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' ##2.3.3 DCOM NA ##2.3.4 Devices 2.3.4.1 Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' ##2.3.5 Domain controller 2.3.5.1 Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only) 2.3.5.2 Ensure 'Domain controller: Allow vulnerable Netlogon secure channel connections' is set to 'Not Configured' (DC Only) 2.3.5.3 Ensure 'Domain controller: LDAP server channel binding token requirements' is set to 'Always' (DC Only) 2.3.5.4 Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only) 2.3.5.5 Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only) ##2.3.6 Domain member 2.3.6.1 Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' 2.3.6.2 Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' 2.3.6.3 Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' 2.3.6.4 Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' 2.3.6.5 Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' 2.3.6.6 Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' ##2.3.7 Interactive logon 2.3.7.1 Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' 2.3.7.2 Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled' 2.3.7.3 Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' 2.3.7.4 Configure 'Interactive logon: Message text for users attempting to log on' 2.3.7.5 Configure 'Interactive logon: Message title for users attempting to log on' 2.3.7.6 (L2) Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (MS only) 2.3.7.7 Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' 2.3.7.8 Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) 2.3.7.9 Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher ##2.3.8 Microsoft network client 2.3.8.1 Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' 2.3.8.2 Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' 2.3.8.3 Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' ##2.3.9 Microsoft network server 2.3.9.1 Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)' 2.3.9.2 Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' 2.3.9.3 Ensure 'Microsoft network server: Digitally sign

communications (if client agrees)' is set to 'Enabled' 2.3.9.4 Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' 2.3.9.5 Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only) ##2.3.10 Network access 2.3.10.1 Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' 2.3.10.2 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only) 2.3.10.3 Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only) 2.3.10.4 Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' 2.3.10.5 Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' 2.3.10.6 Configure 'Network access: Named Pipes that can be accessed anonymously' (DC only) 2.3.10.7 Configure 'Network access: Named Pipes that can be accessed anonymously' (MS only) 2.3.10.8 Configure 'Network access: Remotely accessible registry paths' is configured 2.3.10.9 Configure 'Network access: Remotely accessible registry paths and sub-paths' is configured 2.3.10.10 Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' 2.3.10.11 Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only) 2.3.10.12 Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' 2.3.10.13 Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' ##2.3.11 Network security 2.3.11.1 Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' 2.3.11.2 Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' 2.3.11.3 Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' 2.3.11.4 Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' 2.3.11.5 Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' 2.3.11.6 Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' 2.3.11.7 Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' 2.3.11.8 Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher 2.3.11.9 Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' 2.3.11.10 Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' 2.3.11.11 Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts' 2.3.11.12 Ensure 'Network security: Restrict NTLM: Audit NTLM authentication in this domain' is set to 'Enable all' (DC only) 2.3.11.13 Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher ##2.3.12 Recovery console NA ##2.3.13 Shutdown 2.3.13.1 Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' ##2.3.14 System cryptography NA ##2.3.15 System objects 2.3.15.1 Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' 2.3.15.2 Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled ##2.3.16 System settings NA ##2.3.17 User Account Control 2.3.17.1 Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' 2.3.17.2 Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' or higher 2.3.17.3 Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' 2.3.17.4 Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' 2.3.17.5 Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' 2.3.17.6 Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' 2.3.17.7 Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' 2.3.17.8 Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations'

is set to 'Enabled' #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) ##9.1 Domain Profile 9.1.1 Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' 9.1.2 Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' 9.1.3 Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' 9.1.4 Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log' 9.1.5 Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' 9.1.6 Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' 9.1.7 Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' ##9.2 Private Profile 9.2.1 Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' 9.2.2 Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' 9.2.3 Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' 9.2.4 Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log' 9.2.5 Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' 9.2.6 Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' 9.2.7 Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' ##9.3 Public Profile 9.3.1 Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' 9.3.2 Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' 9.3.3 Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No' 9.3.4 Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' 9.3.5 Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' 9.3.6 Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log' 9.3.7 Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' 9.3.8 Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' 9.3.9 Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' #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 17.1.1 Ensure 'Audit Credential Validation' is set to 'Success and Failure' 17.1.2 Ensure 'Audit Kerberos Authentication Service' is set to 'Success and Failure' (DC Only) 17.1.3 Ensure 'Audit Kerberos Service Ticket Operations' is set to 'Success and Failure' (DC Only) ##17.2 Account Management 17.2.1 Ensure 'Audit Application Group Management' is set to 'Success and Failure' 17.2.2 Ensure 'Audit Computer Account Management' is set to include 'Success' (DC only) 17.2.3 Ensure 'Audit Distribution Group Management' is set to include 'Success' (DC only) 17.2.4 Ensure 'Audit Other Account Management Events' is set to include 'Success' (DC only) 17.2.5 Ensure 'Audit Security Group Management' is set to include 'Success' 17.2.6 Ensure 'Audit User Account Management' is set to 'Success and Failure' ##17.3 Detailed Tracking 17.3.1 Ensure 'Audit PNP Activity' is set to include 'Success' 17.3.2 Ensure 'Audit Process Creation' is set to include 'Success' ##17.4 DS Access 17.4.1 Ensure 'Audit Directory Service Access' is set to include 'Failure' (DC only) 17.4.2 Ensure 'Audit Directory Service Changes' is set to include 'Success' (DC only) ##17.5 Logon/Logoff 17.5.1 Ensure 'Audit Account Lockout' is set to include 'Failure' 17.5.2 Ensure 'Audit Group Membership' is set to include 'Success' 17.5.3 Ensure 'Audit Logoff' is set to include 'Success' 17.5.4 Ensure 'Audit Logon' is set to 'Success and Failure' 17.5.5 Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' 17.5.6 Ensure 'Audit Special Logon' is set to include 'Success' ##17.6 Object Access 17.6.1 Ensure 'Audit Detailed File Share' is set to include 'Failure' 17.6.2 Ensure 'Audit File Share' is set to 'Success and Failure' 17.6.3 Ensure 'Audit Other Object Access Events' is set to 'Success and Failure'

17.6.4 Ensure 'Audit Removable Storage' is set to 'Success and Failure' ##17.7 Policy Change 17.7.1 Ensure 'Audit Audit Policy Change' is set to include 'Success' 17.7.2 Ensure 'Audit Authentication Policy Change' is set to include 'Success' 17.7.3 Ensure 'Audit Authorization Policy Change' is set to include 'Success' 17.7.4 Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure' 17.7.5 Ensure 'Audit Other Policy Change Events' is set to include 'Failure' ##17.8 Privilege Use 17.8.1 Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' ##17.9 System 17.9.1 Ensure 'Audit IPsec Driver' is set to 'Success and Failure' 17.9.2 Ensure 'Audit Other System Events' is set to 'Success and Failure' 17.9.3 Ensure 'Audit Security State Change' is set to include 'Success' 17.9.4 Ensure 'Audit Security System Extension' is set to include 'Success' 17.9.5 Ensure 'Audit System Integrity' is set to 'Success and Failure' #18.Administrative Templates ##18.1 Control Panel ###18.1.1 Personalization 18.1.1.1 Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' 18.1.1.2 Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' ###18.1.2 Regional and Language Options 18.1.2.1 Handwriting personalization 18.1.2.2 Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled' ###18.1.3 Ensure 'Allow Online Tips' is set to 'Disabled' ##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

From:
https://trident365.com/ - **三叉戟**

Permanent link:
https://trident365.com/doku.php?id=resources:os:windows_server_2022:baseline&rev=1732021152

Last update: **2024/11/19 21:59**