说明

参考CIS Benchamrk的资料 https://workbench.cisecurity.org/benchmarks/16913 共分为19个大类，每大类又划分为若干小类，下面分别来介绍。

1. Account Policies

1.1Password Policy

1.1.1 Ensure 'Enforce password history' is set to '24 or more password(s)' 1.1.2 Ensure 'Maximum password age' is set to '365 or fewer days, but not 0' 1.1.3 Ensure 'Minimum password age' is set to '1 or more day(s)' 1.1.4 Ensure 'Minimum password length' is set to '14 or more character(s)' 1.1.5 Ensure 'Password must meet complexity requirements' is set to 'Enabled' 1.1.6 Ensure 'Relax minimum password length limits' is set to 'Enabled' 1.1.7 Ensure 'Store passwords using reversible encryption' is set to 'Disabled'

1.2Account Lockout Policy

1.2.1 Ensure 'Account lockout duration' is set to '15 or more minute(s)' 1.2.2 Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0' 1.2.3 Ensure 'Allow Administrator account lockout' is set to 'Enabled' (MS only) 1.2. Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'

2.Local Policies

2.1 Audit Policy

NA

2.2 User Rights Assignment

2.2.1 Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' 2.2.2 Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS' (DC only) 2.2.3 Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users' (MS only) 2.2.4 Ensure 'Act as part of the operating system' is set to 'No One' 2.2.5 Ensure 'Add workstations to domain' is set to 'Administrators' (DC only) 2.2.6

Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' 2.2.7 Ensure 'Allow log on locally' is set to 'Administrators, ENTERPRISE DOMAIN CONTROLLERS' (DC only) 2.2.8 Ensure 'Allow log on locally' is set to 'Administrators' (MS only) 2.2.9 Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators' (DC only) 2.2.10 Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (MS only) 2.2.11 Ensure 'Back up files and directories' is set to 'Administrators' 2.2.12 Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' 2.2.13 Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' 2.2.14 Ensure 'Create a pagefile' is set to 'Administrators' 2.2.15 Ensure 'Create a token object' is set to 'No One' 2.2.16 Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' 2.2.17 Ensure 'Create permanent shared objects' is set to 'No One' 2.2.18 Ensure 'Create symbolic links' is set to 'Administrators' (DC only) 2.2.19 Ensure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines' (MS only) 2.2.20 Ensure 'Debug programs' is set to 'Administrators' 2.2.21 Ensure 'Deny access to this computer from the network' to include 'Guests' (DC only) 2.2.22 Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group' (MS only) 2.2.23 Ensure 'Deny log on as a batch job' to include 'Guests' 2.2.24 Ensure 'Deny log on as a service' to include 'Guests' 2.2.25 Ensure 'Deny log on locally' to include 'Guests' 2.2.26 Ensure 'Deny log on through Remote Desktop Services' to include 'Guests' (DC only) 2.2.27 Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account' (MS only) 2.2.28 Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'Administrators' (DC only) 2.2.29 Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (MS only) 2.2.30 Ensure 'Force shutdown from a remote system' is set to 'Administrators' 2.2.31 Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' 2.2.32 Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (DC only) 2.2.33 Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' and (when the Web Server (IIS) Role with Web Services Role Service is installed) 'IIS_IUSRS' (MS only) 2.2.34 Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group' 2.2.35 Ensure 'Load and unload device drivers' is set to 'Administrators' 2.2.36 Ensure 'Lock pages in memory' is set to 'No One' 2.2.37 (L2) Ensure 'Log on as a batch job' is set to 'Administrators' (DC Only) 2.2.38 Ensure 'Manage auditing and security log' is set to 'Administrators' and (when Exchange is running in the environment) 'Exchange Servers' (DC only) 2.2.39 Ensure 'Manage auditing and security log' is set to 'Administrators' (MS only) 2.2.40 Ensure 'Modify an object label' is set to 'No One' 2.2.41 Ensure 'Modify firmware environment values' is set to 'Administrators' 2.2.42 Ensure 'Perform volume maintenance tasks' is set to 'Administrators' 2.2.43 Ensure 'Profile single process' is set to 'Administrators' 2.2.44 Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' 2.2.45 Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' 2.2.46 Ensure 'Restore files and directories' is set to 'Administrators' 2.2.47 Ensure 'Shut down the system' is set to 'Administrators' 2.2.48 Ensure 'Synchronize directory service data' is set to 'No One' (DC only) 2.2.49 Ensure 'Take ownership of files or other objects' is set to 'Administrators'

2.3 Security Options

2.3.1 Account

2.3.1.1 Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' 2.3.1.2 Ensure 'Accounts: Guest account status' is set to 'Disabled' (MS only) 2.3.1.3 Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' 2.3.1.4 Configure 'Accounts: Rename administrator account' 2.3.1.5 Configure 'Accounts: Rename guest account' s

2.3.2 Audit

2.3.2.1 Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' 2.3.2.2 Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' t

2.3.3 DCOM

2.3.4 Devices

2.3.5 Domain controller

2.3.6 Domain member

2.3.7 Interactive logon

2.3.8 Microsoft network client

2.3.9 Microsoft network server

2.3.10 Network access

2.3.11 Network security

2.3.12 Recovery console

2.3.13 Shutdown

2.3.14 System cryptography

2.3.15 System objects

2.3.16 System settings

2.3.17 User Account Control

3.Event Log

NA

4.Restricted Groups

NA

5.System Services

5.1 Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (DC only)

5.2 Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (MS only)

6.Registry

NA

7.File System

NA

8.Wired Network (IEEE 802.3) Policies

NA

9.Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security)

10.Network List Manager Policies

NA

11.Wireless Network (IEEE 802.11) Policies

NA

12.Public Key Policies

NA

13.Software Restriction Policies

NA

14.Network Access Protection NAP Client Configuration

NA

15.Application Control Policies

NA

16.IP Security Policies

NA

17.Advanced Audit Policy Configuration

17.1 Account Logon

17.2 Account Management

17.3 Detailed Tracking

17.4 DS Access

17.5 Logon/Logoff

17.6 Object Access

17.7 Policy Change

17.8 Privilege Use

17.9 System

18.Administrative Templates

18.1 Control Panel

18.2 Desktop

NA

18.3 LAPS(legacy)

NA

18.4 MS Security Guide

18.5 MSS(Legacy)

18.6 Network

18.7 Printers

18.8 Start Menu and Taskbar

18.9 System

18.10 Windows Components

19.Administrative Templates (User)

19.1 Control Panel

NA

19.2 Desktop

NA

19.3 Network

NA

19.4 Shared Folders

NA

19.5 Start Menu and Taskbar

19.6 System

19.7 Windows Components