

Security Audit Report

Policy Evaluation - Windows Servers

Audited on August 02 2005, August 02 2005

Reported on August 04 2005

1. Policy Evaluations

1.1. Policy Evaluation for 192.168.8.101

An in-depth policy evaluation was performed against 192.168.8.101 using the security policy "Default Security Settings. Requires environment vars DSDIT DSLOG and SYSVOL be set. Must be joined to a domain in order to open. User Rights\Restricted Groups not included. (Windows 2000 DCs)". The system is not in conformance with the policy. A total of 22 policy elements were found to be in violation on the system, and an additional 5 policy elements could not be evaluated due to errors.

Policy element	Result	Additional information
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NTDS	Conforms	Key does not exist
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Non-Driver Signing	Conforms	Key does not exist
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseCertificates	Conforms	Key does not exist
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Driver Signing	Conforms	Key does not exist
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor	Conforms	Key does not exist
%SystemRoot%\Debug\UserMode	Conforms	Directory C:\WINNT\Debug\UserMode does not exist.
c:\ntbootdd.sys	Conforms	c:\ntbootdd.sys does not exist.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider	Skipped	Not configured
%SystemRoot%\Installer	Skipped	Not configured
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature	Violation	Value not present, should be 1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole	Violation	SD flags are "DaclAutoInheritReq", should be "DaclProtected"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetDDE	Violation	SD flags are "DaclAutoInheritReq", should be "DaclProtected"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	Violation	SD flags are "DaclAutoInheritReq", should be "DaclProtected"
HKEY_LOCAL_MACHINE\SOFTWARE\Classes	Violation	The ACL for HKEY_LOCAL_MACHINE\SOFTWARE\Classes is (AccessAllowed;ContainerInherit;ReadControl Read Execute;;;Everyone)(AccessAllowed;ContainerInherit;ReadControl StandardDelete Read Write

Security Audit Report

Policy element	Result	Additional information
		Execute;;;INTERACTIVE)(AccessAllowed;ContainerInherit;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;Administrators)(AccessAllowed;ContainerInherit;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;SYSTEM)(AccessAllowed;ContainerInherit;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;Administrators), which does not match (AccessAllowed;ContainerInherit;GenericRead;;;Everyone)
HKEY_LOCAL_MACHINE\SOFTWARE	Violation	SD flags are "DaclAutoInheritReq", should be "DaclProtected"
%SystemRoot%\explorer.exe	Violation	The ACL for %SystemRoot%\explorer.exe is (AccessAllowed;ObjectInherit ContainerInherit;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;Administrators)(AccessAllowed;ObjectInherit ContainerInherit;ReadControl Read Execute;;;Everyone)(AccessAllowed;ObjectInherit ContainerInherit;ReadControl StandardDelete Read Write Execute;;;Server Operators)(AccessAllowed;ObjectInherit ContainerInherit;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;SYSTEM), which does not match (AccessAllowed;GenericRead GenericExecute;;;Everyone)
%SystemRoot%	Violation	SD flags are "DaclAutoInheritReq", should be "DaclProtected"
%ProgramFiles%	Violation	SD flags are "DaclAutoInheritReq", should be "DaclProtected"
c:\config.sys	Violation	SD flags are "", should be "DaclProtected"
c:\autoexec.bat	Violation	SD flags are "", should be "DaclProtected"
c:\ntldr	Violation	SD flags are "DaclAutoInheritReq", should be "DaclProtected"
c:\ntdetect.com	Violation	SD flags are "DaclAutoInheritReq", should be "DaclProtected"
c:\boot.ini	Violation	SD flags are "DaclAutoInheritReq", should be "DaclProtected"
Do not allow the utl_file package to access directories containing sensitive information (e.g. Oracle config files, trace files, core dump trace files). A value of "*" allows access to any file.	Conforms	utl_file_dir is set to and utl_file_dir is set to

Security Audit Report

Policy element	Result	Additional information
Do not allow roles to be set outside the database. This ensures that Oracle roles and OS roles are managed and granted separately (e.g. keeping Domain admins and Oracle DBA's separate).	Conforms	os_roles is set to FALSE
Do not trust remote client's operating system to assign the user's roles, otherwise users could effectively grant themselves any role.	Conforms	remote_os_roles is set to FALSE
Do not trust remote client's operating system to authenticate users, otherwise users could log in with no password.	Conforms	remote_os_authent is set to FALSE
Ensure that Oracle will check the name of a database link is the same as that of a remote database.	Conforms	global_names is set to TRUE
Profile '%'	Error	Error processing profile limit element: Invalid column index
Profile '%'	Error	Error processing profile limit element: Invalid column index
Profile '%'	Error	Error processing profile limit element: Invalid column index
Profile '%'	Error	Error processing profile limit element: Invalid column index
Profile '%'	Error	Error processing profile limit element: Invalid column index
Ensure that the fixed_date parameter is not being used. If fixed_date is set to a particular date, then the SYSDATE procedure will always return this date instead of the current time/date. The fixed_date parameter is only used for debugging and if it is set, it can indicate that someone is trying to interfere with calculations involving the date.	Violation	fixed_date is set to empty value found, expected
Ensure that Oracle enforces resource limits as specified in user profiles. If resource_limit is set to FALSE, Oracle will not enforce the resource limits that have been defined in user profiles.	Violation	resource_limit is set to FALSE (expected TRUE)
Require SELECT privileges on a table	Violation	sql92_security is set to FALSE (expected TRUE)

Security Audit Report

Policy element	Result	Additional information
are required to execute UPDATE or DELETE statements that use WHERE clauses. If SQL92 security is not enabled, then a user can figure out which values they are not allowed to see, which somewhat defeats the purpose of restricting them.		
Ensure that password encryption is enabled for database links. When Oracle attempts to connect to a remote database, it first sends the encrypted password. If this fails, Oracle sends the unencrypted password. This behavior is intended to preserve the ability to connect to Oracle servers older than v7.2, which do not support encryption.	Violation	dblink_encrypt_login is set to FALSE (expected TRUE)
Do not allow accounts to be used externally unless the user is created by explicitly using IDENTIFIED EXTERNALLY.	Violation	os_authent_prefix is set to empty value found, expected
Ensure that basic auditing is performed. For critical environments or for HIPAA/SOX/GLB environments, a value of OS is recommended because it is easier to preserve and secure the audit trail data (otherwise the audit trail data is stored in the database itself and could be modified by the DBA).	Violation	audit_trail is set to NONE (expected OS) or audit_trail is set to NONE (expected DB) or audit_trail is set to NONE (expected TRUE)
Prevent the use of a TNS Listener on a remote system. Using remote listeners is an obscure feature that is typically only needed in a multi-master replication environment.	Violation	remote_listener is not present as a configuration parameter
Limit the maximum number of enabled roles a user can have in their security domain at one time.	Violation	max_enabled_roles is set to 30 (expected 20)

1.2. Policy Evaluation for 192.168.8.110

An in-depth policy evaluation was performed against 192.168.8.110 using the security policy "Default Security Settings. User Rights\Restricted Groups not included. (Windows 2000 Server)". The system is not in conformance with the policy. A total of 5 policy elements were found to be in violation on the system, and an additional 2 policy elements could not be evaluated due to errors.

Security Audit Report

Policy element	Result	Additional information
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel	Conforms	Value is 1, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount	Conforms	Value is 10, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect	Conforms	Value is 15, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateF	Conforms	Value is 0, as expected

Security Audit Report

Policy element	Result	Additional information
loppies		
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel	Conforms	Value is 1, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption	Conforms	Value is , as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing	Conforms	Value is 00, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff	Conforms	Value is 1, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature	Conforms	Value is 1, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon>PasswordExpiryWarning	Conforms	Value is 14, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session	Conforms	Value is 1, as expected

Security Audit Report

Policy element	Result	Additional information
Manager\ProtectionMode		
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText	Conforms	Value is , as expected
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole	Conforms	ACLs match
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetDDE	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetDDE	Conforms	ACLs match
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Non-Driver Signing	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Non-Driver Signing	Conforms	ACLs match
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseCertificates	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseCertificates	Conforms	ACLs match
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Driver Signing	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE	Conforms	ACLs match

Security Audit Report

Policy element	Result	Additional information
E\Microsoft\Driver Signing		
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	Conforms	ACLs match
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor	Conforms	ACLs match
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\hlp	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\hlp	Conforms	ACLs match
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\helpfile	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\helpfile	Conforms	ACLs match
HKEY_LOCAL_MACHINE\Software\Classes	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\Software\Classes	Conforms	ACLs match
HKEY_LOCAL_MACHINE\Software	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\Software	Conforms	ACLs match
%SystemRoot%	Conforms	Object ACLs are compatible
%SystemRoot%	Conforms	ACLs match
%ProgramFiles%	Conforms	Object ACLs are compatible
%ProgramFiles%	Conforms	ACLs match
c:\ntbootdd.sys	Conforms	c:\ntbootdd.sys does not exist.
c:\ntldr	Conforms	Object ACLs are compatible
c:\ntldr	Conforms	ACLs match
c:\ntdetect.com	Conforms	Object ACLs are compatible
c:\ntdetect.com	Conforms	ACLs match
c:\boot.ini	Conforms	Object ACLs are compatible
c:\boot.ini	Conforms	ACLs match
MaximumPasswordAge	Conforms	Maximum password age is 42, as expected
LockoutBadCount	Conforms	Lockout bad count is 0, as expected

Security Audit Report

Policy element	Result	Additional information
RequireLogonToChangePassword	Conforms	Require logon to change password is 0, as expected
MinimumPasswordLength	Conforms	Minimum password length is 0, as expected
MinimumPasswordAge	Conforms	Minimum password age is 0, as expected
PasswordHistorySize	Conforms	Password history size is 0, as expected
PasswordComplexity	Error	Cannot check password complexity settings for the domain
ClearTextPassword	Error	Cannot check clear text password settings for the domain
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider	Skipped	Not configured
%SystemRoot%\CSC	Skipped	Not configured
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon	Violation	Value is 1, should be 0
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers	Violation	Value is 0, should be 1
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD	Violation	Value not present, should be 0
c:\config.sys	Violation	SD flags are "", should be "DaclProtected"
c:\autoexec.bat	Violation	SD flags are "", should be "DaclProtected"

1.3. Policy Evaluation for 192.168.8.115

An in-depth policy evaluation was performed against 192.168.8.115 using the security policy "Default Security Settings. User Rights\Restricted Groups not included. (Windows 2000 Server)". The system is not in conformance with the policy. A total of 5 policy elements were found to be in violation on the system, and an additional 2 policy elements could not be evaluated due to errors.

Policy element	Result	Additional information
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Para	Conforms	Value is 0, as expected

Security Audit Report

Policy element	Result	Additional information
meters\RequireSignOrSeal		
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel	Conforms	Value is 1, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount	Conforms	Value is 10, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect	Conforms	Value is 15, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel	Conforms	Value is 1, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand	Conforms	Value is 0, as expected

Security Audit Report

Policy element	Result	Additional information
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption	Conforms	Value is , as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing	Conforms	Value is 00, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff	Conforms	Value is 1, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature	Conforms	Value is 1, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon>PasswordExpiryWarning	Conforms	Value is 14, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\ProtectionMode	Conforms	Value is 1, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects	Conforms	Value is 0, as expected

Security Audit Report

Policy element	Result	Additional information
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel	Conforms	Value is 0, as expected
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText	Conforms	Value is , as expected
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole	Conforms	ACLs match
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetDDE	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetDDE	Conforms	ACLs match
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Non-Driver Signing	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Non-Driver Signing	Conforms	ACLs match
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseCertificates	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseCertificates	Conforms	ACLs match
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Driver Signing	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Driver Signing	Conforms	ACLs match
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	Conforms	ACLs match
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE	Conforms	ACLs match

Security Audit Report

Policy element	Result	Additional information
E:\Microsoft\Command Processor		
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\hlp	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\hlp	Conforms	ACLs match
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\helpfile	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\helpfile	Conforms	ACLs match
HKEY_LOCAL_MACHINE\Software\Classes	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\Software\Classes	Conforms	ACLs match
HKEY_LOCAL_MACHINE\Software	Conforms	Object ACLs are compatible
HKEY_LOCAL_MACHINE\Software	Conforms	ACLs match
%SystemRoot%	Conforms	Object ACLs are compatible
%SystemRoot%	Conforms	ACLs match
%ProgramFiles%	Conforms	Object ACLs are compatible
%ProgramFiles%	Conforms	ACLs match
c:\ntbootdd.sys	Conforms	c:\ntbootdd.sys does not exist.
c:\ntldr	Conforms	Object ACLs are compatible
c:\ntldr	Conforms	ACLs match
c:\ntdetect.com	Conforms	Object ACLs are compatible
c:\ntdetect.com	Conforms	ACLs match
c:\boot.ini	Conforms	Object ACLs are compatible
c:\boot.ini	Conforms	ACLs match
MaximumPasswordAge	Conforms	Maximum password age is 42, as expected
LockoutBadCount	Conforms	Lockout bad count is 0, as expected
RequireLogonToChangePassword	Conforms	Require logon to change password is 0, as expected
MinimumPasswordLength	Conforms	Minimum password length is 0, as expected
MinimumPasswordAge	Conforms	Minimum password age is 0, as expected
PasswordHistorySize	Conforms	Password history size is 0, as expected
PasswordComplexity	Error	Cannot check password complexity settings for the domain
ClearTextPassword	Error	Cannot check clear text password settings for the

Security Audit Report

Policy element	Result	Additional information
		domain
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider	Skipped	Not configured
%SystemRoot%\CSC	Skipped	Not configured
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon	Violation	Value is 1, should be 0
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers	Violation	Value is 0, should be 1
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD	Violation	Value not present, should be 0
c:\config.sys	Violation	SD flags are "", should be "DaclProtected"
c:\autoexec.bat	Violation	SD flags are "", should be "DaclProtected"

1.4. Policy Evaluation for 10.1.30.11

An in-depth policy evaluation was performed against 10.1.30.11 using the security policy "Default Security Settings. Requires environment vars DSDIT DSLOG and SYSVOL be set. Must be joined to a domain in order to open. User Rights\Restricted Groups not included. (Windows 2000 DCs)".

Policy element	Result	Additional information
c:\ntbootdd.sys	Conforms	c:\ntbootdd.sys does not exist.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider	Skipped	Not configured
%SystemRoot%\Installer	Skipped	Not configured
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature	Violation	Value is 0, should be 1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole	Violation	The ACL for HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole is (AccessAllowed;ContainerInherit;GenericRead;;;Users)(AccessAllowed;ContainerInherit;GenericRead;;;S-1-5-32-547)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ContainerInherit;GenericAll;;;Ad

Security Audit Report

Policy element	Result	Additional information
		ministrators), which does not match (AccessAllowed;ContainerInherit;GenericRead;;;Authenticated Users)(AccessAllowed;ContainerInherit;GenericRead;;;Server Operators)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NTDS	Violation	SD flags are "DaclAutoInheritReq DaclAutoInherited", should be "DaclProtected"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetDDE	Violation	The ACL for HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetDDE is (AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators), which does not match (AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Non-Driver Signing	Violation	The ACL for HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Non-Driver Signing is (AccessAllowed;ContainerInherit;GenericRead;;;Users)(AccessAllowed;ContainerInherit;GenericRead;;;S-1-5-32-547)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators), which does not match (AccessAllowed;ContainerInherit;GenericRead;;;Authenticated Users)(AccessAllowed;ContainerInherit;GenericRead;;;Server Operators)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseCertificates	Violation	The ACL for HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseCertificates is (AccessAllowed;ContainerInherit;GenericRead;;;Users)(AccessAllowed;ContainerInherit;GenericRead;;;S-1-5-32-547)(AccessAllowed;ContainerInherit;GenericAll;;;Admini

Security Audit Report

Policy element	Result	Additional information
		<p>strators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators), which does not match (AccessAllowed;ContainerInherit;GenericRead;;;Authenticated Users)(AccessAllowed;ContainerInherit;GenericRead;;;Server Operators)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)</p>
<p>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Driver Signing</p>	<p>Violation</p>	<p>The ACL for HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Driver Signing is (AccessAllowed;ContainerInherit;GenericRead;;;Users)(AccessAllowed;ContainerInherit;GenericRead;;;S-1-5-32-547)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators), which does not match (AccessAllowed;ContainerInherit;GenericRead;;;Authenticated Users)(AccessAllowed;ContainerInherit;GenericRead;;;Server Operators)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)</p>
<p>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography</p>	<p>Violation</p>	<p>The ACL for HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography is (AccessAllowed;ContainerInherit;GenericRead;;;Users)(AccessAllowed;ContainerInherit;GenericRead;;;S-1-5-32-547)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators), which does not match (AccessAllowed;ContainerInherit;GenericRead;;;Authenticated Users)(AccessAllowed;ContainerInherit;GenericRead;;;Server Operators)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)</p>

Security Audit Report

Policy element	Result	Additional information
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor	Violation	<p>The ACL for HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor is (AccessAllowed;ContainerInherit;GenericRead;;;Users)(AccessAllowed;ContainerInherit;GenericRead;;;S-1-5-32-547)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators), which does not match (AccessAllowed;ContainerInherit;GenericRead;;;AuthenticatedUsers)(AccessAllowed;ContainerInherit;GenericRead;;;ServerOperators)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)</p>
HKEY_LOCAL_MACHINE\SOFTWARE\Classes	Violation	<p>The ACL for HKEY_LOCAL_MACHINE\SOFTWARE\Classes is (AccessAllowed;ContainerInherit;GenericRead;;;Users)(AccessAllowed;ContainerInherit;GenericReadGenericWrite StandardDelete;;;S-1-5-32-547)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators), which does not match (AccessAllowed;ContainerInherit;GenericRead;;;Everyone)</p>
HKEY_LOCAL_MACHINE\SOFTWARE	Violation	<p>The ACL for HKEY_LOCAL_MACHINE\SOFTWARE is (AccessAllowed;ContainerInherit;GenericRead;;;Users)(AccessAllowed;ContainerInherit;GenericReadGenericWrite StandardDelete;;;S-1-5-32-547)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericReadGenericWrite StandardDelete;;;TERMINAL SERVER USER), which does not match (AccessAllowed;ContainerInherit;GenericRead;;;AuthenticatedUsers)(AccessAllowed;ContainerInherit;GenericReadGenericWrite StandardDelete;;;ServerOperators)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ContainerInherit;GenericAll;;;Administrators)</p>

Security Audit Report

Policy element	Result	Additional information
%SystemRoot%\explorer.exe	Violation	The ACL for %SystemRoot%\explorer.exe is (AccessAllowed;;ReadControl Read Execute;;;Users)(AccessAllowed;;ReadControl Read Execute;;;S-1-5-32-547)(AccessAllowed;;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;Administrators)(AccessAllowed;;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;SYSTEM), which does not match (AccessAllowed;;GenericRead GenericExecute;;;Everyone)
%SystemRoot%\Debug\UserMode	Violation	The ACL for %SystemRoot%\Debug\UserMode is (AccessAllowed;;;;;Users)(AccessAllowed;ObjectInherit InheritOnly;;;;;Users)(AccessAllowed;ObjectInherit ContainerInherit;GenericRead GenericWrite GenericExecute StandardDelete;;;S-1-5-32-547)(AccessAllowed;ObjectInherit ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ObjectInherit ContainerInherit;GenericAll;;;SYSTEM), which does not match (AccessAllowed;ObjectInherit InheritOnly;;;;;Authenticated Users)(AccessAllowed;ObjectInherit ContainerInherit;GenericRead GenericWrite GenericExecute StandardDelete;;;Server Operators)(AccessAllowed;ObjectInherit ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ObjectInherit ContainerInherit;GenericAll;;;SYSTEM)
%SystemRoot%	Violation	The ACL for %SystemRoot% is (AccessAllowed;ObjectInherit ContainerInherit;GenericRead GenericExecute;;;Users)(AccessAllowed;ObjectInherit ContainerInherit;GenericRead GenericWrite GenericExecute StandardDelete;;;S-1-5-32-547)(AccessAllowed;ObjectInherit ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ObjectInherit ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed; ObjectInherit ContainerInherit;GenericAll;;;Administrators), which does not match (AccessAllowed;ObjectInherit ContainerInherit;GenericRead GenericExecute;;;Authenticated Users)(AccessAllowed;ObjectInherit ContainerInherit;GenericRead GenericWrite GenericExecute StandardDelete;;;Server Operators)(AccessAllowed;ObjectInherit

Security Audit Report

Policy element	Result	Additional information
		<p>ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ObjectInherit</p> <p>ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ObjectInherit</p> <p>ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;;GenericRead GenericExecute;;;Everyone)</p>
%ProgramFiles%	Violation	<p>The ACL for %ProgramFiles% is (AccessAllowed;ObjectInherit ContainerInherit;GenericRead GenericExecute;;;Users)(AccessAllowed;ObjectInherit ContainerInherit;GenericRead GenericWrite GenericExecute StandardDelete;;;S-1-5-32-547)(AccessAllowed;ObjectInherit ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ObjectInherit ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ObjectInherit ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ObjectInherit ContainerInherit;GenericRead GenericWrite GenericExecute StandardDelete;;;TERMINAL SERVER USER), which does not match (AccessAllowed;ObjectInherit ContainerInherit;GenericRead GenericExecute;;;Authenticated Users)(AccessAllowed;ObjectInherit ContainerInherit;GenericRead GenericWrite GenericExecute StandardDelete;;;Server Operators)(AccessAllowed;ObjectInherit ContainerInherit;GenericAll;;;Administrators)(AccessAllowed;ObjectInherit ContainerInherit;GenericAll;;;SYSTEM)(AccessAllowed;ObjectInherit ContainerInherit;GenericAll;;;Administrators)</p>
c:\config.sys	Violation	<p>The ACL for c:\config.sys is (AccessAllowed;;ReadControl Read Execute;;;Users)(AccessAllowed;;ReadControl StandardDelete Read Write Execute;;;S-1-5-32-547)(AccessAllowed;;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;Administrators)(AccessAllowed;;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;SYSTEM), which does not match (AccessAllowed;;GenericRead GenericExecute;;;Authenticated Users)(AccessAllowed;;GenericRead GenericWrite GenericExecute StandardDelete;;;Server Operators)(AccessAllowed;;GenericAll;;;Administrators)(</p>

Security Audit Report

Policy element	Result	Additional information
		AccessAllowed;;GenericAll;;;SYSTEM)
c:\autoexec.bat	Violation	The ACL for c:\autoexec.bat is (AccessAllowed;;ReadControl Read Execute;;;Users)(AccessAllowed;;ReadControl StandardDelete Read Write Execute;;;S-1-5-32-547)(AccessAllowed;;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;Administrators)(AccessAllowed;;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;SYSTEM), which does not match (AccessAllowed;;GenericRead GenericExecute;;;Authenticated Users)(AccessAllowed;;GenericRead GenericWrite GenericExecute StandardDelete;;;Server Operators)(AccessAllowed;;GenericAll;;;Administrators)(AccessAllowed;;GenericAll;;;SYSTEM)
c:\ntldr	Violation	The ACL for c:\ntldr is (AccessAllowed;;ReadControl Read Execute;;;S-1-5-32-547)(AccessAllowed;;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;Administrators)(AccessAllowed;;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;SYSTEM), which does not match (AccessAllowed;;GenericRead GenericWrite GenericExecute StandardDelete;;;Server Operators)(AccessAllowed;;GenericAll;;;Administrators)(AccessAllowed;;GenericAll;;;SYSTEM)
c:\ntdetect.com	Violation	The ACL for c:\ntdetect.com is (AccessAllowed;;ReadControl Read Execute;;;S-1-5-32-547)(AccessAllowed;;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;Administrators)(AccessAllowed;;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;SYSTEM), which does not match (AccessAllowed;;GenericRead GenericWrite GenericExecute StandardDelete;;;Server Operators)(AccessAllowed;;GenericAll;;;Administrators)(AccessAllowed;;GenericAll;;;SYSTEM)
c:\boot.ini	Violation	The ACL for c:\boot.ini is (AccessAllowed;;ReadControl Read Execute;;;S-1-5-32-547)(AccessAllowed;;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;Administrators)(AccessAllowed;;WriteOwner WriteDACL ReadControl StandardDelete FullAccess;;;SYSTEM), which does not match (AccessAllowed;;GenericRead GenericWrite

Security Audit Report

Policy element	Result	Additional information
		GenericExecute StandardDelete;;;Server Operators)(AccessAllowed;;GenericAll;;;Administrators)(AccessAllowed;;GenericAll;;;SYSTEM)