datalinknetworks

Security Assessment

Security Policy Assessment

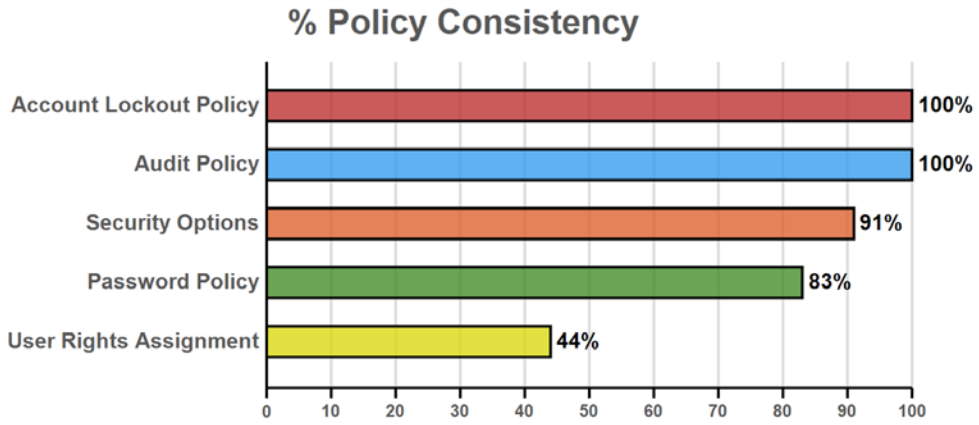
Prepared for: Jonathan Doe
Prepared by: Austin Archer

3/23/2018

Scan Date: 4/1/2014

Table of Contents

1 - Summary



1.1 - Sampled Systems

IP Addresses	Computer Name	Operating System
10.0.7.28	tandem	Windows 7 Enterprise
172.20.1.3, 10.0.1.3	DC01	Windows Server 2012 Standard

2 - Local Security Settings (Sampled Systems)

2.1 - Account Policies

2.1.1 - Password Policy

Policy	Setting	Computers
Enforce password history	0 passwords remembered	TANDEM
	24 passwords remembered	DC01
Maximum password age	42 days	All Sampled
Minimum password age	1 days	All Sampled
Minimum password length	7 characters	All Sampled
Password must meet complexity requirements	Enabled	All Sampled
Store passwords using reversible encryption	Disabled	All Sampled

2.1.2 - Account Lockout Policy

Policy	Setting	Computers
Account lockout duration	Not Applicable	All Sampled
Account lockout threshold	Disabled	All Sampled
Reset account lockout counter after	Not Applicable	All Sampled

2.2 - Local Policies

2.2.1 - Audit Policy

Policy	Setting	Computers
Audit account logon events	No auditing	All Sampled
Audit account management	No auditing	All Sampled
Audit directory service access	No auditing	All Sampled
Audit logon events	No auditing	All Sampled
Audit object access	No auditing	All Sampled
Audit policy change	No auditing	All Sampled
Audit privilege use	No auditing	All Sampled
Audit process tracking	No auditing	All Sampled
Audit system events	No auditing	All Sampled

2.2.2 - User Rights Assignment

Policy	Setting	Computers
Access this computer from the network	Everyone,Administrators	TANDEM
	Everyone,Authenticated Users,Administrators,Pre-Windows 2000 Compatible Access,ENTERPRISE DOMAIN CONTROLLERS	DC01
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,SQLServer2005MSSQLUser$tandem$SQLEXPRESS,Administrators	TANDEM
	LOCAL SERVICE,NETWORK SERVICE,Administrators,*S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,*S-1-5-82-604604840-3341247844-1790606609-4006251754-2470522317	DC01
Allow log on locally	Everyone,PIT\Domain Admins,Administrators	TANDEM
	Administrators,Account Operators,Server Operators,Print Operators,Backup Operators	DC01

Policy	Setting	Computers
Allow log on through Remote Desktop Services	Administrators,Remote Desktop Users	TANDEM
	Administrators	DC01
Back up files and directories	Administrators,Backup Operators	TANDEM
	Administrators,Server Operators,Backup Operators	DC01
Bypass traverse checking	Everyone,LOCAL SERVICE,NETWORK SERVICE,SQLServer2005MSSQLUser$tandem$SQLEXPRESS,Administrators,Users,Backup Operators	TANDEM
	Everyone,Authenticated Users,LOCAL SERVICE,NETWORK SERVICE,Administrators,Pre-Windows 2000 Compatible Access	DC01
Change the system time	LOCAL SERVICE,Administrators	TANDEM
	LOCAL SERVICE,Administrators,Server Operators	DC01
Change the time zone	LOCAL SERVICE,Administrators,Users	TANDEM
	LOCAL SERVICE,Administrators,Server Operators	DC01
Create a pagefile	Administrators	All Sampled
Create global objects	LOCAL SERVICE,NETWORK SERVICE,Administrators,SERVICE	All Sampled
Create symbolic links	Administrators	All Sampled
Debug programs	Administrators	All Sampled
Deny access to this computer from the network	Guest	TANDEM
Deny log on locally	Guest	TANDEM
Force shutdown from a remote system	Administrators	TANDEM
	Administrators,Server Operators	DC01
Generate security audits	LOCAL SERVICE,NETWORK SERVICE	TANDEM
	LOCAL SERVICE,NETWORK SERVICE,*S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,*S-1-5-82-604604840-3341247844-1790606609-4006251754-2470522317	DC01
Impersonate a client after authentication	LOCAL SERVICE,NETWORK SERVICE,Administrators,SERVICE	All Sampled

Policy	Setting	Computers
Increase a process working set	Users	TANDEM
	Users,Window Manager\Window Manager Group	DC01
Increase scheduling priority	Administrators	All Sampled
Load and unload device drivers	Administrators	TANDEM
	Administrators,Print Operators	DC01
Log on as a batch job	SQLServer2005MSSQLUser$tandem$SQLEXPRESS,Administrators,Backup Operators,internal Log Users	TANDEM
	Administrators,Backup Operators,internal Log Users	DC01
Log on as a service	SQLServer2005SQLBrowserUser$tandem,SQLServer2005MSSQLUser$tandem$SQLEXPRESS,NT SERVICE\ALL SERVICES	TANDEM
	NT SERVICE\ALL SERVICES	DC01
Manage auditing and security log	Administrators	TANDEM
	Exchange Servers,Administrators	DC01
Modify firmware environment values	Administrators	All Sampled
Perform volume maintenance tasks	Administrators	All Sampled
Profile single process	Administrators	All Sampled
Profile system internal	Administrators,NT SERVICE\WdiServiceHost	All Sampled
Remove computer from docking station	Administrators,Users	TANDEM
	Administrators	DC01
Replace a process level token	LOCAL SERVICE,NETWORK SERVICE,SQLServer2005MSSQLUser$tandem$SQLEXPRESS	TANDEM
	LOCAL SERVICE,NETWORK SERVICE,*S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,*S-1-5-82-604604840-3341247844-1790606609-4006251754-2470522317	DC01
Restore files and directories	Administrators,Backup Operators	TANDEM
	Administrators,Server Operators,Backup Operators	DC01
Shut down the system	Administrators,Users,Backup Operators	TANDEM

Policy	Setting	Computers
	Administrators,Server Operators,Print Operators,Backup Operators	DC01
Take ownership of files or other objects	Administrators	All Sampled
Add workstations to domain	Authenticated Users	DC01
Enable computer and user accounts to be trusted for delegation	Administrators	DC01

2.2.3 - Security Options

Policy	Setting	Computers
Accounts: Administrator account status	Disabled	TANDEM
	Enabled	DC01
Accounts: Guest account status	Disabled	All Sampled
Accounts: Limit local account use of blank passwords to console logon only	Enabled	All Sampled
Accounts: Rename administrator account	Administrator	All Sampled
Accounts: Rename guest account	Guest	All Sampled
Audit: Audit the access of global system objects	Disabled	All Sampled
Audit: Audit the use of Backup and Restore privilege	Disabled	All Sampled
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Not Defined	All Sampled
Audit: Shut down system immediately if unable to log security audits	Disabled	All Sampled
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined	All Sampled
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined	All Sampled
Devices: Allow undock without having to log on	Enabled	All Sampled

Policy	Setting	Computers
Devices: Allowed to format and eject removable media	Not Defined	All Sampled
Devices: Prevent users from installing printer drivers	Disabled	TANDEM
	Enabled	DC01
Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined	All Sampled
Devices: Restrict floppy access to locally logged-on user only	Not Defined	All Sampled
Domain controller: Allow server operators to schedule tasks	Not Defined	All Sampled
Domain controller: LDAP server signing requirements	Not Defined	TANDEM
	None	DC01
Domain controller: Refuse machine account password changes	Not Defined	All Sampled
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	All Sampled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	All Sampled
Domain member: Digitally sign secure channel data (when possible)	Enabled	All Sampled
Domain member: Disable machine account password changes	Disabled	All Sampled
Domain member: Maximum machine account password age	30 days	All Sampled
Domain member: Require strong (Windows 2000 or later) session key	Enabled	All Sampled
Interactive logon: Display user information when the session is locked	Not Defined	All Sampled
Interactive logon: Do not display last user name	Disabled	All Sampled
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined	TANDEM
	Disabled	DC01
Interactive logon: Number of previous logons to	10 logons	All Sampled

Policy	Setting	Computers
cache (in case domain controller is not available)		
Interactive logon: Prompt user to change password before expiration	5 days	All Sampled
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled	All Sampled
Interactive logon: Require smart card	Disabled	All Sampled
Interactive logon: Smart card removal behavior	No Action	All Sampled
Microsoft network client: Digitally sign communications (always)	Disabled	All Sampled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	All Sampled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	All Sampled
Microsoft network server: Amount of idle time required before suspending session	15 minutes	All Sampled
Microsoft network server: Digitally sign communications (always)	Disabled	TANDEM
	Enabled	DC01
Microsoft network server: Digitally sign communications (if client agrees)	Disabled	TANDEM
	Enabled	DC01
Microsoft network server: Disconnect clients when logon hours expire	Enabled	All Sampled
Microsoft network server: Server SPN target name validation level	Not Defined	All Sampled
Network access: Allow anonymous SID/Name translation	Disabled	All Sampled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	All Sampled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled	All Sampled
Network access: Do not allow storage of passwords and credentials for network authentication	Disabled	All Sampled

Policy	Setting	Computers
Network access: Let Everyone permissions apply to anonymous users	Disabled	All Sampled
Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions,System\CurrentControlSet\Control\Server Applications,Software\Microsoft\Windows NT\CurrentVersion	All Sampled
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSet\Control\Print\Printers,System\CurrentControlSet\Services\Eventlog,Software\Microsoft\OLAP Server,Software\Microsoft\Windows NT\CurrentVersion\Print,Software\Microsoft\Windows NT\CurrentVersion\Windows,System\CurrentControlSet\Control\ContentIndex,System\CurrentControlSet\Control\Terminal Server,System\CurrentControlSet\Control\Terminal Server\UserConfig,System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration,Software\Microsoft\Windows NT\CurrentVersion\Perflib,System\CurrentControlSet\Services\SysmonLog	All Sampled
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	All Sampled
Network access: Shares that can be accessed anonymously	Not Defined	All Sampled
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves	All Sampled
Network security: Allow Local System to use computer identity for NTLM	Not Defined	All Sampled
Network security: Allow LocalSystem NULL session fallback	Not Defined	All Sampled
Network Security: Allow PKU2U authentication requests to this computer to use online identities	Not Defined	TANDEM
Network security: Configure encryption types allowed for Kerberos	Not Defined	All Sampled
Network security: Do not store LAN Manager hash value on next password change	Enabled	All Sampled
Network security: Force logoff when logon hours expire	Disabled	All Sampled
Network security: LAN Manager authentication	Not Defined	All Sampled

Policy	Setting	Computers
level		
Network security: LDAP client signing requirements	Negotiate signing	All Sampled
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require 128-bit encryption	All Sampled
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require 128-bit encryption	All Sampled
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not Defined	All Sampled
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined	All Sampled
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined	All Sampled
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined	All Sampled
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined	All Sampled
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined	All Sampled
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined	All Sampled
Recovery console: Allow automatic administrative logon	Disabled	All Sampled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled	All Sampled
Shutdown: Allow system to be shut down without having to log on	Enabled	TANDEM
	Disabled	DC01
Shutdown: Clear virtual memory pagefile	Disabled	All Sampled
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined	All Sampled
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled	All Sampled

Policy	Setting	Computers
System objects: Require case insensitivity for non-Windows subsystems	Enabled	All Sampled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	All Sampled
System settings: Optional subsystems	Posix	All Sampled
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Disabled	All Sampled
User Account Control: Admin Approval Mode for the Built-in Administrator account	Disabled	All Sampled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled	All Sampled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent for non-Windows binaries	All Sampled
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials	All Sampled
User Account Control: Detect application installations and prompt for elevation	Enabled	All Sampled
User Account Control: Only elevate executables that are signed and validated	Disabled	All Sampled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled	All Sampled
User Account Control: Run all administrators in Admin Approval Mode	Enabled	All Sampled
User Account Control: Switch to the secure desktop when prompting for elevation	Disabled	TANDEM
	Enabled	DC01
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled	All Sampled
Accounts: Block Microsoft accounts	Not Defined	DC01
Interactive logon: Machine account lockout threshold	Not Defined	DC01

Policy	Setting	Computers
Interactive logon: Machine inactivity limit	Not Defined	DC01
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined	DC01
Network access: Named Pipes that can be accessed anonymously	,netlogon,samr,lsarpc	DC01