**Windows Server Hardening Script**

* Items that is highlighted in Yellow mean it will not push successfully from Domain , it required manually to edit the setting for hardening.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Baseline | | |
| 1 | Minimum password length | **Set to at least 8 characters** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Account Policy->Password Policy |
| 2 | Minimum password Age | The minimum password age specifies the minimum amount of time a user must keep his or her password in effect. This prevents users from using a script to rotate through the password history and reuse an old password.  **Set to 0 Days** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Account Policy->Password Policy |
| 3 | Enforce Password History | **Set to 12 password remembered** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Account Policy->Password Policy |
| 4 | Password Maximum Age | The maximum password age establishes the amount of time before the system requires a user to change their password.  **Set Maximum password age to 60 Days** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Account Policy->Password Policy |
| 5 | Account Lockout Threshold | Password attacks are often automated “guessing” programs that can brute force user passwords. The threshold setting can help deter password compromise.  **Set Account Lockout Threshold to 3.** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Account Policy->Account Lockout Policy |
| 6 | Account Lockout Duration | The account lockout duration determines the number of minutes the account remains unavailable.  **Set Account Lockout Duration to 0 minutes** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Account Policy->Account Lockout Policy |
| 7 | Reset Account Lockout | Users may sometimes accidentally forget their passwords and lock themselves out of the system. This setting allows them to wait a minimum amount of time and try again. Must be set lower than or equal to the Account lockout duration.  **Set Reset Account lockout to 99999 minutes.** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Account Policy->Account Lockout Policy |
| 8 | Rename Administrator Account | Rename the Administrator account to prevent an attacker from easily guessing the Administrator username. Create a dummy administrator account to log attempted accesses.  Administrator account to **bpm888** and Logoff.  Login bpm888 and create a “Administrator” account.  Add a strong password (i.e. Pa$$worD07) to the account and keep securely. | Built-in administrator have renamed to bpm888  Added local administrator “Penril” and password “P@$$w0rd”  Add one more administrator and password Pa$$worD07 |
| 9 | Rename & Disable Guest Account | The Guest account should be disabled to prevent access to unauthorized users. A malicious user could use this account and escalate privileges or insert malware onto the system.  Rename Guest account to **pelawat** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Security Options |
| 10 | Local Audit Account Logon Events | This provides a method of tracking user logon and logout activities.  **Set Audit account logon events to Success, Failure** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Audit Policy |
| 11 | Local Audit Account Management | This action provides a method of tracking management actions, like creating new users.  **Set Audit account management to Success, Failure** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Audit Policy |
| 12 | Local Audit Directory Services Access | This feature provides a method of tracking access to the Windows 2000 Active Directory.  **Set Audit directory service access to Success, Failure.** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Audit Policy |
| 13 | Local Audit Logon Events | This feature allows for the tracking of logon events and is useful in forensic analyses after a system has been compromised.  **Set Audit logon events to Success, Failure** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Audit Policy |
| 14 | Local Audit Object Access | This feature allows for the tracking of access to system objects like specifically defined files, folders, or hardware like printers.  **Set Audit object access to Success, Failure** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Audit Policy |
| 15 | Local Audit Policy Change | This feature is used to monitor policy changes and can be used as an early warning indication that event logging has been disabled.  **Set Audit policy change to Success, Failure** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Audit Policy |
| 16 | Local Audit Privilege Use | This feature can be used to track user attempts to exercise privileges on file systems, folders, and objects.  **Set Audit privilege use to Failure only.** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Audit Policy |
| 17 | Local Audit System Events | Used to track system events like services starting and stopping. Can be very useful in troubleshooting problems with servers and processes.  **Set Audit system events to Success, Failure.** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Audit Policy |
| 18 | Audit process tracking | This security setting determines whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access.  If you define this policy setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when the process being tracked succeeds. Failure audits generate an audit entry when the process being tracked fails.  To set this value to No auditing, in the Properties dialog box for this policy setting, select the Define these policy settings check box and clear the Success and Failure check boxes.  **Set Audit process tracking to Failure only.** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Audit Policy |
| 19 | Maximum Log Size | Sets the Maximum size of this event log.  **Application Log Size - 30016 KB**  **Security Log Size - 50496 KB**  **System Log Size - 30016 KB** | GPEDIT->  Computer Configuration -> Administrative Templates -> Windows Components -> Event Log Service |
| 20 | Retention Method For Application/Security/System Logs | This feature allows the administrator to choose how log files will archived, rotated, or retained for backup.  **Set to Overwrite events as needed** | GPEDIT->  Computer Configuration -> Administrative Templates -> Windows Components -> Event Log Service->APP->Retain (Disable) |
| 21 | Allow System Shut Down Without Logon | This feature allows for shut down of the computer without logging on.  **Set Allow system to be shut down without having to log on to DISABLED.** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Security Options -> shutdown : |
| 22 | Do Not Display Last User Name In Logon Screen | A malicious person with physical access to a computer could gain username information and later run automated brute force tools to compromise an account.  **Set do not display last user name to ENABLED.** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Security Options |
| 23 | Interactive logon: Message text for users attempting to log on | This feature provides criminal trespass warnings for those that unlawfully enter your system.  **Set to:**  **"The Server you are about to enter is strictly confidential. Only authorized personnel for authorized purposes shall have and is entitle to access to this system. Any unauthorized User shall be subject to legal and disciplinary proceedings."** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Security Options |
| 24 | Interactive logon: Message title for users attempting to log on | This feature provides criminal trespass warnings for those that unlawfully enter your system.  **Set to :**  **“WARNING!: THIS IS A SECURE SERVER”** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Security Options |
| 25 | Interactive logon: Prompt user to change password before expiration | This is a reminder feature designed to let users know their accounts will be disabled if they do not change their password within XX days.  **Set prompt user to change password to 14 days.** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Security Options |
| 26 | Audit the use of Backup and Restore privilege | **Set to Enabled.** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Security Options |
| 27 | Shutdown: Clear virtual memory pagefile | **Set to Enabled.** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Security Options |
| 28 | Recovery Console: Allow Automatic Administrative Logon | **Set to Enabled.** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Security Options |
| 29 | Recovery Console: Allow Floppy Copy and Access to all Drives and all Folders | **Set to Disabled.** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Security Options |
| 30 | Restrict CD-ROM Access to Locally Logged-On User Only | **Set to Enabled.** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Security Options |
| 31 | ResSHUtrict Floppy Access to Locally Logged-On User Only | **Set to Enabled.** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Security Options |
| 32 | Microsoft network client: Send unencrypted password to third-party SMB servers: | **Set to Disabled.** | GPEDIT->  Computer Configuration -> Windows Setting ->Security Setting-> Local Policies->Security Options |
| 33 | Devices: Unsigned driver installation behavior | **Set to Warn but allow installation.** | Not Applicable in Windows Server 2008 R2 |
| 34 | Password Protected Screen Saver | **Password protect the screen saver to enabled.**  **Screen saver timeout to enabled (900 second)** | GPEDIT->User Configuration ->Administrative Templates -> control panel -> Personalization -> Password Protect |
| 35 | Domain Controller/Local – Access Control | Under Control Panel, Administrative Tools, Local Security Policy, Local Policies, Users Right Assignment, **Remove Users, Power Users and Everyone from**  **Access this computer from the local, only**  Administrators  Remote Desktop Users  Backup Operators  IWAM - Guest  IUSR - Guest  Application ID  **Access this computer from the network, only**  Administrators  Remote Desktop Users  Backup Operators  IWAM - Guest  IUSR - Guest  Application ID | GPEDIT->Windows Setting -> security settings-> Local Policies -> User Rights Assignment |
| 36 | Local – Disable Autoplay | Click START, Run, type **gpedit.msc** and click OK, Local Computer Policy, **Computer Configuration**, Administrative Template, System, Turn off Autoplay, Enabled, All Drives, OK  Click START, Run, type **gpedit.msc** and click OK, Local Computer Policy, **User Configuration**, Administrative Template, System, Turn off Autoplay, Enabled, All Drives, OK | GPEDIT->Windows Setting -> Administrative Templates -> Windows Components-> Autoplay Policies  GPEDIT->User Configuration -> Administrative Templates -> Windows Components-> Autoplay Policies |
| 37 | Install Antivirus | **Install Symantec Antivirus (Server Version)** |  |
| 38 | Join Domain | Server join @agrobank.com.my domain |  |
| 39 | Apply Patch | **Windows Update** |  |