




NNT Windows Security Standards Checklist: NNTDEMO-PC

NNT Security Compliance Report 1210b

Total score: 35.36 %

-  24 out of 140 rules passed
-  51 out of 140 rules did not pass completely
-  65 out of 140 rules failed

NNT Windows Security Standards Checklist

1. File System

1. Formatting

1. All disk file systems must be formatted to NTFS

This test assesses whether all drives are formatted to NTFS.

 Passed with a score of 1.0

Rule requires that All conditions pass. The 1 test of this condition in the time period passed.
Passes were: 'drive.driveformat' value must be equal to NTFS. At 16/12/2010 15:01:24 value was 'NTFS' for C:\

2. Security

1. System Drive modify permissions must be restricted


This test assesses whether default modify rights to the system drive are restricted to SYSTEM and Administrator accounts.

 Passed with a score of 1.0

Rule requires that All conditions pass. The 1 test of this condition in the time period passed.
Passes were: Security descriptor 'D:PAI(A;;LC;;;AU)(A;OICIIO;SDGXGWGR;;;AU)(A;;FA;;;SY)(A;OICIIO;GA;;;SY)(A;OICIIO;GA;;;BA)(A;;FA;;;BA)(A;OICI;0x1200a9;;;BU)' must indicate identities with effective right allowed includes only those in given list SYSTEM,Administrators:Modify. At 15/12/2010 17:50:53 value was ImplicitPass (RestrictAccessHonored) for c:\

2. Windows Folder modify permissions must be restricted

This test assesses whether default modify rights to the Windows folder are restricted to SYSTEM and Administrator (and TrustedInstaller on Vista and above) accounts.

 Passed with a score of 1.0

Rule requires that All conditions pass. All 2 tests of this condition in the time period passed. 1 was not tested for the following reasons: 'Rule not relevant to operating system: Windows7'. Passes were: Security descriptor 'D:PAI(A;OICIIO;GA;;;CO)(A;OICIIO;GA;;;SY)(A;0x1301bf;;;SY)(A;OICIIO;GA;;;BA)(A;0x1301bf;;;BA)(A;OICIIO;GXGR;;;BU)(A;0x1200a9;;;BU)(A;CIIO;GA;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)(A;FA;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)' must indicate identities with effective right allowed includes only those in given list SYSTEM,Administrators,TrustedInstaller:Modify. At 15/12/2010 17:50:53 value was ImplicitPass (RestrictAccessHonored) for c:\windows

2. Security Settings


1. Accounts

1. Guest Account must be Disabled

 Failed with a score of 0

Rule requires that All conditions pass. 1 of the 1 tests in the time period failed. Failures were: 'securitypolicy.se_EnableGuestAccount' value must be equal to 0. At 16/12/2010 15:01:24 value was '1' for Local Security Policy

2. Guest Account must be Renamed

 Failed with a score of 0

Rule requires that All conditions pass. 1 of the 1 tests in the time period failed. Failures were: 'securitypolicy.se_NewGuestName' value must be not equal to "Guest". At 16/12/2010 15:01:24 value was ""Guest"" for Local Security Policy

3. Builtin Administrator Account must be Renamed

 Failed with a score of 0

Rule requires that All conditions pass. 1 of the 1 tests in the time period failed. Failures were: 'securitypolicy.se_NewAdministratorName' value must be not equal to "Administrator". At 16/12/2010 15:01:24 value was ""Administrator"" for Local Security Policy

2. Privilege Elevation

1. User Account Control (UAC) must be enabled

This test assesses whether the Vista UAC feature is enabled.

 Passed with a score of 1.0

Rule requires that All conditions pass. The 1 test of this condition in the time period passed.
Passes were: 'regvalue [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA].regvalvalue' value must be greater than 0. At 16/12/2010 15:01:26 value was '1' for hkey_local_machine\software\microsoft\windows\currentversion\policies\system\enablelua

3. Unnecessary Services Disabled

1. Telnet Service must be disabled


This test assesses whether the following service is disabled and stopped: Telnet

 Passed with a score of 1.0

Rule requires that All conditions pass. All 2 tests of this condition in the time period passed.
Passes were: 'service[TIntSvr].startmode' value must be equal to Disabled. Value was [No data collected]
'service[TIntSvr].state' value must be equal to stopped. Value was [No data collected]

2. Remote Registry Service must be disabled

This test assesses whether the following service is disabled and stopped: Remote Registry

 Partial pass with a score of 0.50

Rule requires that All conditions pass. 1 of the 2 tests in the time period failed. Failures were: 'service[RemoteRegistry].startmode' value must be equal to Disabled. At 16/12/2010 15:01:26 value was 'Manual' for RemoteRegistry

3. Computer Browser Service must be disabled

This test assesses whether the following service is disabled and stopped: Computer Browser

 Failed with a score of 0

Rule requires that All conditions pass. 2 of the 2 tests in the time period failed. Failures were: 'service[Browser].startmode' value must be equal to Disabled. At 16/12/2010 15:01:26 value was 'Manual' for Browser
'service[Browser].state' value must be equal to stopped. At 16/12/2010 15:01:26 value was 'running' for Browser

4. Remote Access Service must be disabled


This test assesses whether the following service is disabled and stopped: RemoteAccess (Routing and Remote Access)

 Passed with a score of 1.0

Rule requires that All conditions pass. All 2 tests of this condition in the time period passed.
Passes were: 'service[RemoteAccess].startmode' value must be equal to Disabled. At 16/12/2010 15:01:26 value was 'Disabled' for RemoteAccess
'service[RemoteAccess].state' value must be equal to stopped. At 16/12/2010 15:01:26 value was 'stopped' for RemoteAccess

5. Internet Connection Sharing Service must be disabled

This test assesses whether Internet Connection Sharing is disabled and stopped by checking that the SharedAccess (Internet Connection Sharing) service is disabled.

 Passed with a score of 1.0

Rule requires that All conditions pass. All 2 tests of this condition in the time period passed.
Passes were: 'service[SharedAccess].startmode' value must be equal to Disabled. At 16/12/2010 15:01:26 value was 'Disabled' for SharedAccess
'service[SharedAccess].state' value must be equal to stopped. At 16/12/2010 15:01:26 value was 'stopped' for SharedAccess

6. FTP Publishing Service Service must be disabled

This test assesses whether the following service is disabled and stopped: FTP Publishing Service

 Passed with a score of 1.0

Rule requires that All conditions pass. All 2 tests of this condition in the time period passed.
Passes were: 'service[MSFtpsvc].startmode' value must be equal to Disabled. Value was [No data collected]
'service[MSFtpsvc].state' value must be equal to stopped. Value was [No data collected]

7. World Wide Web Publishing Service must be disabled


This test assesses whether the following service is disabled and stopped: World Wide Web Publishing Service

 Failed with a score of 0

Rule requires that All conditions pass. 2 of the 2 tests in the time period failed. Failures were:
'service[W3SVC].startmode' value must be equal to Disabled. At 16/12/2010 15:01:26 value was 'Auto' for W3SVC
'service[W3SVC].state' value must be equal to stopped. At 16/12/2010 15:01:26 value was 'running' for W3SVC

8. Fax Service must be disabled


This test assesses whether the following service is disabled and stopped: Fax Service

 Partial pass with a score of 0.50

Rule requires that All conditions pass. 1 of the 2 tests in the time period failed. Failures were:
'service[Fax].startmode' value must be equal to Disabled. At 16/12/2010 15:01:26 value was 'Manual' for Fax

9. SNMP Trap Service must be disabled


This test assesses whether the following service is disabled and stopped: SNMP Trap

 Partial pass with a score of 0.50

Rule requires that All conditions pass. 1 of the 2 tests in the time period failed. Failures were: 'service[SNMPTRAP].startmode' value must be equal to Disabled. At 16/12/2010 15:01:26 value was 'Manual' for SNMPTRAP

10. Terminal Services Service must be disabled


This test assesses whether the following service is disabled and stopped: Terminal Services

 Failed with a score of 0

Rule requires that All conditions pass. 2 of the 2 tests in the time period failed. Failures were: 'service[TermService].startmode' value must be equal to Disabled. At 16/12/2010 15:01:26 value was 'Manual' for TermService
'service[TermService].state' value must be equal to stopped. At 16/12/2010 15:01:26 value was 'running' for TermService

11. Telephony Service must be disabled


This test assesses whether the following service is disabled and stopped: Telephony

 Partial pass with a score of 0.50

Rule requires that All conditions pass. 1 of the 2 tests in the time period failed. Failures were: 'service[TapiSrv].startmode' value must be equal to Disabled. At 16/12/2010 15:01:26 value was 'Manual' for TapiSrv

12. Remote Access Connection Manager Service must be disabled

This test assesses whether the following service is disabled and stopped: Remote Access Connection Manager

 Partial pass with a score of 0.50

Rule requires that All conditions pass. 1 of the 2 tests in the time period failed. Failures were: 'service[RasMan].startmode' value must be equal to Disabled. At 16/12/2010 15:01:26 value was 'Manual' for RasMan

13. Print Spooler Service must be disabled

This test assesses whether the following service is disabled and stopped: Print Spooler

 Failed with a score of 0

Rule requires that All conditions pass. 2 of the 2 tests in the time period failed. Failures were: 'service[Spooler].startmode' value must be equal to Disabled. At 16/12/2010 15:01:26 value was 'Auto' for Spooler
'service[Spooler].state' value must be equal to stopped. At 16/12/2010 15:01:26 value was 'running' for Spooler

***** SAMPLE REPORT TRUNCATED *****

We hope you found this sample compliance report of interest and if you would now like to see the full PCI DSS report or compliance reports for other security standards then please contact us at

info@newnettechnologies.com

Thank you!



NNT Change Tracker Enterprise awarded a maximum 5 out of 5 stars
by Secure Computing Magazine

