.8 Create a token object (SeCreateTokenPrivilege): None

PASSED 4.2.9 Create permanent shared objects (SeCreatePermanentPrivilege): None

FAILED 4.2.10 Debug programs (SeDebugPrivilege): None

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

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

PASSED 4.2.17 Generate security audits (SeAuditPrivilege): None

PASSED 4.2.18 Increase quotas: Administrators

PASSED 4.2.19 Increase schedulign priority (SeIncreaseBasePriorityPrivilege): Administrators

PASSED 4.2.20 Load and unload device drivers (SeLoadDriverPrivilege): Administrators

PASSED 4.2.21 Lock pages in memory (SeLockMemoryPrivilege): None

FAILED 4.2.24 Log on locally (SeInteractiveLogonRight): Administrators

PASSED 4.2.25 Manage auditing and security log (SeSecurityPrivilege): Administrators

PASSED 4.2.26 Modify firmware environment values (SeSystemEnvironmentPrivilege): Administrators

FAILED 4.2.27 Profile single process (SeProfileSingleProcessPrivilege): Administrators

PASSED 4.2.28 Profile system performance (SeSystemProfilePrivilege): Administrators

FAILED 4.2.29 Remove computer from docking station (SeUndockPrivilege): Administrators

PASSED 4.2.30 Replace a process level token (SeAssignPrimaryTokenPrivilege): None

FAILED 4.2.31 Restore files and directories (SeRestorePrivilege): Administrators

FAILED 4.2.32 Shut down the system (SeShutdownPrivilege): Administrators

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FAILED	4.4.1.23 %SystemRoot%\Debug\UserMode - Administrators: Full; System: Full; Users (This folder, only): Traverse Folders/Execute Files, List folder/Read data, Create files/Write data; Users (Files only): Create Files/Write Data; Create folders/Append data
FAILED	4.4.1.25 %SystemRoot%\Registration - Administrators: Full; System: Full; Users: Read
FAILED	4.4.1.26 %SystemRoot%\repair - Administrators: Full; System: Full
FAILED	4.4.1.27 %SystemRoot%\security - Administrators: Full; System: Full; Creater Owner: Full
FAILED	4.4.1.28 %SystemRoot%\system32 - Administrators: Full; System: Full; Creater Owner: Full; Users: Read and Execute, List
FAILED	4.4.1.29 %SystemRoot%\system32\at.exe - Administrators: Full; System: Full
FAILED	4.4.1.30 %SystemRoot%\system32\Ntbackup.exe - Administrators: Full; System: Full
FAILED	4.4.1.31 %SystemRoot%\system32\rcp.exe - Administrators: Full; System: Full
FAILED	4.4.1.32 %SystemRoot%\regedit.exe - Administrators: Full; System: Full
FAILED	4.4.1.33 %SystemRoot%\system32\regedt32.exe - Administrators: Full; System: Full
FAILED	4.4.1.34 %SystemRoot%\system32\rexec.exe - Administrators: Full; System: Full
FAILED	4.4.1.35 %SystemRoot%\system32\rsh.exe - Administrators: Full; System: Full
FAILED	4.4.1.36 %SystemRoot%\system32\secedit.exe - Administrators: Full; System: Full
PASSED	4.4.1.37 %SystemRoot%\system32\appmgmt - Administrators: Full; System: Full; Users: Read and Execute, List
FAILED	4.4.1.38 %SystemRoot%\config - Administrators: Full; System: Full
PASSED	4.4.1.39 %SystemRoot%\system32\dllcache - Adminstrators: Full; System: Full; Creater Owner: Full
FAILED	4.4.1.40 %SystemRoot%\system32\DTCLog - Administrators: Full; System: Full; Users: Read and Execute, List
PASSED	4.4.1.41 %SystemRoot%\system32\GroupPolicy - Administrators: Full; System: Full; Authenticated Users: Read and Execute, List
PASSED	4.4.1.42 %SystemRoot%\system32\ias - Administrators: Full; System: Full; Creater Owner: Full
FAILED	4.4.1.43 %SystemRoot%\system32\NTMSData - Administrators: Full; System: Full
PASSED	4.4.1.44 %SystemRoot%\system32\reinstallbackups - Administrators: Full; System: Full; Creater Owner: Full
FAILED	4.4.1.45 %SystemRoot%\system32\Setup - Admininstrators: Full; System: Full; Users: Read and Execute, List
FAILED	4.4.1.46 %SystemRoot%\system32\spool\printers - Administrators: Full; System: Full; Creater Owner: Full; Users: Traverse Folder/Execute file, Read, Read Extended Attributes, Create folders, Append Data
FAILED	4.4.1.48 %SystemRoot%\Temp - Administrators: Full; System: Full; Creater Owner: Full; Users: Traverse Folders/Execute Files, Create Files/Write Data, Create Folders/Append Data
FAILED	4.4.2.1 HKLM\Software\Classes - Administrators: Full; System: Full; Creater Owner: Full; Users: Read
FAILED	4.4.2.2 HKLM\Software - Administrators: Full; System: Full; Creater Owner: Full; Users: Read
FAILED	4.4.2.3 HKLM\Software\Microsoft\NetDDE - Administrators: Full; System: Full

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FAILED 4.4.2.21 HKU\.Default\Software\Microsoft\NetDDE

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

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

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